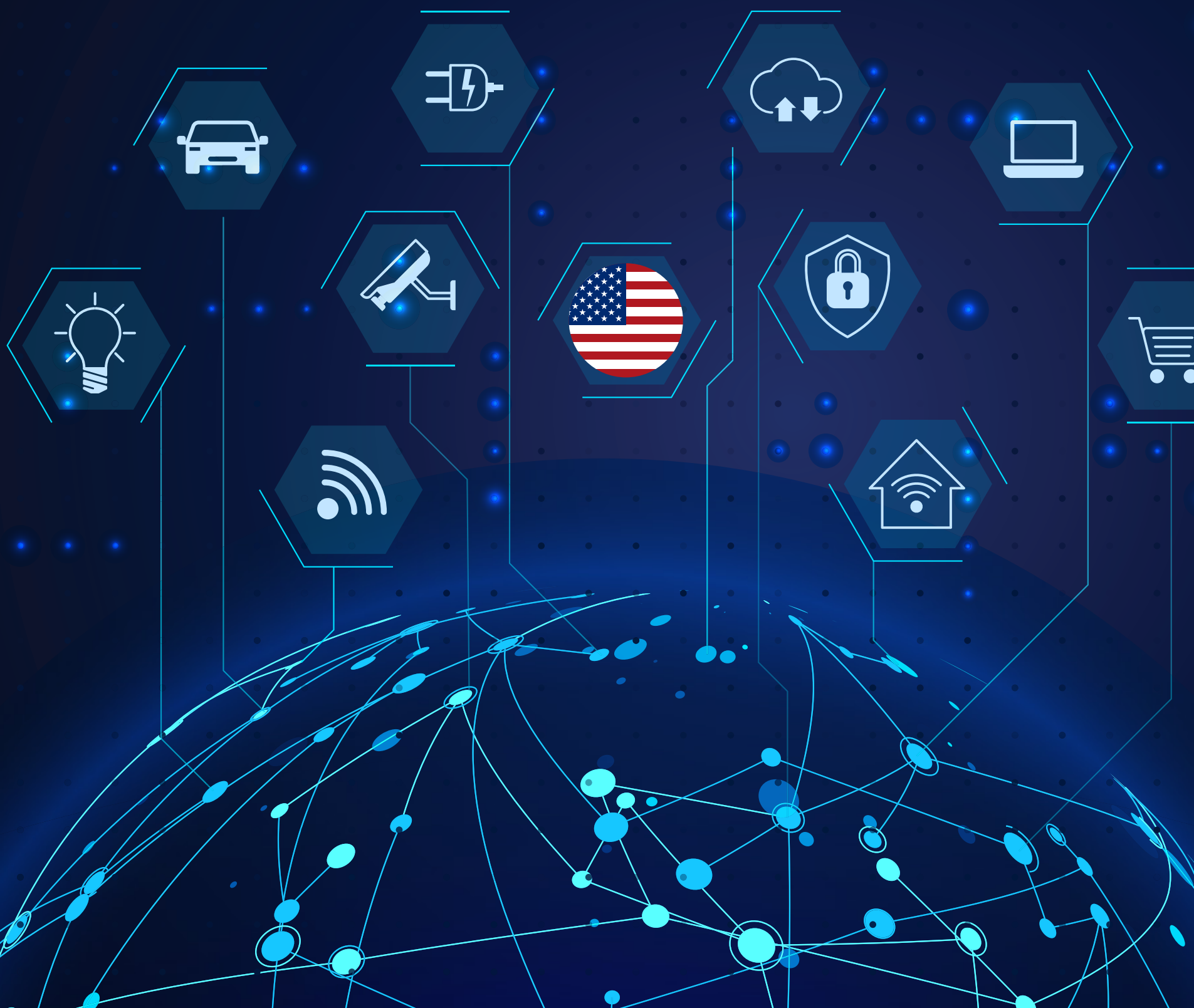
SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

NATIONAL SECURITY SURVEILLANCE IN THE UNITED STATES: LAWS, INSTITUTIONS, AND SAFEGUARDS

Adam Klein



ABOUT THE AUTHOR

Adam Klein is Director of the Strauss Center and Director of Strauss' Program on Technology, Security, and Global Affairs. Adam also serves as a Senior Lecturer at the School of Law. Before joining the Strauss Center, Adam served as Chairman of the United States Privacy and Civil Liberties Oversight Board, the independent, bipartisan federal agency responsible for overseeing counterterrorism programs at the NSA, FBI, CIA, Department of Homeland Security, and other federal agencies. As the Board's Senate-confirmed Chairman, he oversaw its oversight and advice engagements with other federal agencies, while also serving as the Board's chief executive office .

Before entering government, Adam was the Robert M. Gates Senior Fellow at the Center for a New American Security, a bipartisan national-security research institution in Washington, DC. There, his research focused on government surveillance, intelligence powers, and national security law. Previously, Adam practiced law at Wilmer Cutler Pickering Hale & Dorr, LLP and served as a law clerk to Justice Antonin Scalia of the U.S. Supreme Court and Judge Brett Kavanaugh of the U.S. Court of Appeals for the D.C. Circuit. He has also worked on national-security policy at the RAND Corporation, the 9/11 Public Discourse Project (the non-profit successor to the 9/ 1 Commission), and in the U.S. Congress. He received his BA from Northwestern University and his JD from Columbia Law School.

Adam is a former Council on Foreign Relations International Affairs Fellow and Robert Bosch Foundation Fellow in Berlin. He speaks German and French.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

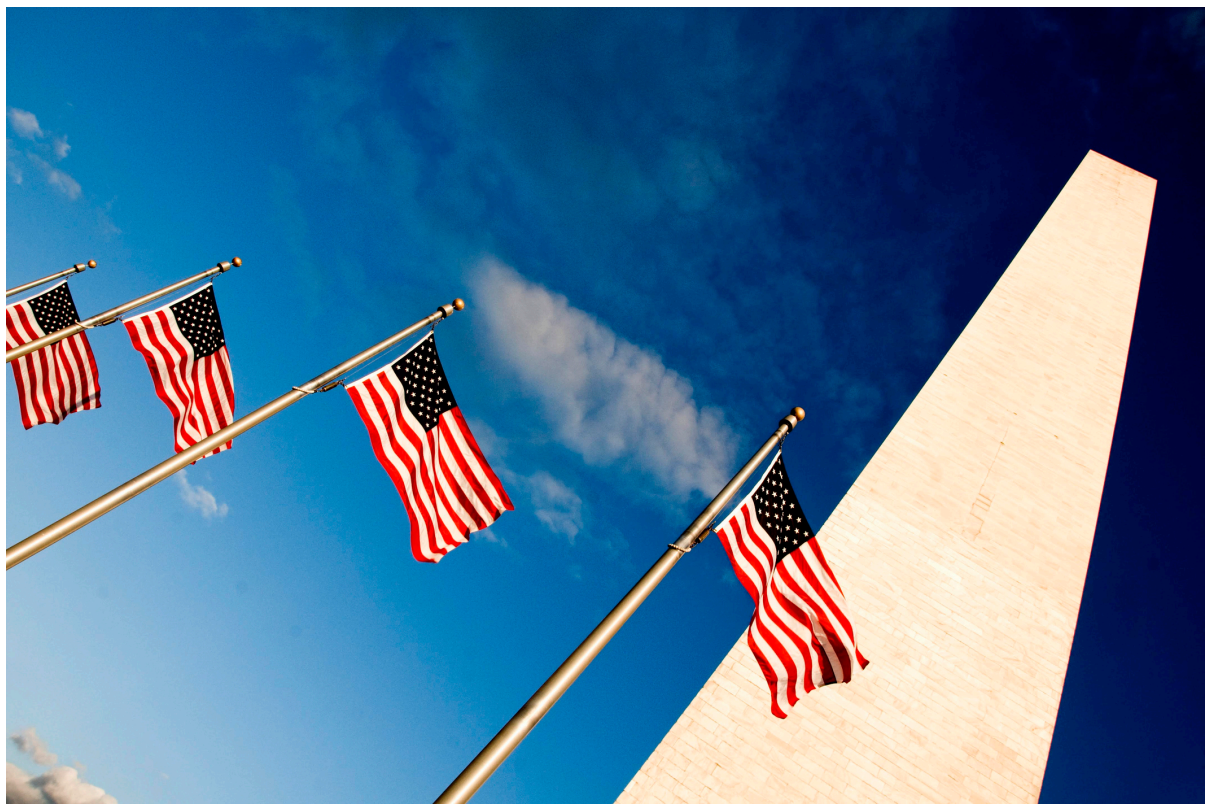
I. INTRODUCTION

The United States' use of electronic surveillance for national security purposes is unique in several respects. Its intelligence agencies boast large workforces, lavish funding, and elite technical prowess. Yet they must supply an unusually broad range of needs generated by America's global military presence, worldwide interests, diversified and globally integrated economy, and open society (with the attendant counterintelligence risks).

The United States also stands out for the sheer volume of information that has been made public, by means fair and foul, about its surveillance and signals-intelligence (SIGINT) activities. Surveillance programs are governed by an extensive body of detailed, publicly available statutes, executive orders, and agency policies.

Unclassified or declassified opinions issued b ordinary courts and the specialized Foreign Intelligence Surveillance Court provide additional insight. Whistleblowers who follow the lawful process are another source of transparency and accountability, though their claims often become entangled in political debates. Finally, unauthorized leaks have made headline-grabbing revelations, uncovering occasional excesses but also burning lawful programs.

The U.S. oversight regime is multilayered and encompasses all three branches of the federal government: executive, legislative, and judicial. The oversight landscape was reshaped by the 2013 Snowden revelations, with new or reinvigorated bodies policing the intelligence agencies.



Despite these improvements, the sufficiency of existing mechanisms remains hotly debated—most notably, the efficacy of the Foreign Intelligence Surveillance Court

U.S. surveillance practices and the attendant safeguards have been an object of intense global interest since the Snowden leaks. One reason is the sheer scale and global reach of the U.S. intelligence community, especially the National Security Agency and its Five Eyes partners. Another is the central position that the United States and its large technology companies occupy in global networks. The U.S. government's interactions with those companies thus influence the privacy and security of billions of internet users around the world.

> ***The United States also stands out for the sheer volume of information that has been made public, by means fair and foul, about its surveillance and signals-intelligence (SIGINT) activities. Surveillance programs are governed by an extensive body of detailed, publicly available statutes, executive orders, and agency policies.***

Much post-Snowden debate about U.S. surveillance practices has focused on the scale of U.S. agencies' collection and whether U.S. safeguards meet European Union standards for outbound data transfers. But transatlantic comparisons quickly reach the point of diminishing returns. The scale of U.S. SIGINT collection may exceed EU member states' collection, but no EU member state has international obligations comparable to the U.S. alliance network and nuclear umbrella. On the other hand, U.S. statutory and administrative rules may be relatively detailed, and transparency and oversight (at least since Snowden) relatively robust, but the U.S. also occupies a singularly sensitive position with respect to technologies on which much of the world depends.

This paper thus does not enter the debate about whether U.S. practices are better or worse than those of EU member states. Nor does it aspire to replicate the existing catalogues of relevant laws and institutions that have been prepared as part of U.S.-EU negotiations.[1]

Instead, it offers an overview of U.S. practices and institutions while situating them within broader trends in governance, technology, and politics. It also attempts to highlight underappreciated factors—for example, the U.S.'s unique geopolitical position—that strongly influence the American approach to national security surveillance.

II. BUDGETS AND CAPABILITIES

Budgets

The United States pours immense resources into intelligence programs. For Fiscal Year 2024, the Biden administration has requested $72.4 billion for the National Intelligence Program, which "includes all programs, projects and activities of the intelligence community as well as any other intelligence community programs designated jointly by the DNI and the head of department or agency, or the DNI and the President."[2] The National Intelligence Program budget funds the CIA, intelligence functions of the FBI, and significant parts certain Department of Defense intelligence agencies, such as the National Security Agency, the National Geospatial-Intelligence Agency (NGA), and National Reconnaissance Office (NRO)

Intelligence programs that support tactical military operations are collectively known for budgetary purposes as the Military Intelligence Program. For FY 2024, the Biden Administration has requested an additional $29.3 billion for those programs.

Until relatively recently, those "top-line" intelligence budgets remained classified. In 2004, the National Commission on Terrorist Attacks Upon the United States, known as the 9/11 Commission, recommended in its final report that "to combat the secrecy and complexity" surrounding the intelligence apparatus, "the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret."[3] Congress implemented this recommendation in 2007, requiring the Director of National Intelligence to disclose the aggregate amount to the public each year.[4]

The budgets of individual intelligence agencies remain classified

Capabilities

While many capabilities remain classified, it can be safely assumed that these generous budgets buy an impressive level of technical and human capability.

Comparisons across nations are difficult given the pervasive secrecy surrounding SIGINT and national security surveillance. However, one respected ranking, the Belfer Center's "National Cyber Power Index" rates the United States as the world's premier cyber and intelligence power.[5] The Belfer Center index also ranks countries within various sub-disciplines, including cyber-enabled "Foreign Intelligence Collection for National Security" and "Surveilling and Monitoring Domestic Groups." The United States led on the former; on domestic surveillance, however, China held the top spot by a wide margin

The United States' SIGINT capabilities are amplified by international partnerships. The most important is the "Five Eyes," named after the five English-speaking countries that participate: the United States, United Kingdom, Canada, Australia, and New Zealand. These allies contribute both technical expertise and geographic presence in important regions of the globe.

The Five Eyes arrangement, born out of the 1946 "UKUSA" agreement,[6] provides a framework for extensive (though not total)[7] cooperation in SIGINT collection and intelligence sharing. The NSA also cooperates closely with counterparts in other allied countries, and the CIA is known to maintain "liaison" relationships with its counterpart services across the world.

Individual agencies' operational capabilities are discussed further in the next section.

III. KEY OPERATIONAL AGENCIES

The agencies with primary responsibility for conducting electronic surveillance and SIGINT for national security purposes are the National Security Agency, the Federal Bureau of Investigation, and the Central Intelligence Agency, though other agencies contribute too.

The scope of each agency's activities is bounded by its *legal authorities*—statutes or executive orders that empower the agency or constrain it. For example, the National Security Act of 1947[8] empowers the CIA to "collect intelligence through human sources and by other appropriate means," "correlate and evaluate intelligence related to the national security," and conduct covert action.[9] However, the Act forbids CIA from carrying out "police, subpoena, or law enforcement powers or internal security functions."[10] Executive Order 12,333 contains other authorities, presidential instructions, and prohibitions directed to the member agencies of the Intelligence Community.

National Security Agency (NSA)

The National Security Agency, which is part of the Department of Defense, is the U.S. Intelligence Community's lead agency[11] for collecting signals intelligence—that is, for "collecting foreign intelligence from communications and information systems and providing it to customers across the U.S. government, such as senior civilian and military officials. [12] The NSA also has a longstanding "information assurance" mission, now carried out by its Cybersecurity Directorate. In that role, NSA is responsible for protecting sensitive government networks and the defense industrial base.[13] The NSA is widely acknowledged as the U.S. government's premier repository of technical expertise on global communications networks, cryptography, computer network operations, and related technical fields

The NSA was created in the early 1950s, but the U.S. government had been episodically intercepting and decoding electronic communications on an organized basis since at least World War I, and in a less institutionalized fashion as far back as the Civil War. That history, however, was uneven. In 1929, Secretary of State Henry Stimson terminated the government's successful "Cipher Bureau," which for more than a decade had intercepted and decoded foreign diplomatic cables.[14] "Gentlemen," Stimson famously sniffed, "do not read each other's mail."[15] Even SIGINT successes were sometimes undermined by ineffectual analysis. Before Pearl Harbor, for example, the government failed to realize the significance of decrypted Japanese government cables describing preparations for war.

The intense U.S.-Soviet rivalry of the early Cold War left no room for gentlemanly sentiments. President Truman permanently established the NSA in 1952 by Top Secret memorandum.[16] Even that memorandum remained classified for decades, and the agency became known for extreme secrecy: NSA, the joke ran, stood for "No Such Agency." The Snowden leaks of 2013 jolted NSA leaders out of their insularity. Since then, NSA leaders have engaged regularly with the press and public to explain the NSA's mission and the legal and institutional constraints.

Most NSA activities remain classified today, though oversight reports, journalistic accounts, and illegal disclosures have filled in some details. Generally speaking, the NSA's global SIGINT activities collect and analyze communications and other electronic signals to produce foreign intelligence relevant to topics identified by the President and National Security Council in the National Intelligence Priorities Framework.[17] The Framework is not public, but outsiders can hazard a reasonable guess by considering the United States' geopolitical priorities and consulting the Intelligence Community's Annual Threat Assessment.[18]

> ***The NSA was created in the early 1950s, but the U.S. government had been episodically intercepting and decoding electronic communications on an organized basis since at least World War I, and in a less institutionalized fashion as far back as the Civil War.***

NSA's SIGINT activities are characterized by an elite level of technical sophistication and geographic reach, the latter being helped by the United States' worldwide alliance network and military footprint. The SIGINT agencies of the four other members of the "Five Eyes," known in agency jargon as "second-party" partners, are the NSA's closest international collaborators, though NSA also collaborates closely with a wide network of allied "third-party" services.

NSA is a *foreign*-intelligence agency, and a focus on foreign targets is embedded in its legal authorities and internal culture. However, NSA is one of the two agencies publicly acknowledged as participating in surveillance conducted in the United States under the Foreign Intelligence Surveillance Act.[19] It also has a lead role in implementing U.S.-based surveillance of overseas targets under FISA Section 702.[20]

Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation, which is part of the Department of Justice, has primary responsibility for clandestine national security surveillance inside the United States. But the Bureau's mission is not limited to threats of domestic origin.

The FBI also uses electronic surveillance to collect foreign intelligence and to protect against foreign threats to U.S. national security, such as counterintelligence and counterterrorism.

The Bureau's history of electronic surveillance dates back more than a century, to its origins as the "Bureau of Investigation" within the Department of Justice. Over more than a half-century, the Bureau conducted thousands of clandestine wiretaps of dubious legality. Many targeted legitimate threats like Nazi and Soviet spies. Many others, however, targeted political dissidents, peaceful civil-rights campaigners, and even government officials who were opponents of longtime FBI Director J. Edgar Hoover. Hoover was an organizational genius who made the FBI the world's preeminent crime-fighting o ganization. Yet he was also a paranoid manipulator who gathered political *kompromat* to discredit opponents and protect his power.

Successive waves of reform have brought important legal and institutional constraints to the Bureau. Yet its intelligence activities remain a source of controversy, and a series of high-profile recent errors have contributed to polarization around its work.[21]

Today's FBI has three missions,[22] each of which involves the use of electronic surveillance:

- Criminal investigation: the Bureau is the federal government's principal investigative agency for violations of federal criminal law.
- Protecting against threats to national security: the FBI is tasked with detecting and helping prevent acts of terrorism, espionage, sabotage, and assassination.
- Collecting foreign intelligence: the FBI also collects information that may not relate directly to an immediate threat to national security, but that nonetheless constitutes foreign intelligence.[23]

These missions often overlap. Terrorism, for example, is both a crime and a threat to national security, and terrorist organizations are priority foreign-intelligence targets.

Before 9/11, however, Justice Department employees often drew an unduly hard line between criminal and intelligence investigations of terrorism. The resulting "wall" impeded information sharing and contributed to the government's failure to stop the 9/11 attacks.[24] The USA PATRIOT Act of 2001 and subsequent court decisions eliminated those barriers, with the effect that criminal and national security investigations are better coordinated today.[25]

Globally, the FBI stands out as the rare domestic service with both criminal-investigative and intelligence duties. The dual mission has drawn criticism, however. After the 9/11 attacks, prominent voices called for stripping the FBI of its intelligence role and creating a new domestic, intel-only service like Britain's Security Service (MI5).[26] The 9/11 Commission considered this idea but ultimately did not recommend it. Instead, FBI Director Robert Mueller sought to remake the Bureau into an intelligence-driven organization, with analysts integrated alongside its traditional "special agents" in the FBI workforce.[27] The debate has never entirely disappeared, however, and calls to strip the FBI of its national-security mission have revived in response to recent controversies surrounding the Bureau.[28]

The FBI can call upon wide-ranging surveillance powers in its criminal investigations: wiretaps for real-time interception,[29] grand-jury subpoenas and court orders[30] to compel the production of data stored by third parties, and search warrants to obtain stored content.[31]

For foreign-intelligence and counterterrorism investigations, however, the FBI can also draw upon powers granted by the Foreign Intelligence Surveillance Act. The FBI uses "traditional" FISA authorities, such as electronic surveillance and physical search, to monitor "agents of a foreign power" in the United States.[32] Other provisions of FISA permit the Bureau to obtain various types of metadata.

The FBI can also use "National Security Letters," which are essentially administrative subpoenas issued with the approval of a supervisory FBI official. There is no judicial involvement. NSLs are available only in national security investigations and can be used to obtain "customer and consumer transaction information"—but not content—from "communications providers, financial institutions, and credit agencies. [33]

Congress tightened the rules for NSLs in 2015's USA Freedom Act.[34] The Act banned the use of NSLs for bulk collection, seeking to close loopholes that might allow a recurrence of something resembling the bulk telephone-call-records program revealed by Edward Snowden. It also boosted transparency by allowing companies that receive NSLs to report in numerical bands how many NSLs they received. And it narrowed (though not to the complete satisfaction of civil libertarians) the FBI's ability to impose "gag orders" on companies that receive NSLs.[35]

The FBI can call upon wide-ranging surveillance powers in its criminal investigations: wiretaps for real-time interception, grand-jury subpoenas and court orders to compel the production of data stored by third parties, and search warrants to obtain stored content.

For foreign-intelligence and counterterrorism investigations, however, the FBI can also draw upon powers granted by the Foreign Intelligence Surveillance Act.

The FBI is also involved in targeting and receiving raw data under FISA's powerful Section 702, which permits the intelligence community to target non-U.S. persons located abroad who use U.S. communications infrastructure and providers. The Bureau can nominate targets for 702 collection[36] and receives a small percentage of the "raw take" from the program.[37]

Yet the FBI has struggled to adhere to rules governing its use of 702 data—most notably, the rules about when agents can search ("query") the database. As a result, its modest role in the program has produced an outsized share of controversy. As Congress debates reauthorization of Section 702 this year, the FBI's querying of 702 data is one of the most contested elements of the reauthorization debate.

Finally, the FBI uses targeted hacking, sometimes referred to as "network investigative techniques," to investigate crimes ranging from darknet child pornography rings to cryptocurrency theft. Its use of these techniques typically requires a search warrant under Rule 41 of the Federal Rules of Criminal Procedure.[38]

Central Intelligence Agency (CIA)

The CIA's principal missions are to collect human intelligence (HUMINT) and produce all-source intelligence analysis. It is prohibited by law from conducting electronic surveillance in the United States, with very narrow exceptions for training and counterintelligence.[39] Yet CIA's prowess in the digital realm is formidable, and changes in technology are reshaping its traditional human-intelligence mission. As former CIA officer Brian Katz has explained

> The digitization of secrets sought by the IC is blurring the traditional boundaries that separate the HUMINT, SIGINT, and cyber disciplines—and the agencies organized around them. The blending of technical tools with collection missions, such as HUMINT officers using SIGINT tools, could enable more penetrating foreign intelligence collection . . . .[40]

Public information suggests that CIA has developed impressive capabilities in the digital realm. In 2015, Director John Brennan created a new "Directorate of Digital Innovation" within CIA to "lead efforts to track and take advantage of advances in cyber technology to gather intelligence."[41] The "Vault 7" leaks and the subsequent conviction of former CIA programmer Joshua Schulte provide some indication of the CIA's significant investment in cyber capabilities [42]

In short, digitization has reshaped what and how CIA collects. In the digital age, hacking operations and even more traditional methods of espionage[43] can yield large datasets, not just individual fragments of information. The CIA also receives raw intelligence from FISA Section 702. The opportunities and compliance challenges that come with the large volumes of raw data that digital-age spying could bring onto CIA systems are thus conceptually similar to those that face NSA, a pure SIGINT agency.[44] That would not have been true before the ubiquitous digitization of the last 20 years.

Other Agencies

Other intelligence community and law-enforcement agencies may collect signals or conduct electronic surveillance for purposes within their authorized missions.

Some of these lesser-known programs ingest large quantities of data. For example, the Terrorist Finance Tracking Program, which is operated by the Department of the Treasury pursuant to an agreement between the United States and the European Union, collects data from the interbank communications consortium SWIFT. Treasury then runs queries against that data for counterterrorism purposes. Many of those queries are run on behalf of foreign partners, including Europol and the governments of EU Member States.[45]

In addition, many agencies *receive* the fruits of collection via sharing from Intelligence Community partners.[46] How to regulate such "dissemination" of intelligence information across the government has been an important focus of post-9/11 reforms.

Greater sharing was a key recommendation of the 9/11 Commission, and intelligence community leaders have sought to reduce legal[47] and technical[48] barriers to sharing information. These efforts seek to enable agencies to "connect the dots": that is, to discover hidden connections in the intelligence community's holdings.[49]

Other efforts, however, have focused on *limiting* such disseminations in various respects to protect civil liberties and prevent political abuses. For example, the rules governing "masking" and "unmasking" of the identities of Americans named in intelligence reports have come under scrutiny since the 2016 presidential campaign and transition.[50] The Office of the Director of National Intelligence has also reissued and updated rules protecting the identities of Members of Congress named in intelligence reports.[51]

IV. AUTHORIZATION AND OVERSIGHT

In the U.S. system, surveillance targets are sometimes approved by a court (for foreign-intelligence surveillance, as opposed to criminal investigations, the Foreign Intelligence Surveillance Court), other times by officials within an agency. The process depends upon the legal authority for the surveillance.

Oversight, by contrast, implies after-the-fact review. It can be granular, as in the case of an inspector general reviewing an individual case of misconduct. Or it can be programmatic, as in the case of the Privacy and Civil Liberties Oversight Board, which typically assesses programs holistically, rather than reviewing individual incidents.

Authorization: Ex Ante Review

Grand Juries and Ordinary Federal Courts

Wiretaps and requests for stored data in criminal investigations are commonly used in national security investigations. Espionage, terrorism, sanctions-busting, dodging export controls, and hacking are crimes, as well as national security threats. The process for conducting criminal investigations is well understood, supervised by courts, and subject to public accountability in open trials and appeals. It is thus not covered in detail here.

Foreign Intelligence Surveillance Court

Surveillance under the Foreign Intelligence Surveillance Act must be approved by the Foreign Intelligence Surveillance Court, or FISA Court.[52]

The Court operates out of a secure courtroom in the E. Barrett Prettyman Federal Courthouse in Washington, DC.

It consists of life-tenured "Article III"[53] judges who have been presidentially appointed and Senate confirmed to seats on other federal district courts. The Chief Justice of the United States designates 11 district judges to serve on the FISA Court and three circuit judges to serve on the appellate Foreign Intelligence Surveillance Court of Review (FISCR).[54]

The Court is advised by a panel of court-appointed amici curiae, or "friends of the court," who hold top-secret clearances and are available to assist the court upon request.[55] The current amici are lawyers and technologists with expertise in national security, civil liberties, and technology.[56]

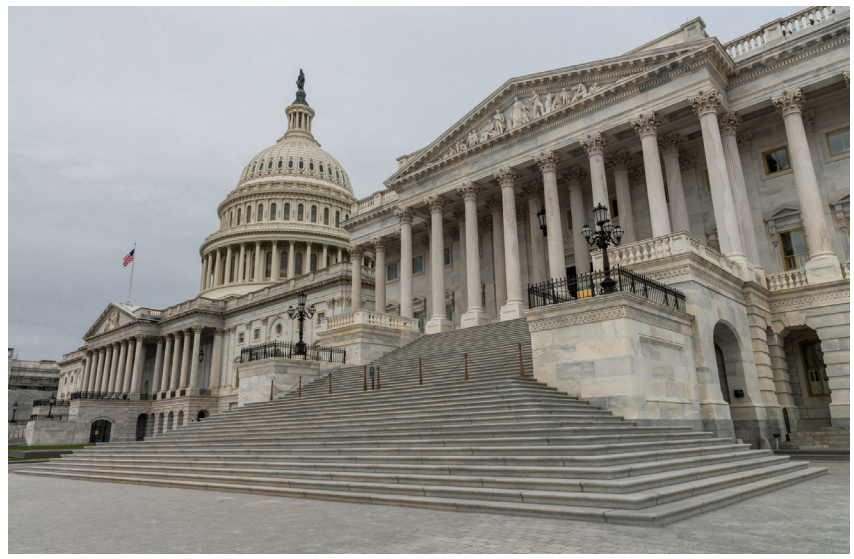
Whether to appoint an amicus in a given case is largely up to the judge. Under the statute, the court "shall appoint" an amicus when a case, "in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate"; the court "may" appoint an amicus in other matters.[57] In 2022, the FISA Court made four amicus appointments and one finding that such an appointment would not be appropriate.[58]

Observers have proposed strengthening the FISC's amicus panel in various ways. Some have focused on expanding the set of cases in which an amicus must be appointed—for example, by requiring an amicus appointment in every annual review of 702 certifications, on the theory that these are by their nature complex and systemically significant.[59] Amici could also be empowered to cast an independent and skeptical eye on the facts (rather than merely providing legal or technical input) in certain sensitive matters.[60] No amicus opined, for instance, during the reviews of the four flawed applications to surveil Trump campaign advisor Carter Page.

Others would go further and give the amicus the power to appeal to the FISCR from decisions in the government's favor. It is unclear, however, whether an amicus, who is not personally affected by the surveillance, would have constitutional standing to appeal. Another persistent concern with expanding the amicus's role has been the "originator control" principle, which limits onward sharing of information provided by a cooperating foreign service.[61]

The amicus has proven its value in various FISC proceedings since the panel was formalized in 2015. Amici have raised new legal arguments, proposed new remedies, and helped the FISC respond to government noncompliance.[62]

The process by which the Court authorizes surveillance, and the rigor of its proceedings, are considered in more detail below.[63]



Oversight Entities: Ex Post Review

Many institutions oversee the U.S. government's use of national security surveillance.

These bodies have emerged over five decades, as successive waves of reform created new control bodies within and outside the Executive Branch.

That growth has not been entirely smooth, however. Many of these reforms were prompted by scandals or embarrassing revelations, beginning with the Watergate scandal and the revelations of the 1970s Church Committee, which revealed widespread abuses of intelligence powers. A more recent shock was Edward Snowden's disclosure that the NSA was collecting, in bulk, metadata records of Americans' phone calls. He also revealed that the FISA Court had approved the program, in secret, based on a dubious interpretation of the relevant statute—suggesting that there were deep shortcomings in the existing oversight system.

The system has changed considerably since then. Improvements include a fully constituted Privacy and Civil Liberties Oversight Board, a statutorily mandated FISC amicus panel, new transparency mandates, and stronger Civil Liberties and Privacy Officers within agencies.

Congress

The most powerful and important oversight bodies are in Congress: the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

The committees pass legislation related to U.S. intelligence programs, approve nominations to senior positions in the Intelligence Community, and conduct oversight of classified and unclassified aspects of U. intelligence activities.

The committees' oversight is aided by a broad statutory requirement that intelligence agencies keep the committees "fully and currently informed of all intelligence activities . . . which are the responsibility of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government."[64] The agencies must also hand over all information requested by the committees. Each Committee maintains a "Sensitive Compartmented Information Facility," or SCIF, to enable it to receive and store classified material and hold classifie meetings or hearings.

Other committees have more limited jurisdiction with respect to certain intelligence programs. The House and Senate Judiciary Committees oversee and legislate with respect to FISA.[65] The Armed Services Committees oversee certain military intelligence activities conducted by the Department of Defense.

Congress also controls the purse, a power exercised through the powerful House and Senate Appropriations Committees. Intelligence programs are funded through the appropriations subcommittees on defense.

In theory, the purse should be a powerful source of leverage for the appropriations committees. The 9/11 Commission doubted the efficacy of this arrangement, however, and recommended that intelligence funding be split off into its own subcommittee.[66] Most of the subcommittees' attention, it reasoned, would naturally fall on the much larger defense budget, leading to insufficient scrutiny of intelligence spending

Whatever the merits of that critique, the Commission's recommendation on this point was not adopted—one of the few 9/11 Commission recommendations that was never implemented.[67]

Executive Branch

Many entities within the Executive Branch contribute to oversight of national security surveillance.

Within Agencies - CLPOs, Compliance Offices, Offices of General Counsel

Closest to the operational level are oversight and compliance entities within the agencies: compliance and audit units, offices of general counsel, and Civil Liberties and Privacy Officers (CLPOs). These are not "independent" oversight entities—they are part of the agencies they oversee—but they contribute significantly to the cultures of legal and policy compliance within agencies.

There is some variation across agencies. NSA's CLPO reports to the Director and the agency's compliance office manages a technically sophisticated, robust compliance program. Over time, NSA has developed a strong tradition of self-reporting potential compliance errors.

By contrast, the FBI's compliance mechanisms are less centralized and less digitized. In response to a series of errors related to the 2016 presidential campaign, Attorney General William Barr ordered the FBI to create a new Office of Internal Auditing.[68] The new office is now operational and has begun producing publicly available reports about its work.[69]

Department of Justice

The Department of Justice (DOJ) oversees certain surveillance activities conducted by other agencies. Lawyers in the Department's National Security Division (NSD) review every target under Section 702 to ensure compliance with the court-approved targeting procedures. NSD lawyers also travel periodically to FBI field offices to conduct compliance reviews. That low-tech approach, while conducted in good faith, stands out as an opportunity for improvement in an era of cloud-computing and AI.

Justice Department lawyers also represent the government before the FISA Court. In theory, this should make them a powerful check on misrepresentations and omissions in FISA applications. At times, however, the Department's oversight has been undermined by inaccurate information given to DOJ lawyers by the FBI.[70] In the wake of damaging blunders (and some intentional FBI misconduct) in preparing the Carter Page FISA applications, the Department has started checking many FISA applications for omissions, which it can only do by reviewing the full case file. This is labor-intensive but will help bolster the accuracy and credibility of FISA applications.

Inspectors General

After the Watergate scandal of the early 1970s, Congress began creating inspectors general to detect waste, fraud, and abuse within the Executive Branch. NSA and CIA have their own inspectors general, who periodically issue public reports.[71] The Department of Justice Inspector General oversees the FBI. The current occupant of that office, Michael Horowitz, has issued several important reports that triggered national debate about the FBI and resulted in major reforms. There is also an Intelligence Community Inspector General, whose office became embroiled in the firs impeachment of former President Donald Trump.[72]

Privacy and Civil Liberties Oversight Board

The 9/11 Commission recommended that there be "a board within the executive branch to oversee . . . the commitment the government makes to defend our civil liberties."[73] The Bush Administration established the bipartisan Privacy and Civil Liberties Oversight Board as part of the Executive Office of the President in 2004, shortly after the 9/11 Commission issued its final report. In 2007, Congress transformed the Board from a White House body into an independent agency within the Executive Branch.[74]

The Board consists of a full-time Chairman and four part-time members, all of whom must be nominated by the President and confirmed by the Senate. Its mission is to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties" and "ensure that liberty concerns are appropriately considered in the development and implementation" of relevant laws, regulations, and policies.[75]

The Board accomplishes this mission in two ways: by providing advice to executive agencies on programs in development and by conducting oversight of activities and polices within its jurisdiction.[76] PCLOB's advice and oversight are programmatic; unlike inspectors general, it does not typically examine individual cases of noncompliance or abuse.

Because the Board is part of the Executive Branch, it can advise agencies on non-final policies without vitiating privileges that protect agencies' pre-decisional deliberations. Yet the Board's statutory charter and bipartisan membership make it legally and functionally independent. Indeed, the Board's challenge has often been establishing sufficient trust with agencies to execute its advice function. That may be because the Board's oversight function, always hovering in the background, makes agencies wary of revealing too much.

Transparency is part of the Board's statutory mission. It is required to hold public hearings and "to make its reports . . . available to the public to the greatest extent that is consistent with the protection of classified information and applicable law."[77]

Over the years, the Board and individual Board Members have produced many public reports, though at sporadic intervals driven by frequent vacancies and the resulting struggles to maintain a quorum.

President's Intelligence Advisory Board

Historically, the President's Intelligence Advisory Board (known, until the George W. Bush presidency, as the President's *Foreign* Intelligence Advisory Board) was an important advisory body on intelligence matters. Part of the Executive Office of the President, PIAB members are appointed directly by the President, without Senate confirmation. The PIAB thus enjoys proximity to the President and the ability to serve as a trusted sounding board on the efficacy and utility of intelligence programs.

A sub-entity of the PIAB, the Intelligence Oversight Board, receives reports of noncompliance from the intelligence agencies, and is in theory expected "to oversee the Intelligence Community's compliance with the Constitution and all applicable laws, Executive Orders, and Presidential Directives." That may have been true in earlier eras. Today, however, the PCLOB, inspectors general, CLPOs, the congressional intelligence committees, and the FISA Court play a more active role than the IOB in identifying noncompliance and potential illegality.

The PIAB recently re-emerged from a long period of dormancy with an influential report on Section 702 of the Foreign Intelligence Surveillance Act.[78]

Data Protection Review Court

In 2022, President Biden issued Executive Order 14,086, "Enhancing Safeguards for United States Signals Intelligence Activities."[79] EO 14,086 replaced President Obama's Presidential Policy Directive 28, issued in the wake of the Snowden leaks to create protections for non-U.S. persons affected by U.S. surveillance.

Executive Order 14,086 established a new "signals intelligence redress mechanism" within the Executive Branch.

As part of the new mechanism, the order required the Attorney General to establish within the Department of Justice a "Data Protection Review Court" to review complaints from residents of "qualifying state[s]" alleging unlawful surveillance by U.S. agencies.[80] The order further orders "each element of the Intelligence Community" to accord "binding effect" to the DPRC's order.

The Department of Justice has issued implementing regulations to create the DRPC and designate the United Kingdom, the members of the European Union, and the members of the European Economic Area as "qualifying states."[81] As of this writing, the appointment of the first DPRC judges is believed to be imminent.

By creating the DPRC, the Biden Administration seeks to satisfy the European Union's longstanding demand for an independent mechanism to provide judicial redress for alleged unlawful surveillance. The previous solution, an "Ombudsperson" within the State Department, was a politically appointed official who could be terminated for cause. Providing judicial redress for speculative claims of illegal surveillance before an Article III court would run up against Article III "standing" doctrine, a constitutional requirement for a matter to constitute a justiciable "case" or "controversy" that can be heard in federal court.[82]

The DPRC is a clever substitute that provides binding, independent judgments without contravening Article III. Indeed, the DPRC arguably offers residents of "qualifying states" a simpler and more effective remedy than is available to similarly situated Americans.

Courts

The Foreign Intelligence Surveillance Court's principal role is to *authorize* surveillance, but it also has come to provide ex post oversight.

For Section 702, a degree of oversight is baked into the Court's statutory role. The Court is tasked each year with deciding whether the program as the government proposes to operate it complies with the Fourth Amendment.[83] That naturally prompts the Court to look back at whether those rules were effective in the past.

In "traditional" FISA, the Court's rules require the government to disclose any instances of noncompliance in activities the Court has authorized.[84] The Court then responds with remedial orders requiring the government to correct those errors.[85] The Court thus finds itself in the unusual position (for an American court) of conducting ongoing supervision of government activities, rather than simply issuing judgments in one-off disputes.

It is thus unsurprising that some litigants and scholars[86] have questioned whether the FISA Court's activities exceed the constitutional limits of the "judicial Power of the United States." Courts have thus far rejected Article III challenges to the FISA Court's structure.[87] On at least one occasion, however, the FISA Court of Review has rebuked the FISC for exceeding the boundaries of the judicial role in imposing detailed remedial schemes on the FBI and Department of Justice.[88]

V. PROCESS FOR CONDUCTING SURVEILLANCE

Who authorizes national security surveillance, and by what process, depends on the legal authority under which the surveillance is conducted. That, in turn, depends on the nationality of the targets and the location of both the targets and the collection, as the table below illustrates:

Nationality of Target	**Location of Target**	**Location of Collection**	**Legal Regime**
U.S. person	In the U.S.	In the U.S.	FISA Title I/III (probable cause required)
Non-U.S. person	In the U.S.	In the U.S.	FISA Title I/III (probable cause required)
Non-U.S. person	Outside the U.S.	In the U.S.	FISA 702 (probable cause not required, no individualized court order - EO 14,086 limits and remedies apply)
Non-U.S. person	Outside the U.S.	Outside the U.S.	EO 12,333 (no judicial role - EO 14,086 limits and remedies apply)
U.S. person	Outside the U.S.	Outside the U.S.	FISA 704 - FISC probable cause order required

"Traditional" FISA

Electronic surveillance and physical search of foreign powers and their agents in the United States are known as "traditional" FISA (to distinguish them from the more recent Section 702). In these cases, the FISA court reviews individualized filings in which the government must establish probable cause to believe that the target is a foreign power (which can include a terrorist group) or agent of a foreign power.[89]

The standard is slightly more lenient for non-U.S. persons.[90] They can be surveilled for being unwitting agents of a foreign powers, but U.S. persons must engage in the relevant conduct "knowingly."[91] The government's application must also specify the "facilities" (phone numbers, online accounts, etc.) that it will tap or search.

There is a similar individualized process for using FISA to deploy pen registers or trap-and-trace devices and obtain third-party business records (which can include metadata but not content). These provisions do not require a showing of probable cause, however; mere relevance suffices [92]

After 9/11, FISA's business-records provision was used to obtain call detail records in bulk from domestic telephone carriers.[93] The USA Freedom Act of 2015 now prohibits the use of these provisions for bulk collection.[94]

The maximum length of electronic surveillance depends on whether the target is a foreign power, an agent of a foreign power who is not a U.S. person, or a U.S. person.[95] The government can then seek to renew the surveillance for periods of time that similarly vary based on nationality.[96]

Renewals have come under scrutiny since the 2020 revelation that the misbegotten surveillance of onetime Trump aide Carter Page was renewed three times.[97] Subsequent oversight reviews have found that the process for renewing surveillance lacks sufficient focus and have proposed requiring additional, renewal-specific findings before surveillance can be renewe [98]

This "traditional" FISA process typically applies only to surveillance of people in the United States. However, there is one exception. If the government wishes to collect the content of the communications of a U.S. person outside the United States, or otherwise target a roaming American using a technique that would trigger the Fourth Amendment's warrant requirement if used at home, it must obtain an order from the FISA Court.[99]

The maximum length of electronic surveillance depends on whether the target is a foreign power, an agent of a foreign power who is not a U.S. person, or a U.S. person.

Does the FISA Court process provide rigorous scrutiny? The judges are the court's strongest feature: the life-tenured federal judges designated to serve on the FISC are insulated from political pressure and accustomed to grilling (and ruling against) government lawyers in their home courts. They are also familiar with the Fourth Amendment and criminal wiretaps from their work superintending criminal trials.

On the other hand, the process has in recent years produced some notorious whiffs. One example: the secret orders, revealed by Edward Snowden, that authorized bulk collection under a since-lapsed version of FISA's business-records authority.[100] More recently, the court approved and thrice renewed FISA surveillance of Carter Page based on the contrived "Steele dossier."[101] The government's applications also tend to be dense, repetitive, and poorly structured to facilitate critical analysis.[102]

In the wake of the Snowden disclosures, published data showed that the Court rejected only a small percentage of government surveillance applications. Defenders responded, however, that the statistics obscured the back-and-forth between the Court's professional legal advisers and government lawyers.[103] In their telling, those informal discussions often led to changes to the government's initial filing or persuaded the government to withdraw a potential filing altogether rather than risk rejection.[104]

Scrutiny appears to have grown more rigorous in recent years. Public reports now break out the number of orders that were "modified," "denied in part," and denied outright. This table, drawn from the Administrative Office of the U.S. Courts annual FISA report,[105] provides the numbers for 2022:

Section	Applications or Certifications	Orders Granted	Orders Modified	Orders Denied in Part	Applications or Certifications Denied
1805 only	41	30	7	3	1
1824 only	24	15	9	0	0
1805 and 1824*	259	176	64	13	6
1842	4	3	1	0	0
1861	10	6	5†	0	0
1881a	0	0	[redacted]‡	0	0
1881b	0	0	0	0	0
1881c	20	19	1	0	0

The first three rows correspond to orders seeking electronic surveillance, physical search (including compelled production of stored content), and both of those—the core, "traditional" FISA powers that require a finding of probable cause

Ultimately, however, what matters is not simply whether the Court rejects more applications, but whether its decisions are *correct* on the most consequential questions of law and fact. Strengthening the process to ensure critical scrutiny will raise the odds that the court gets key decisions right.[106]

Section 702

An individualized court order is not required to collect the communications of a *non-U.S. person* located *outside the United States*. Whether the FISA Court is involved at all depends on *where* the collection takes place.

If the collection takes place in the United States, Section 702 applies.[107] Once a year, the FISA Court approves the rules under which the Intelligence Community proposes to implement Section 702 and the operational purposes for which it plans to use the authority.

Once those are approved, however, targeting takes place within the Executive Branch without judicial review of individual targeting decisions.[108]

Declassified versions of statutorily required ta geting, minimization (i.e., storing, using, and sharing 702 data), and querying rules, which are specific to each of the agencies involved, are publicly available.[109] Recently, the Office of the Director of National Intelligence also declassified for the first time the approved se of categories of foreign intelligence information that agencies use 702 to obtain: "(1) foreign governments and related entities, (2) counterterrorism, and (3) combatting proliferation."[110]

Overseas Targeting of Non-U.S. Persons under Executive Order 12,333

Statutory authorization is not required for SIGINT collection conducted abroad on a foreign target.[111] Instead, targets are nominated and approved internally within the agency.

Yet such collection is still constrained by law and policy. Constraints include Executive Orders (12,333 and 14,086), Executive Branch legal opinions, and internal agency guidance. Agencies are also limited by their own organizing statutes (for example, the National Security Act's prohibition on "internal security" activities by the CIA) and by the priorities in the National Intelligence Priorities Framework. For overseas SIGINT targeting, such constraints are implemented by internal agency processes rather than judicial supervision.

VI. RELEVANT LAW

The sources of law governing U.S. surveillance have been described in detail elsewhere.[112] Instead of reproducing those details, this paper will attempt to sketch out, for those not steeped in U.S. public law, how different bodies of law structure, authorize, and regulate the U.S. government's use of electronic surveillance to collect intelligence.

The Constitution

In the American system of government, every exercise of federal power must have a basis in the Constitution. That document does not explicitly address national security surveillance, nor even intelligence. Nonetheless, it contains many provisions that bear upon those fields

Article I of the Constitution discusses the Congress. Relevant here are various powers related to national defense:

- The power to tax and spend to "provide for the common Defence,"[113]
- The power to create and fund military forces and make rules for their governance,[114]
- The exclusive power to appropriate funds from the Treasury,[115] and
- The power to "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof. [116]

Article II also gives the Senate important roles in approving treaties and confirming nominees for senior Executive Branch positions.[117]

The President's constitutional powers have been interpreted to confer broad powers over foreign affairs and diplomacy.[118]

They include:

- The Executive Vesting Clause, which provides that the "executive Power shall be vested in a President of the United States of America,"
- The President's constitutional role as "Commander in Chief of the Army and Navy of the United States"
- The power, "by and with the Advice and Consent of the Senate, to make Treaties,"
- The power to appoint "Officers of the United States and many other Executive Branch employees,
- The power to "receive Ambassadors and other public Ministers," which has been interpreted, in concert with related presidential powers, to confer the power of diplomatic recognition,[119] and
- The duty to "take Care that the Laws be faithfully executed."

The Constitution also requires the President to swear an oath to "preserve, protect and defend the Constitution of the United States."[120]

Finally, "the judicial Power of the United States" is vested in the Supreme Court and "such inferior Courts" as Congress chooses to establish. The judicial power, however, extends only to enumerated categories of "cases" and "controversies." Those terms have been interpreted as precluding nonbinding "advisory opinions," requiring genuine adverseness between the parties to litigation, and excluding plaintiffs who lack a concrete, personal, redressable injury that is fairly traceable to the defendant's conduct, and who thus lack "standing" to sue.[121]

One interesting, unanswered question is whether the President has inherent power to authorize surveillance for foreign-intelligence purposes. If so, can Presidents authorize domestic surveillance outside of FISA's constraints during a national security crisis?

The Bush Administration asserted such a power after September 11th. Its "STELLARWIND" surveillance program operated for several years on the basis of asserted presidential authority, without adhering to FISA's requirements for electronic surveillance conducted in the United States.[122] The legal theory behind STELLARWIND was never tested in court, however.

Finally, some amendments to the Constitution are relevant to surveillance. Most important is the Fourth Amendment, which bars "unreasonable" searches and seizures and sets out the requirements for warrants.[123] The Supreme Court has held that warrantless searches are presumptively unreasonable and that wiretapping constitutes a "search."[124] Collection of telephone metadata, however, does not.[125] Lower courts have also held that access to the contents of email messages constitutes a Fourth Amendment search, even if the messages are in the custody of a third party (such as an electronic communications service provider or ISP).[126]

Criminal defendants surveilled in violation of the Fourth Amendment can move to suppress the illegal surveillance and other evidence derived from it. The Foreign Intelligence Surveillance Court of Review has held that there is a "foreign intelligence" exception to the warrant requirement; the Supreme Court has not yet addressed that question, however.[127]

The First Amendment, which protects freedom of speech and the press, often lurks in the background of surveillance-related controversies. Surveillance, after all, can be used to suppress or indirectly chill dissent. The Supreme Court has thus acknowledged the unique "convergence of First and Fourth Amendment" present when the government monitors its citizens to protect national security, rather than prosecute ordinary crime.[128] Despite this acknowledgment, however, "judicial application of the First Amendment to state surveillance demands has generally been narrow."[129] One possible reason: it is difficult to formulate a judicially administrable standard for deciding when broad surveillance programs that do not specifically target speech, the press, or association go so far as to inhibit First Amendment rights.

Statutes

Relevant statutes fall into two categories: those that authorize and structure the relevant agencies, and those that permit and prohibit various forms of agency action.

In the former category are statutes ranging from the venerable National Security Act of 1947 and CIA Act of 1949, which create and structure to the CIA,[130] to the more-recent Intelligence Reform and Terrorism Prevention Act of 2004, which created the Director of National Intelligence and National Counterterrorism Center.[131]

In the latter category, the most notable example is FISA, which sets forth a detailed system for conducting foreign-intelligence surveillance and requests for stored data in the United States and for surveillance of U.S. persons abroad. Similarly, the Electronic Communications Privacy Act sets for the process for intercepting communications and obtaining stored data in criminal investigations.[132]

> ***One interesting, unanswered question is whether the President has inherent power to authorize surveillance for foreign-intelligence purposes. If so, can Presidents authorize domestic surveillance outside of FISA's constraints during a national security crisis?***

Executive Orders

Many U.S. intelligence programs, including virtually all overseas SIGINT activities, are conducted under presidential authority rather a statute.

Executive orders are "directives issued by the President of the United States."[133] They "are generally directed to, and govern actions by, Government officials and agencies" rather than private citizens.[134]

The most important executive order related to surveillance is Executive Order 12,333. As the Privacy and Civil Liberties Oversight Board explained in its capstone report on EO 12,333:

> EO 12,333 contains three parts. Part 1 establishes the goals of U.S. intelligence and assigns roles and responsibilities to the entities that comprise the IC. . . . Part 2 of the Order explains the need for foreign intelligence information and establishes principles that balance that need with the protection of the rights of U.S. persons. It specifically requires IC elements to adopt certain procedures for the collection, retention, and dissemination of information concerning U.S. persons and the use of specific collection techniques. . . . Part 3 addresses oversight, instructs intelligence agencies on how to implement the Order, and defines certain terms [135]

For example, Part 1 instructs the National Security Agency to (among other missions) "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions."[136] It further designates the NSA as the Intelligence Community's "[f]unctional [m]anager" for signals intelligence.[137]

Part 2 of EO 12,333 contains rules to protect privacy and civil liberties. Section 2.3 limits the types of information concerning United States persons that IC agencies are permitted to collect, retain, and disseminate, and requires that U.S.-persons' data be handled in accordance with agency-specific procedures approved by the Attorney General. Those procedures, which are themselves an important legal guardrail, are discussed further below.

Part 2 also contains several exotic prohibitions that address specific instances of misconduct revealed in the 1970s by the Church Committee.[138] These include bans on unconsented human experimentation, assassination, inducing others to undertake activities that the intelligence community is barred from conducting directly ("indirect participation"), and covert action intended to influence domestic audiences. It also restricts clandestine participation by intelligence community employees in domestic organizations.[139]

President Biden's EO 14,086 adds significant new constraints to those in EO 12,333. Many of these constraints are carried over from President Obama's Presidential Policy Directive 28, issued in the wake of the Snowden leaks to mollify critics abroad.

Most notably, EO 14,086:

- Adopts the requirements, imported from European human-rights law, that SIGINT collection be "necessary" and "proportionate" (as opposed to simply lawful and potentially useful)
- Limits SIGINT collection to specific, enumerate objectives
- Bans other objectives, such "collect[ing] foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially"
- Requires SIGINT activities to be "as tailored as feasible"
- Restricts bulk collection to an even narrower set of six permissible objectives
- Subjects the collection, retention, and dissemination of non-U.S. persons' data collected via SIGINT to protections comparable to those provided to U.S. persons.
- Creates a "signals intelligence redress mechanism," described above, for residents of "qualifying states" designated by the Attorney General.

Agency Policies or Guidance Documents

Below the level of Executive Orders, internal agency documents provide more detailed rules applicable to each agency's unique missions and internal structures.

Among the most elevated such documents—because they cannot be changed without approval by the Attorney General—are each IC agency's Attorney-General-approved guidelines for collecting, retaining, and disseminating the data of U.S. persons. These are required by Section 2.3 of Executive Order 12,333 and are publicly available with modest redactions.[140] Because these guidelines are specific to each agenc , they are often the most relevant, on-point source of law for agency lawyers analyzing proposed actions.

The statutorily required minimization, targeting, and querying procedures for FISA 702 collection must be approved annually by the FISA Court. They are also public, with limited redactions.[141]

Other internal agency procedures provide further restrict how agency employees perform their missions.[142]

Legal Compliance in Practice

Legal constraints are not self-executing. In the day-to-day hustle of intelligence collection, compliance depends on the institutional structures that surround the operators and help them find lawful ways to achieve their goals.

These constraints include internal and external oversight and compliance bodies. They also include technical mechanisms, like audit and logging systems, as well as lawyers deployed in operational units to provide real-time guidance to operators. Finally, intangibles like a "culture of compliance" both support and are shaped by these other, formal controls.

Along each of these dimensions, some agencies are stronger than others. In the author's experience, NSA has a solid compliance architecture and sophisticated technical systems in place to ensure that analysts' use of data complies with the rules. NSA is not perfect of course; some mistakes are inevitable in any large, human enterprise engaged in complex work.[143] Still, NSA's technical compliance architecture and institutional mechanisms supply a promising model for other agencies.

The FBI, by contrast, has struggled to develop an effective compliance system. Queries of 702 databases, for example, are not audited in near-real-time by experts familiar with the analyst's mission, as at NSA. Instead, Justice Department lawyers must travel to FBI field offices to review past querie [144] In fairness to the Bureau, its decentralized structure and unwieldy legacy IT systems make building a modern, tech-enabled compliance architecture a formidable bureaucratic challenge.

VII. TRANSPARENCY

There is considerable public information available about U.S. surveillance programs. Some of this emerged lawfully, though authorized transparency initiatives. But much has emerged through leaks, which continue to bedevil intelligence community leaders.

Official Transparency Efforts

The fundamental legal architecture for U.S. national security surveillance is public, from statutes and executive orders down to agency implementing procedures.[145] These legal instruments delineate whom the government can surveil, which officials or agencies are responsible, and what conditions apply.

Since the shock of the Snowden disclosures, the government has also provided significant transparency about how these programs are implemented.

One of the most useful resources is the Intelligence Community's Annual Statistical Transparency Report.[146] Its detailed statistics and explanations give the reader a general sense of the scale of U.S. collection programs.

For example, the report shows the great size of FISA Section 702 collection against foreign targets compared to "traditional" FISA collection on people in the United States. In 2022, it reveals, there were only 417 total targets of traditional, court-approved, individualized FISA orders, and only 11% of those were Americans. By contrast, the U.S. government targeted 246,073 non-U.S. persons overseas under FISA 702.

Congress apparently finds these statistical reports useful as well. It has periodically required the Director of National Intelligence to add additional categories to the report.[147]

The Administrative Office of the U.S. Courts also issues its own annual statistical report on the activities of the Foreign Intelligence Surveillance Court.[148] That report breaks out the numbers of orders denied and modified and the number of and the Court s use of the statute's amicus provision.

The USA Freedom Act of 2015, enacted in response to the Snowden leaks, made various enhancements to transparency practices.[149] Most notably, it:

- Required the DNI to release to the public, to the extent consistent with national security, past and future FISA Court decisions in cases presenting significant or novel issues [150]
- Allowed private companies to provide the public with more detail about the volume of surveillance orders they receive.[151]
- Added certain required categories to the annual statistical reports issued by Office of the Director o National Intelligence and the Administrative Offic of the Courts.[152]

Routine declassification of important FIS Court opinions has added greatly to experts' understanding of the ongoing dialogue between the Court and the intelligence agencies about the agencies' compliance with applicable rules. For example, after an inspector general report revealed the serial errors and omissions in the Carter Page FISA applications, the FISC issued a series of remedial orders scolding the Justice Department and requiring new safeguards.[153] These opinions were then made public in redacted form.

Similarly, each year the Office of the Director of National Intelligence redacts and then releases the FISC's opinion on the annual certifications submitted by the government to operate the Section 702 program.[154]

The Limits of Transparency

If there is a catch, it is this: transparency can only ever be partial in intelligence matters. The deep secrecy that remains the norm carries with it the potential for unwelcome surprises. People operating deep in the bureaucracy, even assuming the best of intentions, typically lack critical distance from their own work. And their work, by its nature, is insulated from scrutiny by people outside the national security enterprise.

It is in this regard that such independent voices as the PCLOB and FISA amici can be most helpful. These outsiders bring fresh views, independent thinking, and critical distance to secret programs and legal interpretations that would otherwise receive none.

Even these cleared observers, of course, must find their way to the key questions through the shadowy byways of the classified world. And the sheer scale of the U.S. intelligence enterprise—the many (perhaps uncounted) compartmented programs, the archipelago of secret facilities, the dozens of agencies and hundreds of thousands of people involved—make it impossible, as a practical matter, for anyone to take stock of everything. Still, the existence of independent, cleared reviewers able to peer into the system at least improves the odds that *someone* will cast an independent eye on the most consequential programs.

> ***If there is a catch, it is this: transparency can only ever be partial in intelligence matters. The deep secrecy that remains the norm carries with it the potential for unwelcome surprises.***

Whistleblowers?

In theory, whistleblowers are the ultimate pressure valve in the system. But who is a whistleblower?

U.S. law offers strong protections to those entrusted with classified information who have followed the approved process for reporting waste, fraud, abuse, or illegality to inspectors general or Congress.[155] Those protections extend to contractors as well.[156]

The law does *not*, however, protect intelligence community employees or contractors who, like Edward Snowden, illegally remove classified material from their workplaces and provide it to journalists or other uncleared people. Quite the contrary: They can be charged under the Espionage Act with willfully providing nation-defense information "to any person not entitled to receive it."[157] Nor, despite calls from civil liberties activists, does the law allow such leakers to mount a defense based on the public interest in their disclosures.[158]

The U.S. intelligence apparatus, for all its strengths in other areas, has proven quite poor at preventing leaks of classified information. The Snowden and Manning leaks appear to have been leading indicators of an emerging trend. One possible cause is the ongoing generational shift in the intelligence community workforce and the intense engagement of new, younger employees in online communities beyond the awareness of their security officers. Air Force National Guardsman Jack Teixeira, for instance, appears to have removed and posted online highly sensitive classified briefing documents to win credibility in an online gaming forum.[159]

VIII. REFORMS

U.S. intelligence law has historically been shaped by moments of searing crisis that birthed major reforms.[160] Yet the prevalence of "sunset clauses" in post-9/11 legislation has changed this somewhat, bringing surveillance topics to the public's awareness at more frequent intervals.

Cycles of Crisis and Reform

The modern national security state emerged in the crucible of the early Cold War. Things then continued much as they were until the 1970s, with Congress often expressing little interest in intelligence.[161]

Everything changed in the mid-1970s, after the Watergate scandal brought down President Nixon and exposed many dark recesses of government. Subsequent investigations by the congressional Church and Pike Committees revealed widespread abuses of intelligence powers.[162] Those disclosures led to FISA and the congressional intelligence committees, twin pillars of the system of law and oversight described in this essay.

The terrorist attacks of September 11, 2001, delivered a violent shock that pushed things in the direction of greater powers for security agencies. In its celebrated final report, the 9/ 1 Commission concluded that underinvestment in intelligence collection and fragmentation in the intelligence community had allowed the eventual hijackers to evade detection.

To remedy that, the Commission recommended greater concentration of information and authority: a new Director of National Intelligence, a National Counterterrorism Center, and an integrated information-sharing environment within the Intelligence Community.[163] The result was more collection, more synthesis of that information, and more sharing within and outside of the federal government.

Simultaneously, the rapid digitization of global telecommunications and many sectors of the economy dramatically expanded the field for SIGIN agencies. Prized intelligence could be found in the stream of traffic across global digital networks and extracted at little cost or risk compared with other techniques—if agencies had access to those networks and the know-how and resources to find the nuggets. The collection now conducted under Section 702 is a response to this epochal shift in how modern societies (and thus how intelligence targets) communicate.

Snowden provided the next major jolt. Though his leaks did not reveal any intentional lawbreaking, they did show an oversight system that had failed to prevent a major, legally dubious intrusion into Americans' privacy: the bulk collection of telephone call detail records. They also alerted people around the globe to the potential scale and intrusiveness of digital surveillance in the internet age.

Sunsets

"Sunset" clauses have, to some extent, decoupled surveillance legislation from the vicissitudes of events. Sunset clauses are simply expiration dates for all or some provisions of a statute. After 9/11, Congress began to incorporate such clauses into legislation conferring new surveillance powers.

Several provisions of the USA Patriot Act of 2001, for example, were given a five-year sunset [164] This included the newly expanded "business records" provision of FISA, which empowered the government to obtain a much broader class of "tangible things" from third parties in investigations of international terrorism.[165] Similarly, when Section 702 was enacted in 2008, Congress included a four-year sunset.[166]

These sunsets have the practical effect of granting opponents of surveillance programs considerable leverage when these programs are set to expire. Because of sunsets, debate over surveillance reforms has become a regular feature of American lawmaking rather than a once-in-a-generation rarity.

FISA Business Records

In 2015, civil libertarians used the leverage provided by a sunset of certain Patriot Act provisions to secure the reforms in the USA Freedom Act.[167] The USA Freedom Act extended those Patriot Act authorities, with significant modifications, for another four year [168] The next time around, however the politics of surveillance had shifted again,[169] and Congress was ultimately unable to agree on a reauthorization deal. Those Patriot Act provisions thus lapsed in 2020, ending some powers altogether and returning others to their more limited, pre-9/11 scope.[170]

Section 702

Section 702's existence has also been shaped by sunset clauses. Congress reauthorized it the first time around, in 2012, by wide margins.[171] The next reauthorization was far from smooth, however. At a critical moment, a presidential tweet nearly scuttled reauthorization, which the Trump administration had previously endorsed.[172] Rather than the "clean" reauthorization they had sought, the intelligence community was forced to concede some (albeit modest) reforms to garner the needed votes.

The 2018 reauthorization extended Section 702 until December 31, 2023. As of this writing, Congress faces an even more difficult reauthorization fight, at a tim when its capacity to deal with complex legislation is at a low ebb.

The key factor this time around is intense skepticism among Republicans, whose confidence in the FBI is at an all-time low after the Bureau misused FISA to monitor former Trump campaign aide Carter Page in 2016. Other controversies, including hotly contested investigations of former President Trump and Hunter Biden, have amped up the polarization around the FBI and Justice Department.

At present, the likeliest outcome is that Congress will renew Section 702 with some reforms, rather than allowing it to lapse. Agencies have made a compelling case that Section 702 is a vital tool for addressing contemporary national security challenges, ranging from the People's Republic of China to deadly fentanyl trafficking

It remains unclear, however, which package of reforms can unite enough votes around a reauthorization deal. As in the past, energy on the progressive left has focused on requiring a warrant or warrant-like court order before searching 702 databases for information about Americans.[173] Republicans, however, are animated more by concerns about political and ideological weaponization of government power and would likely expect a reform package to address the instances of misconduct from the 2016 campaign.[174] Other issues, like government-induced censorship of social media,[175] have also undermined trust in security agencies.

IX. OTHER IMPORTANT FACTORS

The American approach to electronic surveillance and SIGINT is heavily influenced by the United States unique geopolitical circumstances.

Global Alliance Commitments

The United States stands alone in the breadth and depth of its global security commitments. The United States is committed to the defense of the (as of this writing) 31 member states of NATO, many of which border Russia. As of 2022, more than 100,000 U.S. service members were stationed in Europe to back that pledge with steel.[176]

The United States has pledged to defend many allies in Asia and the Pacific: most prominentl , Japan, South Korea, Australia, New Zealand, the Philippines, and Thailand.[177] U.S. service members are stationed in their tens of thousands at bases across East Asia. Today, those bases lie within range of thousands of conventional ballistic missiles being readied by China's People's Liberation Army Rocket Force.

American defense commitments to these countries extend to the use of nuclear weapons.[178] Technologically sophisticated but vulnerable frontline countries like Japan and South Korea forbear from producing their own nuclear weapons on the understanding that the U.S. nuclear umbrella deters their adversaries. Of course, keeping this pledge *in extremis* would expose the American homeland to massive retaliation.

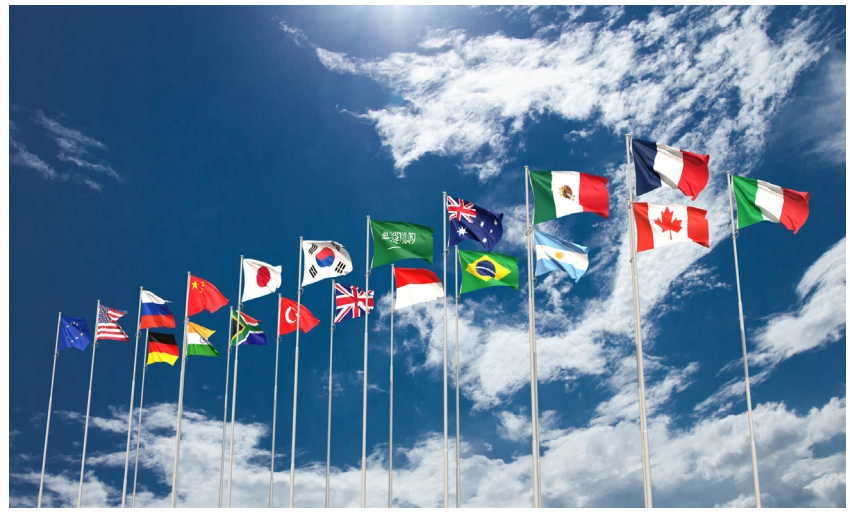
Other, less formal commitments also exert their pull. In the Middle East, U.S. interests are powerfully entwined with the security of Israel, Saudi Arabia and other Gulf monarchies, and Egypt.

The result: Iran must be watched and checked.

Perhaps the most important commitment, ironically, is barely a commitment at all: Taiwan. The Taiwan Relations Act is hardly clear: it declares that it is "the policy of the United States" to "maintain the capacity of the United States to resist any resort to force or other forms of coercion that would jeopardize the security, or the social or economic system, of the people on Taiwan."

Yet that ambiguous pledge of U.S. credibility, when coupled with sympathy for Taiwan's democratic experiment and the strategic interest in keeping the island out of PRC hands, makes it likely that the United States would defend Taiwan from what would be a fearsome invasion force.[179] And if that is so, it is equally likely that China would strike first at the U.S. bases in the Pacific that would enable such a defense. Tellingly, the PLA Rocket Force trains on mockups of U.S. aircraft carriers and bases in Japan.[180]

This global web of bases and defense commitments means that the American President rises each day to face a world of complexity, vulnerability, and risk.



Managing that risk drives constant, profound intelligence requirements. For each adversary, intelligence agencies must be prepared to provide the President and military leaders with "warning"[181] of tactical and strategic developments that threaten not just the U.S. homeland, but dozens of treaty allies around the world.

Is China preparing to invade Taiwan? Is Russia preparing cyberattacks against energy infrastructure in NATO countries? Are terrorists plotting to sneak sleeper cells into Western Europe? In each case, only prevention counts as success. And prevention requires insight that often can be obtained only through clandestine means.

What would happen if NSA dramatically curtailed its collection against overseas targets? U.S. policymakers would have far less insight into adversaries' capabilities and plans, raising the risk of tactical and strategic "surprise," and thus defeat.

American Presidents, U.S. military planners, and allies reliant on U.S. protection would be less confident in our ability to anticipate, deter, or frustrate adversaries' moves. U.S. defense commitments would be less credible. Americans would be asked to take on more risk to protect distant allies. Would they?

U.S. allies might disagree with this framing. Why can't you commit not to spy on us, they might argue, while continuing to spy on our mutual adversaries? (Tellingly, *intelligence* officials in allied countries rarely ask such questions.)[182]

The reason is that allies also bring risks. Indeed, alliance commitments can be quite dangerous for the *stronger* party: weaker nations may be tempted to act provocatively if they enjoy the protection of a global superpower. When the stakes are nuclear, American willingness to retain these commitments depends on confidence that those dangers can be mitigated.

Another concern is that allies can be unpredictable. NATO ally Turkey bought Russian S-400 air-defense systems and has zigged and zagged unpredictably in its regional policies.[183] German Chancellor Gerhard Schröder left the Chancellery in 2005 and, head still full of government secrets and NATO plans, quickly accepted a lucrative sinecure from the Russian Nord Stream pipeline consortium.[184] A "no-spy" agreement of the type sought, for example, by German politicians after the Snowden leaks, would presuppose near-lockstep alignment on foreign, defense, and security policy, as exists within the Five Eyes.[185]

Diversity of Threats

U.S. intelligence collection underwrites American and multilateral responses to the world's most pressing security threats and transnational challenges.

In Ukraine, the U.S. intelligence community is providing direct support to Ukrainian forces. We can infer from Ukrainian successes in precision targeting that the scale of this assistance is vast and probably unprecedented. U.S. officials have also disclosed that information from FISA Section 702 has also helped detect and document atrocities by Russian forces. Russian leadership machinations must be analyzed, potential escalations forecast, sanctions-dodging sniffed out. U.S. intelligence agencies, working together with allied services, provide indispensable insight on each of those aspects of the conflict

Alongside the threat of a Chinese invasion of Taiwan, the People's Republic and the United States are engaged in a comprehensive technology competition. Both countries are racing to occupy the high ground in such strategic technologies as quantum computing, cutting-edge semiconductors, AI, hypersonics, autonomous systems, and space. In chips, for example, the United States has deployed export controls aimed at keeping U.S. technology durably in front of China. The PRC, for its part, will use any means, open or clandestine, to gain technology and know-how in these critical areas. Intelligence is vital to closing off access to controlled technologies.

The list of potential intelligence priorities seems endless: Iran, North Korea, terrorism, coups and Wagner mercenaries in West Africa, the origins of COVID-19, drug cartels and fentanyl smuggling, transnational repression of dissidents, and many more.

At home, the United States' diversified, technologically advanced economy and open society combine to present an inviting attack surface for foreign espionage. Using our own intelligence collection to detect foreign services' moves before they happen is the best form of defense.

Polarization and Mistrust

Yet even as Ukraine demonstrates the U.S. intelligence community's prowess, agencies have struggled to maintain support at home.

Views of intelligence and law-enforcement agencies are increasingly polarized along partisan lines.[186] After high-profile revelations of FBI misconduct and years of feuding between former President Trump and prominent intelligence officials, Republicans' elf-reported confidence in intelligence services is at a historically low ebb.

During the George W. Bush years, Republicans voted overwhelmingly in favor of counterterrorism programs; today, Republicans in Congress are deeply split on FISA 702 and other intelligence powers.

Intense political polarization makes this a perilous moment for U.S. intelligence. Agencies cannot endure without the legal authorities and funding on which their work depends. Both of those, in turn, depend on Congress, and thus on broad public support. Only an ironclad culture of credible, apolitical professionalism can keep the agencies out of dangerous partisan currents.

ENDNOTES

1. *See,* e.g., Privacy Shield Framework, 81 Fed. Reg. 51041 (Aug. 2, 2016), https://www.federalregister.gov/documents/2016/08/02/2016-17961/privacy-shield-framework; Commission Implementing Decision of Oct. 7, 2023, C(2023), 4745 final, at 130, Ann. VII *et seq*., https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.
2. *U.S. Intelligence Community Budget*, Office of the Director of National Intelligence, https://www.dni.gov/index.php/what-we-do/ic-budget (last visited Oct. 11, 2023).
3. National Commission on Terrorist Attacks Upon the United States, Final Report 416 (July 22, 2004), available at https://www.9-11commission.gov/report/911Report.pdf [hereinafter "9/11 Commission Report"].
4. Implementing Recommendations of the 9/11 Commission Act of 2007, 50 U.S.C. § 515(c), Pub. L. No. 110-53, § 601, 121 Stat. 265, 335 (2007).
5. Julia Voo, Irfan Hemani, & Daniel Cassidy, *National Cyber Power Index 2022*, Belfer Center, Report (Sept. 2022), https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.
6. British-U.S. Communication Intelligence Agreement, 5 March 1946, https://media.defense.gov/2021/Jul/15/2002763709/-1/-1/0/AGREEMENT_OUTLINE_5MAR46.PDF (approved for release by NSA on Aug. 11, 2014, MDR Case #78775).
7. Richard Aldrich, *Allied code-breakers co-operate – but not always*, The Guardian (24 June 2010), https://www.theguardian.com/world/2010/jun/24/intelligence-sharing-codebreakers-agreement-ukusa.
8. National Security Act of 1947, 61 Stat. 496 (1947) (as amended through Pub. L. No. 117-328, enacted Dec. 29, 2022).
9. *Id*. at § 104A(c)–(d) ("perform such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct") (codified at 50 U.S.C. § 3036).
10. *Id.* at § 104A(d)(1).
11. Exec. Order No. 12,333, § 1.3(b)(12)(A)(i).
12. *Frequently Asked Questions (FAQs)*, NSA/CSS, https://www.nsa.gov/about/faqs/sigint-faqs/ (last visited Oct. 11, 2023).
13. *See, e.g., 2021: NSA Cybersecurity Year in Review,* NSA (2021), https://media.defense.gov/2022/Feb/03/2002932462/-1/-1/0/2021_NSA_CYBERSECURITY_YEAR_IN_REVIEW.PDF.
14. *The Many Lives of Herbert O. Yardley,* NSA, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/many_lives.pdf; A Historical Note on the Closing of the Black Chamber, available at https://media.defense.gov/2021/Jul/21/2002807351/-1/-1/0/19510319_PRENSA_DOC_3978470_BLACKCHAMBER.PDF.
15. *The Many Lives of Herbert O. Yardley,* NSA, at 10.
16. President Harry S. Truman, *Communications Intelligence Activities, Memo for Sec. of State & Sec. of Defense* (Oct. 24, 1952), available at https://media.defense.gov/2021/Jul/20/2002806255/-1/-1/0/19521024_1950_DOC_3978766_COMMS.PDF.
17. Intelligence Community Directive 204, Director of National Intelligence (2021), https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf; *see also National Security Memorandum on The President's Intelligence Priorities,* White House (July 12, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/12/national-security-memorandum-on-the-presidents-intelligence-priorities/.
18. *Annual Threat Assessment of the U.S. Intelligence Community,* Office of the Director of National Intelligence (Feb. 6, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
19. David Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 4:3 (April 2023).
20. *Section 702 Overview,* Office of the Director of National Intelligence, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf (last visited Oct. 11, 2023).
21. *See, e.g., infra* notes 170-172 and accompanying text.
22. *The Attorney General's Guidelines for Domestic FBI Operations*, U.S. Attorney General (2008), at 6–9, https://www.justice.gov/archive/opa/docs/guidelines.pdf.
23. *Id.* at 8 (defining foreign intelligence to mean information that relates "to the capabilities, intentions, or activities of foreign governments . . ., foreign organizations or foreign persons, or international terrorists").
24. *See* 9/11 Commission Report, supra note 3, at 254–77.
25. *See, e.g., In re Sealed Case,* 310 F.3d 717, 732-36 (FISCR 2002) (FISA, as amended after 9/11 by the PATRIOT Act, permits the FISA Court to approve FISA surveillance if "the government entertains a realistic option of dealing with the agent other than through criminal prosecution").
26. *E.g.,* William E. Odom, *Break Up the FBI,* WSJ (June 12, 2002); Richard A. Posner, *We Need Our Own MI5,* Wash. Post (Aug. 15, 2006); Duncan Deville, *How to Split Up the Bipolar F.B.I*., N.Y. Times (June 18, 2002).
27. 9/11 Commission Report, *supra* note 3, at 78; The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States,* March 31, 2005, at 452, https://www.govinfo.gov/content/pkg/GPO-WMD/pdf/GPO-WMD.pdf ("The FBI has spent the past three and a half years building the beginnings of an intelligence service and striving to transform itself into a hybrid law enforcement and intelligence agency.").
28. Joe Popularis, *It's Long Past Time For Congress To Break Up The FBI,* The Federalist (May 23, 2022), https://thefederalist.com/2022/05/23/its-long-past-time-for-congress-to-break-up-the-fbi/.
29. *See*18 U.S.C. §§ 2510–13.
30. *See* 18 U.S.C. § 2703.
31. *See* Fed R. Crim. Pro. 41; *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010).
32. *See* 50 U.S.C. § 1801(f) ; 50 U.S.C. § 1821(5).
33. Report, *National Security Letters in Foreign Intelligence Investigations: Legal Background, CRS* (July 30, 2015), available at https://crsreports.congress.gov/product/pdf/RL/RL33320.
34. USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, Title V (June 2, 2015).
35. *Id.*
36. *See* Glenn S. Gerstell, *How FBI Querying Under FISA Section 702 Works*, Lawfare (July 10, 2023), https://www.lawfaremedia.org/article/how-fbi-querying-under-fisa-section-702-works.
37. *See* Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Sept. 28, 2023), Priv. & Civ. Liberties Oversight Bd., at B-14, available at https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf (FBI receives "information collected by the NSA only from targets who are relevant to predicated national security investigations—which in 2022 was approximately 3.2 percent of the total number of Section 702 targets, or about 8,000 of them.").
38. Rule 41was revised in 2016 to reflect that the government often does not know where the computers to be digitally searched or seized are located because they use technical means to obscure their locations. See Committee Notes on Rules–2016 Amendment ("First, subparagraph (b)(6)(A) provides authority to issue

a warrant to use remote access within or outside that district when the district in which the media or information is located is not known because of the use of technology such as anonymizing software.").
39. *See* Exec. Order No. 12,333 § 2.4(a).
40. *See*, Brian Katz, *The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection*, Center for Strategic and International Studies (July 13, 2020), at 4, available at https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.
41. Mark Hosenball, *CIA to make sweeping changes, focus more on cyber ops: agency chief*, Reuters (March 6, 2015), https://www.reuters.com/article/us-usa-cia/cia-to-make-sweeping-changes-focus-more-on-cyber-ops-agency-chief-idUSKBN0M223920150306.
42. U.S. Attorney's Office, *Statement Of U.S. Attorney Damian Williams On The Espionage Conviction Of Ex-CIA Programmer Joshua Adam Schulte*, Press Release (July 13, 2022), https://www.justice.gov/usao-sdny/pr/statement-us-attorney-damian-williams-espionage-conviction-ex-cia-programmer-joshua.
43. Philipp Wittrock, *Berlin Risks Spat with Switzerland over Tax Evaders*, Spigel International (Feb. 2, 2010), https://www.spiegel.de/international/germany/data-dilemma-berlin-risks-spat-with-switzerland-over-tax-evaders-a-675371.html ("In 2007, the Bundesnachrichtendienst (BND), Germany's foreign intelligence agency, paid a thief about €5 million for stolen data that included evidence of tax evasion by German citizens in the tiny Alpine principality of Liechtenstein.").
44. *See, e.g., Report and Recommendations on CIA Counterterrorism Activities Conducted Pursuant to E.O. 12,333*, U.S. Priv. & Civ. Liberties Oversight Bd., https://documents.pclob.gov/prod/Documents/OversightReport/f01950e2-75ff-4fb4-9b2e-9e7d6937ae3a/PCLOB%20Report%20on%20CIA%20Activities%20-%20508,%20Mar%2022,%202022%201305.pdf (Feb. 10, 2022); *Recommendations from PCLOB Staff*, Priv. & Civ. Liberties Oversight Bd. (released Feb. 10, 2022), https://documents.pclob.gov/prod/Documents/OversightReport/3e1012b2-15fe-43df-a3eb-4bb4b22320f0/PCLOB%20Staff%20Recommendations%20Regarding%20CIA%20Activity%20-%20508,%20Mar%2011,%202022%201015.pdf.
45. *Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program*, Priv. & Civ. Liberties Oversight Bd. (Nov. 19, 2020), https://documents.pclob.gov/prod/Documents/Projects/96bd2a55-ea48-4426-8b5f-06571ce7c357/TFTP%20Chairman%20Statement%2011_19_20.pdf.
46. Exec. Order No. 12,333 §§ 1.3(a), (b)(1), (6), (16).
47. Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency Under Section 2.3 of Executive Order 12,333 (Raw SIGINT Availability Procedures), ODNI/IMD/rwt, (Jan. 3, 2017), https://www.documentcloud.org/documents/3283349-Raw-12,333-surveillance-sharing-guidelines.html.
48. *Strategic Plan to Advance Cloud Computing in the Intelligence Community,* ODNI (June 26, 2019), https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf.
49. *See* 9/11 Commission Report, supra note 3, at 416–19; *see also id.* at 355–56 (missed opportunities to uncover 9/11 plot by connecting fragments of intelligence).
50. John Bash, *Requests for U.S. Person Identities in Intelligence Reports During the 2016 Presidential-Election Period and the Ensuing Presidential-Transition Period, Report for the Attorney General* (Sept. 2020), https://www.justice.gov/oip/foia-library/foia-processed/general_topics/bash_unmasking_report_05_31_22/download.
51. *Gates Procedures,* ICD 112 (Jan. 2017), Annex A, https://www.dni.gov/files/documents/71017/ES-2017-00045-DNI-Signed-Annex-Gates_Jan-2017_.pdf.
52. As will be discussed below, for Section 702, that preapproval is programmatic rather than individualized.
53. "Article III" in this context denotes judges who possess the constitutionally mandated attributes for exercising the "judicial Power of the United States" under Article III of the Constitution. Article III judges must be appointed by the President with the advice and consent of the Senate. They "hold their Offices during good Behaviour" (i.e., they have life tenure, unless they are impeached and removed by Congress) and their pay "cannot be diminished during their Continuance in Office." U.S. Const. Art. III. This distinguishes them from other adjudicators, such as federal magistrate judges and administrative law judges, who hold judicial or quasi-judicial offices that do not have these features.
54. 50 U.S.C. § 1803(a)(1).
55. The court always had discretion to appoint amici on an ad hoc basis, but the post-Snowden USA Freedom Act of 2015 required the Court to maintain a formal, structured amicus panel. Pub. L. No. 114-23, § 401, 129 Stat. 268, 279 (June 2, 2015).
56. *See Amici Curiae*, Foreign Intel. Surv. Ct., https://www.fisc.uscourts.gov/amici-curiae (last visited Oct. 22, 2023); 50 U.S.C. § 1803(i).
57. 50 U.S.C. § 1803(i).
58. Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2022, Dir. Admin. Office U.S. Cts. (2022), https://www.uscourts.gov/sites/default/files/fisc_annual_report_2022.pdf.
59. See Adam Klein, Testimony before the Senate Committee on the Judiciary, Hearing on *The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties* (June 27, 2017), https://www.judiciary.senate.gov/imo/media/doc/06-27-17%20Klein%20Testimony.pdf.
60. *See* Adam Klein, *FISA Section 702 (2008–2023?)*, Lawfare (Dec. 27, 2022), https://perma.cc/5FP5-L9ZV.
61. See, e.g., Scarlet Kim, Diana Lee, Asaf Lubin & Paulina Perlin, *Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, Yale L. School Media Freedom & Info. Access Clinic (April 25, 2018) ("Governments have also interpreted the third party rule as prohibiting disclosure to other third parties and have included oversight bodies within that prohibition. Under this interpretation, the rule can be fundamentally detrimental to intelligence oversight."), https://law.yale.edu/mfia/case-disclosed/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing.
62. *See, e.g.,* Document regarding the Section 702 2018 Certification, FISC Opinion, Oct. 8, 2019, available at https://int.nyt.com/data/documenthelper/1880-fisa-rulings/40a12372947056b0dc08/optimized/full.pdf; David S. Kris, Amicus Curiae Letter Brief to Hon. James E. Boasberg, FISC Docket No. Misc. 19-02, Jan. 15, 2020, available at https://www.fisc.uscourts.gov/sites/default/files/FISC%20Misc%2019%2002%20Amicus%20Curiae%20letter%20brief%20January%2015%202020%20200115.pdf.
63. See Section V, *infra.*
64. 50 U.S.C. § 3092(a)(1).
65. Steven T. Dennis, *Judiciary Committee Tries to Assert Jurisdiction on FISA Rewrite*, Roll Call (March 28, 2014), https://rollcall.com/2014/03/28/judiciary-committee-tries-to-assert-jurisdiction-on-fisa-rewrite/.
66. /11 Commission Report, *supra* note 3, at 419–22.
67. In 2007, the House of Representatives under created a temporary panel within the House Appropriations Committee to oversee intelligence appropriations. *See* Jonathan Weisman, *Pelosi Looks to Boost Oversight of Intelligence and Ethics*, Wash. Post (Dec. 15, 2006), https://www.washingtonpost.com/archive/politics/2006/12/15/pelosi-looks-to-boost-oversight-of-intelligence-and-ethics/a6dbb382-a7e8-470d-bbb8-d7903bd95922/; Andrea Seabrook, *Congress Under Scrutiny Over Plane Bomb Plot*, NPR (Jan. 8, 2010), https://www.npr.org/2010/01/08/122372392/congress-under-scrutiny-over-plane-bomb-plot. The panel ultimately lapsed, however, and does not exist today.
68. Attorney Gen. W.P. Barr, Memorandum on Augmenting the Internal Compliance Functions of the FBI, Aug. 31, 2020, available at https://www.justice.gov/archives/ag/page/file/1311696/download.
69. *See e.g.*, FISA Query Audit, FBI Office of Internal Auditing (May 10, 2023), https://www.fbi.gov/file-repository/fisa-query-audit-051023.pdf/view.
70. Office of the Inspector General, Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation, 248, 252–55 (discussing the provision of inaccurate information to DOJ lawyers), https://www.justice.gov/storage/120919-examination.pdf.
71. *See Recent OIG Reports*, NSA Office Inspector Gen., https://oig.nsa.gov/ (last visited Oct. 22, 2013); *Office of Inspector General*, CIA, https://www.cia.gov/about/organization/inspector-general/ (last visited Oct. 22, 2023).
72. *See,* e.g., Steve Holland, *Trump fires intelligence official involved in his impeachment probe*, Reuters (April 3, 2020), https://www.reuters.com/article/us-usa-trump-inspectorgeneral-idUSKBN21M04U; Ed Pilkington, *Ousted US intelligence inspector general urges whistleblowers not to be 'silenced' by Trump*, The Guardian (April 6, 2020), https://www.theguardian.com/us-news/2020/apr/06/ousted-us-intelligence-inspector-general-urges-others-to-speak-out-and-defend-

whistleblowers; Jeremy Herb, *Trump fires intelligence community watchdog who told Congress about whistleblower complaint that led to impeachment,* CNN (April 4, 2020), https://edition.cnn.com/2020/04/03/politics/trump-fires-inspector-general-michael-atkinson/index.html.
73. 9/11 Commission Report, *supra* note 3, at 395.
74. Implementing Recommendations of the 9/11 Commission Act of 2007, 50 U.S.C. § 515(c), Pub. L. No. 110-53, 121 Stat. 265 (2007) (codified at 42 U.S.C. § 2000ee).
75. 42 U.S.C. § 2000ee(c)(1).
76. The Board's statutory jurisdiction is limited to activities of the Executive Branch "relating to efforts to protect the Nation from terrorism." *Id.* at § 2000ee(d). That does not mean, however, that the Board is able to review only programs used exclusively for counterterrorism. In practice, all systemically significant surveillance programs are used for counterterrorism and other intelligence purposes. Those programs are thus "related to efforts to protect the Nation against terrorism," and thus subject to oversight by the Board. Examples include Section 702 and the NSA's XKEYSCORE tool, both of which the Board has reviewed.
77. *Id.* at § 2000ee(f).
78. *Review of FISA Section 702 and Recommendations for Reauthorization*, President's Intelligence Advisory Board (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/Presidents-Intelligence-Advisory-Board-and-Intelligence-Oversight-Board-Review-of-FISA-Section-702-and-Recommendations-for-Reauthorization.pdf.
79. Exec. Order No. 14,086.
80. *Id.* at §§ 3(c)(iii), (f).
81. *Executive Order 14086: Attorney General designations of "qualifying states" under section 3(f) of EO 14086*, U.S. Dep't of Justice, Office of Priv. & Civ. Liberties (June 30, 2023), https://www.justice.gov/d9/2023-07/Attorney%20General%20Designation%20Pursuant%20to%20Section%203%28f%29%20of%20Executive%20Order%2014086%20of%20the%20EU%20EEA.pdf.
82. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).
83. 50 U.S.C. § 1881a.
84. FISC R. 13(b); *see also* 50 U.S.C. § 1805(d)(3).
85. *See, e.g., In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, Corrected Op. & Order, FISC Docket No. Misc. 19-02 (Boasberg, J.), Mar. 5, 2020, available at https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Corrected%20Opinion%20and%20Order%20JEB%20200305.pdf.
86. *See* Stephen I. Vladeck, *The FISA Court and Article III*, 72 Wash. & Lee L. Rev. 1161 (2015).
87. *United States v. Muhtorov,* 20 F.4th 558, 582 (10th Cir. 2021).
88. *In re Sealed Case,* 310 F.3d at 736.
89. 50 U.S.C. § 1801(a)(4).
90. "U.S. persons" include citizens, lawful permanent residents, U.S. companies, and unincorporated associations with "a substantial number" of U.S.-person members. *Id.* § 1801(i.)
91. *Id.* § 1801(b).
92. *Id.* at § 1842(c)(2).
93. 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, Priv. & Civ. Liberties Oversight Bd. (Jan. 23, 2014), at 8, 98, https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf ("PCLOB Call Records Report").
94. USA Freedom Act of 2015, Pub. L. No. 114-23, § 201, 129 Stat. 268, 277 (June 2, 2015).
95. 50 U.S.C. § 1805(d)(1).
96. *Id.* at § 1805(d)(2).
97. Crossfire Hurricane Report, *supra note* 70, at 74.
98. Adam I. Klein, *Chairman's White Paper: Oversight of the Foreign Intelligence Surveillance Act,* Priv. & Civ. Liberties Bd. (June 2021), at 21–22 https://documents.pclob.gov/prod/Documents/EventsAndPress/ec2bfc95-f111-4123-87d5-8a7827bf2fdd/Chairman's%20FISA%20White%20Paper.pdf.
99. 50 U.S.C. §§ 1881c(a)(2), (c)(1)-(2).
100. *See The NSA files: Verizon forced to hand over telephone data – full court ruling*, The Guardian (June 5, 2013), https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order; *ACLU v. Clapper,* 785 F.3d 787, 818–19, 821 (2d Cir. 2015) ("to allow the government to collect phone records only because they may become relevant to a possible authorized investigation in the future fails even the permissive 'relevance' test").
101. *See* Crossfire Hurricane Report, *supra* note 70, at v, 4 n.6; *In re Carter W. Page*, Verified Application, FISC Docket No. 16-1182 (Jan. 13, 2017), available at https://www.judiciary.senate.gov/imo/media/doc/FISA%20Warrant%20Application%20for%20Carter%20Page.pdf.
102. Chairman's White Paper, *supra* note 97, at 2–4.
103. *See* David Kris, *How the FISA Court Really Works*, Lawfare (Sept. 2, 2018), https://www.lawfaremedia.org/article/how-fisa-court-really-works; Letter from the Hon. Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Hon. Patrick Leahy, Chairman, Senate Committee on the Judiciary, July 29, 2013, https://irp.fas.org/news/2013/07/fisc-leahy.pdf (describing then-current practices of the FISA court).
104. *Id.* at 5–7 (explaining the FISA Court's interaction with the government in reviewing proposed applications, seeking additional information, conveying the court's concerns, and adjudicating final applications).
105. Adam I. Klein, *Chairman's White Paper: Oversight of the Foreign Intelligence Surveillance Act*, Priv. & Civ. Liberties Bd. (June 2021), at 6–7, available at https://documents.pclob.gov/prod/Documents/EventsAndPress/ec2bfc95-f111-4123-87d5-8a7827bf2fdd/Chairman's%20FISA%20White%20Paper.pdf (declassified by C28W34B64 on June 8, 2021).
106. Chairman's White Paper, supra note 97, at 6–7.
107. 50 U.S.C. § 1881c(a)(3).
108. There is oversight within the Executive Branch, however. Lawyers at the Department of Justice review every tasking sheet. *See FISA Section 702 Fact Sheet*, Office of the Director of National Intelligence, https://www.intelligence.gov/assets/documents/702%20Documents/FISA_Section_702_Fact_Sheet_JUN2023.pdf (last visited Oct. 24, 2023).
109. *See* Office of the Director of National Intelligence, IC on the Record, https://icontherecord.tumblr.com/.
110. *Release of Documents Related to the 2023 FISA Section 702 Certifications*, Office of the Director of National Intelligence, IC on the Record, (July 21, 2023), https://icontherecord.tumblr.com/.
111. A "non-U.S. person" target, to be precise.
112. *See supra* note 1.
113. U.S. Const. art. I, § 8.
114. *Id.*
115. *Id.* at art. I, §§ 8, 9.
116. *Id.* at art. I, § 8.
117. *Id.* at art. II, § 2.
118. *United States v. Curtiss-Wright Export Corp*., 57 S. Ct. 216, 220 (1936) ("powers of external sovereignty d[o] not depend upon the affirmative grants of the Constitution"); Jean Galbraith, *The Runaway Presidential Power over Diplomacy*, 108 Vir. L. Rev. 81, 85, 91–93 (2022).
119. *Zivotofsky v. Kerry,* 576 U.S. 1, 12–13 (2015).
120. U.S. Const. art. II, § 1.
121. *See generally, United States v. Muhtorov,* 20 F.4th 558, 607 (10th Cir. 2021) (advisory opinions); id. at 609 n.29 (adverseness); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409–10 (2013) (standing).

122. Letter from John Yoo, Dep. Assistant Attorney Gen., to FISC (May 17, 2022) https://www.documentcloud.org/documents/2723976-John-Yoo-to-FISC-2002-Stellarwind.html#document/p7/a280570.
123. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV.
124. *Katz v. United States*, 389 U.S. 347, 359 (1967).
125. *Smith v. Maryland,* 442 U.S. 735, 742 (1979); *but cf. Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (distinguishing historical cell-site location data from earlier forms of third-party data).
United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
126. *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010).
127. *In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004, 1012 (FISCR 2008) ("For these reasons, we hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.").
128. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313 (1972).
129. Alex Abdo, *Why Rely on the Fourth Amendment To Do the Work of the First?*, Yale L. J. Forum (Oct 25, 2017), at 7, https://www.yalelawjournal.org/pdf/Abdo_5czbvbj9.pdf.
130. National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 496 (1947); Central Intelligence Agency Act, Pub. L. No. 81-110, 63 Stat. 208 (1949).
131. Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
132. *See* Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–23.
133. Privacy and Civil Liberties Oversight Board, Report on Executive Order 12,333 (2021), at 14, available at https://documents.pclob.gov/prod/Documents/OversightReport/b11b78e0-019f-44b9-ae4f-60e7eebe8173/12,333%20Public%20Capstone.pdf.
134. *Id.* at 13 (citing House Comm. on Gov't Ops., *Executive Orders and Proclamations: A Study of a Use of Presidential Powers*, U.S. Gov't Printing Office (1957)) (last visited Oct. 26, 2023).
135. *Id.* at 14.
136. Exec. Order No. 12,333 § 1.7(c)(1); *see also Executive Order 12,333*, NSA/CSS, https://www.nsa.gov/Signals-Intelligence/EO-12,333 (last visited Oct. 26, 2023) ("Executive Order (EO) 12,333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information.").
137. Exec. Order No. 12,333 § 1.3(b)(12)(A)(i).
138. *See generally* S. Rep. No. 94-755, Book II (1976) [hereinafter Church Committee Report].
139. Exec. Order No. 12,333 § 2.9.
140. *E.g., Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12,333* (2017), https://www.cia.gov/static/CIA-AG-Guidelines-Signed.pdf.
141. *See, e.g., Release of Documents Related to the 2023 FISA Section 702 Certifications*, Office of the Director of National Intelligence, IC on the Record (July 21, 2023), https://icontherecord.tumblr.com/.
142. *See, e.g.,* USSID SP0018: Legal Compliance and U.S. Persons Minimization Procedures, National Security Agency (Jan. 25, 2011), https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf; FBI Domestic Investigations and Operations Guide (DIOG), https://vault.fbi.gov/FBI%20 Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 (last visited Oct. 26, 2023).
143. Katie Bo Lillis, *NSA watchdog finds 'concerns' with searches of Americans' communications*, CNN (Jan. 31, 2022), https://www.cnn.com/2022/01/31/politics/nsa-watchdog-concerns-searches-american-communications/index.html.
144. For example, in 2019 DOJ lawyers audited queries in 27 of the 56 FBI field offices—fewer than half. *ODNI Releases 25th and 26th Joint Assessments of FISA Section 702 Compliance, Office of the Director of National Intelligence* (Sept. 29, 2023), https://www.intelligence.gov/ic-on-the-record-database/results/1277-25th-and-26th-joint-assessments-of-fisa-section-702-compliance.
145. *See* Sections 4–6, *supra.*
146. *See* Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2022, Office of the Director of National Intelligence (April 2023), available at https://www.odni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.
147. *See, e.g. The FISA Amendments Reauthorization Act of 2017: Enhanced Privacy Safeguards for Personal Data Transfers Under Privacy Shield,* Office of the Director of National Intelligence, at 4 (Oct. 15, 2018), https://www.dni.gov/files/documents/icotr/Summary-FISA-Reauthorization-of-2017---10.15.18.pdf.
148. *See* Section 5.A, *supra.*
149. USA Freedom Act of 2015, Pub. L. No. 114-23, Title VI (June 2, 2015).
150. *Id.* at § 402.
151. *Id*. at § 603.
152. *Id.* at § 602.
153. *See,* e.g., *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, Corrected Op. & Order, Docket No. Misc. 19-02 (FISC 2020); Letter filed by Kevin O'Connor, National Security Div., U.S. Dep't of Justice, in *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC,* Docket No. Misc. 19-02, U.S. Dep't of Justice (March 1, 2021), https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Letter%20of%20March%201%202021.pdf.
154. *E.g., Release of Documents Related to the 2023 FISA Section 702 Certifications* (July 21, 2023), https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
155. *See generally Making Lawful Disclosures*, Office of the Director of National Intelligence, https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-related-menus/icig-related-links/making-lawful-disclosures (last visited Nov. 1, 2023).
156. *Id.*
157. 18 U.S.C. § 793;; *see Federal Government Contractor in Georgia Charged With Removing and Mailing Classified Materials to a News Outlet*, U.S. Dep't of Justice, Office of Public Affairs (June 5, 2017), https://www.justice.gov/opa/pr/federal-government-contractor-georgia-charged-removing-and-mailing-classified-materials-news (NSA contractor Reality Winner charged with removing classified material from a government facility and mailing it to a news outlet in violation of 18 U.S.C. § 793(e)).
158. Yochai Benkler, *A Public Accountability Defense For National Security Leakers and Whistleblowers*, 8 Harv. L. & Pol'y Rev. 281, 284–86 (2014); *see also* Phoebe Greenwood, *Edward Snowden should have right to legal defence in US, says Hillary Clinton*, The Guardian (July 4, 2014), https://www.theguardian.com/world/2014/jul/04/edward-snowden-legal-defence-hillary-clinton-interview ("The laws would not provide [Snowden] with any opportunity to say that the information never should have been withheld from the public in the first place. And the fact that the disclosures have led to the highest journalism rewards, have led to historic reforms in the US and around the world – all of that would be irrelevant in a prosecution under the espionage laws in the United States.") (quoting Ben Wizner).
159. *Air National Guardsman Indicted for Unlawful Disclosure of Classified National Defense Information*, U.S. Dep't of Justice, Office of Public Affairs (June 15, 2023), https://www.justice.gov/opa/pr/air-national-guardsman-indicted-unlawful-disclosure-classified-national-defense-information#:~:text=Jack%20Douglas%20Teixeira%2C%2021%2C%20of,defense%20(National%20Defense%20Information; Glenn Thrush, *Airman Who Leaked Files Is Indicted on Charges of Mishandling Secrets*, The NY Times (June 15, 2023), https://www.nytimes.com/2023/06/15/us/politics/jack-teixeira-indicted-document-leaks.html.
160. *See* Adam Klein, *The Cyclical Politics of Counterterrorism,* 40 Wash. Quarterly 95, 98 (Summer 2017).
161. *See*, e.g., L. Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress*, 1946-2004, at 8 (2008) (noting that oversight meetings were rare and informal and none of the subcommittees responsible for oversight of CIA had the ability to store classified information).

162. *See* Church Committee Report, *supra* note 137, at 1–20.
163. 9/11 Commission Report, *supra* note 3, at 339–428.
164. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. Law No. 107-56, 115 Stat. 272, § 224 (2001).
165. *See* Robert Chesney, *Three FISA Authorities Sunset in December: Here's What You Need to Know*, Lawfare (Jan. 16, 2019), https://www.lawfaremedia.org/article/three-fisa-authorities-sunset-december-heres-what-you-need-know.
166. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, § 403(b)(1) (2008).
167. *See* USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (June 2, 2015).
168. *See* Robert Chesney, *Three FISA Authorities Sunset in December: Here's What You Need to Know*, Lawfare (Jan. 16, 2019), https://www.lawfaremedia.org/article/three-fisa-authorities-sunset-december-heres-what-you-need-know.
169. *See* Section VIII.B.2, *infra.*
170. Chairman's White Paper, supra note 97, at 23–26.
171. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).
172. Phillip Ewing, *Controversial Spy Law Passes House After Shots from Trump, who then Supported it*, National Public Radio (Jan. 11, 2018), https://www.npr.org/2018/01/11/577331402/ahead-of-hill-vote-trump-attacks-spy-bill-his-administration-supports.
173. *E.g., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Priv. & Civ. Liberties Oversight Bd., at 106 (Sept. 28, 2023), available at https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf (majority report).
174. *See id.* at Annex B (minority report of Board Members Beth A. Williams and Richard E. DiZinno).
175. *See, e.g., Missouri v. Biden*, 83 F.4th 350 (5th Cir. 2023).
176. Press Release, *Fact Sheet—U.S. Defense Contributions to Europe*, U.S. Dep't of Defense (June 29, 2022), https://www.defense.gov/News/Releases/Release/Article/3078056/fact-sheet-us-defense-contributions-to-europe/.
177. *See* Treaty of Mutual Cooperation and Security Between the United States and Japan, 11 U.S.T. 1632 (1960); Mutual Defense Treaty Between the United States of America and the Republic of Korea, 5 U.S.T. 2368 (1953); Security Treaty between Australia, New Zealand and the United States of America, U.N.T.S. 83–89 (1952); Mutual Defense Treaty Between the Republic of the Philippines and the United States of America, 3 U.S.T. 3947 (1951); *Rusk-Thanat Communiqué* (Thailand), in American Foreign Policy: Current Documents, 1962, at 1093, available at https://babel.hathitrust.org/cgi/pt?id=pst.000043544141&seq=1167.
178. David Vergun, *U.S. Nuclear Umbrella Extends to Allies, Partners, Defense Official Says*, DoD (Apr. 24, 2019), https://www.defense.gov/News/News-Stories/Article/Article/1822953/us-nuclear-umbrella-extends-to-allies-partners-defense-official-says/.
179. Mark F. Cancian et. al., *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*, Center for Strategic and International Studies (Jan. 9, 2023), https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.
180. Thomas Shugart, *First Strike: China's Missile Threat to U.S. Bases in Asia*, Center for a New American Security (Jun. 28, 2017), https://www.cnas.org/publications/reports/first-strike-chinas-missile-threat-to-u-s-bases-to-asia.
181. *See,* Jack Davis, *Strategic Warning*, in Handbook of Intelligence Studies, Routledge (Dec. 7, 2006), https://www.routledgehandbooks.com/pdf/doi/10.4324/9780203089323.ch13 (achieving tactical and strategic warning require, among other things, "the processing of a vast volume of information from open sources as well as from specialized collection efforts that could signal either pending or over-the-horizon threats").
182. Cf. Adam Rawnsley, *Espionage, Moi?,* Foreign Policy (Jul. 2, 2023), https://foreignpolicy.com/2013/07/02/espionage-moi/; Reuters, German Security Recorded Clinton Conversation, (Aug. 15, 2024), https://www.reuters.com/article/uk-germany-usa-spying-idAFKBN0GF1RR20140815.
183. *See*, Press Release, *U.S. Shoots Down Turkish Drone Threatening Troops in Syria*, Foundation for the Defense of Democracies (Oct. 6, 2023), https://www.fdd. org/analysis/2023/10/06/u-s-shoots-down-turkish-drone-threatening-troops-in-syria/.
184. Katrin Bennhold, *The Former Chancellor who Became Putin's Man in Germany*, N.Y. Times, Apr. 23, 2022, https://www.nytimes.com/2022/04/23/world/europe/schroder-germany-russia-gas-ukraine-war-energy.html.
185. John O'Donnell & Luke Baker, *Germany, France Demand 'no-spy' Agreement with U.S.*, Reuters (Oct. 25, 2023), https://www.reuters.com/article/us-eu-summit/germany-france-demand-no-spy-agreement-with-u-s-idUKBRE99N0BJ20131025.
186. *2021-2022 Public Attitudes on US Intelligence*, Univ. of Texas at Austin, Strauss-Clements Intelligence Studies Project (Sept. 1, 2023) ("There were notable partisan differences in views of US Intelligence. Between the 2020 and 2021 surveys—including the transition between the Trump and Biden administrations—Democrats who believed that the IC was vital increased while Republican support for the IC decreased significantly."), https://intelligencestudies.utexas.edu/news/2021-2022-public-attitudes-on-us-intelligence/.