Protecting Privacy and Promoting Transparency in a Time of Change:
My Perspective after 14 Years as Civil Liberties Protection Officer

Alex Joel

In June 2005, I joined the brand-new Office of the Director of National Intelligence as a detailee from the Central Intelligence Agency's (CIA's) Office of General Counsel. Just a couple of months earlier, President Bush had sworn in the nation's first Director of National Intelligence, John Negroponte. The statute creating the ODNI—the Intelligence Reform and Terrorism Prevention Act of 2004—included a new Intelligence Community position, that of the "Civil Liberties Protection Officer." ODNI named me the "interim" Civil Liberties Protection Officer and removed the "interim" qualifier six months later. I served in that role for 14 years, reporting directly to five different Directors of National Intelligence.

During my tenure, I was privileged to take part in momentous changes in the legal framework governing our intelligence activities. I am now teaching a course on National Security Surveillance and Secrecy, which has given me an opportunity to study that framework in greater depth and wrestle with enduring issues. This may sound simplistic, but as I look back on what I learned and experienced as the Civil Liberties Protection Officer, the key theme that stands out is *change*. Change came at us constantly, manifesting itself as new threats to national security, new organizations and missions, new technologies and sources of data, new imperatives for intelligence agencies to respond to, and new risks to privacy and civil liberties.

We faced these changes with legal tools that had been developed for a different era. Lawyers tend to think of change as happening incrementally. Laws are passed after months or years of debate, often prompted by specific events that happened at a point in time. Courts issue their decisions long after the start of the litigation. Nation states enter into international agreements after years of negotiations. The rapid pace of change in the world around us does not wait for the law to catch up. Yet our national security legal framework must still function effectively in the face of constant change; we must apply old rules to new tools. So, how well does our legal framework hold up to the challenges posed by constant change?

To Authorize and Constrain

At the outset, it is critical to understand that through all the change we see around us, there are certain enduring truths. The most fundamental one for our purposes is this: in a democracy, the national security legal framework must simultaneously achieve two vital goals. It must enable, authorize, and empower government actors to protect the nation from foreign threats; and it must constrain, restrict, and control those actors to protect privacy and civil liberties. Both are equally important. Failing either means failing as a democracy.

Achieving these goals simultaneously is no easy task. To protect against threats, agencies not only need people, resources, and skill; they also need specialized legal authorities that enable them to conduct activities that can be highly intrusive on personal privacy. And they need the ability to do so in secret, to conceal their sources and methods from their adversaries, lest those

adversaries change their behavior to avoid detection. A fully transparent intelligence service, after all, would be fully ineffective.

At the same time, it is vital that our legal framework also constrain and control the exercise of those powers. In other words, our national security agencies must protect the nation from foreign threats, without themselves becoming a threat.

How well does that framework accomplish these twin objectives? In this paper, I will highlight certain aspects that stand out in my mind as I look back on my time at ODNI. My focus is on surveillance and secrecy, and their impact on privacy and transparency. These are enormously complex and nuanced topics that I cover at a high level in a semester-long course; given the constraints of this paper, I can only provide a surface-level overview of a few elements.

Executive Power

Any discussion of rules must start with the way in which the Constitution separates powers between the branches. The Executive is commonly thought of as having primacy on matters of national security. Oft-quoted to this day is the Supreme Court's early pronouncement that "The President is the sole organ of the nation in its external relations" (*United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304 (1936)). But this power is not absolute, as Congress also plays a key role. For separation of powers issues, there is no better construct than that established by Justice Jackson in his concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952). Supreme Court justices continue to refer to it to this day (see, e.g., *Biden v. Texas*, 142 S. Ct. 2528, 2557 (2022) (Alito, J. dissenting). In a nutshell, when asserting executive authority in the national security arena, the President's power will be at its highest if he acts consistent with the will of Congress; at its lowest if he acts contrary to the will of Congress; and in a "zone of twilight" where Congress and the President have concurrent power or distribution is uncertain.

These issues were very much in the public eye when the New York Times broke the news in 2005 about the Terrorist Surveillance Program (later renamed the President's Surveillance Program). After 9/11, President Bush directed the interception of communications under circumstances that ordinarily would have required a court order under FISA. I had joined ODNI only a few months earlier and found out about this program when I woke up to an NPR broadcast describing the story. By chance, later that day I interviewed Tim Edgar from the ACLU, who would join me as one of my new deputies (he recounts this in his book Beyond Snowden). Learning more about the program turned to be more difficult than I first assumed, since, as was reported in detail by the IG reports on the program, it was tightly compartmented with access controlled by the White House (see, e.g., the ODNI IG's report at page 14 (page 72 of the PDF file)). With the support of the DNI, I was eventually able to gain access, along with the then-nascent Privacy and Civil Liberties Oversight Board. Ultimately, thanks to the efforts of the ODNI General Counsel among others, the program was moved under the auspices of the FISC (after major modifications), and then superseded with the passage of the Protect America Act of 2007 and the FISA Amendments Act of 2008. I now teach this as a case study on separation of powers arguments, using this Department of Justice (DOJ) letter as the focal point.

All told, the President's decision to initiate this program after 9/11, however well-intentioned it may have been at the time, created major repercussions throughout the ensuing years. My own takeaway from this experience: the Executive must do all it possibly can to act consistent with the will of Congress. The perceived advantages of moving quickly are likely to be fleeting, and even if arguably constitutional, such action could cause lasting damage to public trust.

The Key Role of Congress

Notwithstanding claims of Executive primacy, Article I of the Constitution provides Congress with a series of important authorities that it can and does exercise over national security matters. Perhaps its most effective power is its control over the Federal purse; the Executive cannot expend funds that have not been appropriated by Congress (*see, e.g.*, *Sierra Club v. Trump*, 963 F.3d 874 (9th Cir. 2020), *vacated and remanded sub nom. Biden v. Sierra Club*, 142 S. Ct. 46 (2021)). If Congress does not provide funding for a program or activity, that effort is dead. If Congress does not fund the Federal Government, it shuts down.

One power that is not expressly listed in Article I is oversight, but the Supreme Court has found that this authority is necessarily implied. There are a range of statutory reporting and related requirements for providing Congress with information and for keeping Congress "fully and currently informed." The DNI updated an intelligence community directive to emphasize the importance of this mandate. In my time at ODNI, I felt that Congress exercised its oversight powers vigorously. The House and Senate intelligence oversight committees are staffed with experienced, dedicated and expert professionals who have the necessary clearances to review sensitive information. Members and staff ask penetrating questions, demand extensive briefings and reports, and are not shy about taking agencies to task for failures or delays in providing information. While the IC likely can do better in providing timely responses to congressional requests, from my perspective, disputes over access to information have been the exception rather than the rule.

Indeed, for me a takeaway from my time at ODNI is that the IC should lean into providing Congress with information. Putting this in terms of Justice Jackson's three categories, the Executive is best positioned when acting in accordance with the express or implied will of Congress, and Congress can only have a "will" about things on which it has been fully and currently informed.

The Judiciary

Turning to the third branch of government, the role of the judiciary in national security is a complicated one. On the one hand, the Supreme Court has interpreted the "cases and controversies" clause in Article III in a manner that sharply limits the ability of individuals to challenge national security programs in civil cases. That is because a plaintiff must show actual injury to establish standing; they cannot rely on "mere speculation" but must, in essence, demonstrate that they have been the subject of surveillance. While this can seem an impossible hurdle in the face of classified information, it can be done (*see Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv.*, 14 F.4th 276 (4th Cir. 2021)).

Even if standing can be established, the Executive could assert the state secrets privilege to prevent a case from going forward if it would necessarily require the disclosure of classified information. This privilege was recently reaffirmed by the Supreme Court in *United States v. Zubaydah*, 142 S. Ct. 959 (2022). Recognizing the seriousness of the concerns raised over this privilege, the Department of Justice has issued guidance under both the Obama and Biden administrations on when and how the privilege can be asserted.

On the other hand, the judiciary is long-accustomed to adjudicating FOIA cases involving requests for national security material. In addition, the Foreign Intelligence Surveillance Court (FISC), an Article III court, plays a key role in FISA. For example, the FISC has played a public role in holding the FBI accountable for FISA violations with respect to the Crossfire Hurricane investigation.

It is important to keep in mind that in criminal cases, the defendants retain their constitutional and statutory rights to a fair trial including access to information being used against them. The Classified Information Procedures Act enables courts to handle criminal cases involving national security information. And in cases where information derived from FISA surveillance is at issue, FISA itself requires the government to so notify the defendant (50 U.S.C. section 1806(c)), enabling the defendant to challenge the legality of the surveillance in the criminal proceeding. Once notified, the defendant should be able to readily meet standing requirements and thus pursue civil remedies, including those laid out in FISA itself (50 U.S.C. section 1810).

Providing individuals with the right to pursue civil remedies in court on matters of national security presents a huge challenge. Who the targets of surveillance are—and who they are not—can often itself be a national security secret. If you cannot pursue a remedy in court due to national security secrecy concerns, what then? This is where nonjudicial mechanisms can play a role. Congress has mandated that civil liberties and privacy officers at key agencies must ensure that their agency has "adequate procedures to receive, investigate, respond to, and redress complaints from individuals" (42 U.S.C. section 2000ee-1). In addition, the National Security Act of 1949 (as amended by the Intelligence Reform and Terrorism Prevention Act of 2004), assigned to the Civil Liberties Protection Officer a complaint resolution and investigation function (50 U.S.C. section 3029). Moreover, offices of inspector general have statutory responsibilities to investigate allegations of fraud, waste, and abuse, and to receive and transmit whistleblower complaints while protecting against retaliation. The independence of the IG community is critical, and I have written about the need for senior leadership—including the President—to fully support that independence. As discussed later in this paper, a recent executive order now provides for an innovative new avenue of redress and includes important independence provisions.

Fourth Amendment

Fourth Amendment jurisprudence is a fundamental part of national security surveillance law. The government is not free to ignore the fourth amendment—or any other part of the Constitution—as it pursues national security objectives. That said, the question of whether and how the Fourth Amendment applies to a national security activity is a complex one.

First, there is the issue of what the Fourth Amendment protects, regardless of whether the government is acting with national security in mind. As established by the Supreme Court in 1967 (*Katz v. United States*, 389 U.S. 347 (1967)), the Fourth Amendment protects reasonable expectations of privacy. The judicial understanding of what that means in the digital age continues to evolve. For example, in *Riley v. California*, 573 U.S. 373 (2014), the Court refused to extend cell phones the "incident to arrest" exception to the warrant requirement, stating "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life'" And in *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018), the Court refused to extend to the third party doctrine to cell site location information (CSLI), holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI" covering an extended period of time. These cases provide hope that the slow-moving judiciary is now grappling with the implications of technological change (this trend is sometimes referred to as "digital is different"), but also raise unanswered questions for practitioners on how to shape policies and programs as technology continues to leap ahead.

Second, courts have found that there is a foreign intelligence exception to the warrant requirement (*see, e.g.*, *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157 (2d Cir. 2008). That is, assuming the Fourth Amendment applies to a government activity, courts have held that the government may collect foreign intelligence information without first obtaining a warrant, so long as the collection is "reasonable" under the fourth amendment.

The warrant requirement continues to be of intense interest in the context of FISA Section 702, where information is initially collected and subsequently queried without a warrant, albeit within a system of controls and oversight. In particular, some have argued that the government should first obtain a warrant when conducting queries targeting U.S. persons. At least one court, when wrestling with this issue directly, stated: "What kinds of querying, subject to what limitations, under what procedures, are reasonable within the meaning of the Fourth Amendment, and when (if ever) such querying of one or more databases, maintained by an agency of the United States for information about a United States person, might require a warrant, are difficult and sensitive questions" (*United States v. Hasbajrami*, 945 F.3d 641, 672-673 (2d Cir. 2019)).

But I get ahead of myself, as these "difficult and sensitive questions" involve FISA, discussed next.

FISA

Intelligence agencies are, of course, bound to follow the laws enacted by Congress. While there are a range of statutes that are deeply relevant to intelligence professionals (as evidenced by the ABA's Intelligence Community Law Sourcebook), the one that occupied most of my time was the Foreign Intelligence Surveillance Act. This is a complex statute with a rich history, and I will only highlight a few aspects here.

Electronic Surveillance and Physical Search. FISA is composed of several key titles, each covering a different type of surveillance authority. Titles I and III cover "electronic surveillance" and "physical search" respectively, each with its own statutory definition. If an activity

constitutes electronic surveillance or physical search as defined in the statute, the government must obtain an order approved by the FISC that establishes, among other things, that there is probable cause to believe that the target of the surveillance or search is a "foreign power" or "agent of a foreign power." One way to (simplistically) think of these authorities is that they apply when a warrant would be required for law enforcement purposes. This is the part of FISA at the center of the Crossfire Hurricane investigation.

Titles IV and V. Title IV covers the use of "pen register" and "trap and trace" devices (again, those terms have specific definitions), while Title V can be thought of as covering certain categories of business records (e.g., from airlines, bus companies, hotel companies). Each title has its own statutory standard that must be met for obtaining a FISC order. Note that the scope of the business records authority had been expanded in 2001 by Section 215 of the USA PATRIOT Act, and the government had obtained court orders from the FISC that, under a broad (and classified) interpretation of "relevance," enabled NSA to obtain staggering volumes of U.S. domestic call detail records. This program generated enormous controversy following disclosures by Edward Snowden in 2013, ultimately resulting in termination of the program under the USA FREEDOM Act, which, among other things, prohibited any bulk collection under this and other key authorities. (An excellent description can be found in this report by the Privacy and Civil Liberties Oversight Board). With the sunset of certain provisions in the USA FREEDOM Act, the language of Title V has now reverted to the text in effect before the PATRIOT Act's Section 215 amendment.

A key takeaway for me is the vital importance of transparency about interpretations of law. The government had put forward and the FISC had approved a novel interpretation of an important national security authority with far-reaching impact. We recognized at the time the importance of public transparency on this issue, but did not find a way to make this interpretation public without disclosing what the IC felt at the time to be highly sensitive information. Director of National Intelligence James Clapper was to later say that the IC should have been transparent about the outlines of this program from the start, and I certainly agree.

Section 702. Section 702 is undoubtedly the statutory provision that occupied most of my time and energy during my tenure as CLPO. Enacted as part of the FISA Amendments Act of 2008, it is often cited as an example of a statutory amendment designed to be "technology neutral." In 1978, Congress deliberately crafted the definition of "electronic surveillance" under Title I to cover certain types of surveillance and exclude others (as reported in S. Rep. 95-604(I)(1977), "[t]he reason for excepting from the definition of 'electronic surveillance' the acquisition of international radio communications … is to exempt from the procedures of the bill certain signals intelligence activities of the National Security Agency"). Congress calibrated this definition based on how the telecommunications traffic flowed at that time, with international communications traveling by satellite ("radio communications")—and therefore outside of the scope of Title I's court order requirements—and domestic communications traveling by "wire"—and therefore in many cases subject to such requirements. Proponents of the FISA Amendments Act argued that in the decades since 1978, global communications flows had changed, with most communications being carried via transatlantic cables (i.e., by wire); this

resulted in a de facto expansion of the scope of communications covered by FISA's probable cause requirement to include foreign terrorist suspects abroad who would otherwise have no Fourth Amendment rights.

Section 702 authorizes the government to target non-U.S. persons reasonably believed to be outside the United States to collect foreign intelligence information, with the compelled assistance of communications providers. The government must do so in accordance with court-approved targeting, minimization, and querying procedures, which have been released in redacted form (see the ODNI's Guide to Posted Documents for links to released procedures). Section 702 is subject to a sunset clause and will expire at the end of 2023 unless it is reauthorized. When I was in government, I was especially heartened at how fulsomely the IC supported the addition of Sections 703, 704, and 705, which in essence extended the requirement to obtain an individualized probable-cause-based FISC order to cover U.S. persons outside the United States.

Section 702 is subject to rigorous compliance and oversight measures, which are described in detail in joint semiannual compliance assessments that have been redacted and released over time (these assessments can be found on IC on the Record). At CLPO, we spent a great deal of time working with OGC, the agencies, and DOJ developing and implementing these measures, reporting incidents to the FISC and Congress, and ensuring that violations were remediated (including destruction of improperly collected or retained data).

The ODNI also publishes an annual statistical transparency report that sets forth important quantitative data about the government's use of FISA (and national security letter) authorities. When I was at CLPO, we assembled and published the first statistical transparency report in 2014 as part of the IC's transparency efforts. Congress codified this into an annual reporting requirement under 50 U.S.C. section 1873(b). The IC has leaned into this reporting requirement, adding detailed explanations, graphical examples, and statistical trends (see the report for calendar year 2020 here).

As with other topics touched on in this paper, Section 702 is a rich and nuanced topic in itself that merits more extended discussion than I can give in this brief overview.

A Rubber Stamp?

Particularly during my early years at ODNI, I heard criticisms that the FISC was a "rubber stamp" – that it would automatically accept government submissions at face value, without serious inquiry, and would approve whatever was put in front of it. This was definitely not the view of those who regularly dealt with the FISC within government. As publicly released opinions show, the FISC did not hesitate to take the government to task for its failings. In public correspondence with Congress, the FISC explained in detail the process by which they review government submissions; in many cases, the court raised questions in exchanges with DOJ that resulted in modifications or withdrawals of orders prior to final submission. The FISC's public reports showing the actions of the court are now broken down into subcategories to better illustrate this iterative process.

A second criticism of the FISC that I still hear is that it is a "secret court," the implication being that because it operates in secret, it cannot be trusted. First, a great deal has been made public about the FISC. It has its own public website which posts the FISC's opinions, orders, pleadings and the like (sometimes redacted); its rules are also available there. The ODNI recently announced it had released all FISA court opinions covered by a congressional transparency mandate. More importantly, a "secret court" is essential to a democracy—as is "secret oversight" in general. If it operated entirely in the public eye, then it would have no ability to conduct judicial oversight over sensitive activities of the intelligence agencies, which would denude its role of much of its substance. We should seek to enhance transparency where we can, but we must ensure that the FISC has the ability to access whatever classified information it needs to see in order to ensure that the agencies are complying with its orders and following FISA requirements.

Executive Order 12333

Those working in the national security space know that Executive Order 12333 is a foundational document for the Intelligence Community. I have written about this Order before (*see, e.g.*, *Protect Privacy. That's an Order* and *The Truth about Executive Order 12333*) and will not belabor it here, other than to highlight a few key points.

- First, it has the full force and effect of law within the government; compliance by intelligence agencies is mandatory.
- Second, it cannot be used to circumvent existing laws; there is no "get out of jail free card" inherent in the order. Rather, it commands agencies to follow applicable law.
- Third, agencies cannot use it to impose binding obligations on those outside government; rather, the order allocates national security responsibilities among government agencies, and restrains those agencies in order to protect privacy and civil liberties.

Although the order establishes restrictions in several areas (including assistance to law enforcement, human experimentation, and assassination), Section 2.3 is the provision that is most relevant in the information age. That section limits how intelligence agencies collect, retain, and disseminate information relating to U.S. persons, and requires agencies to have "procedures" (sometimes referred to as "guidelines") approved by the Attorney General in consultation with the DNI with more detailed protections (there are links to the procedures here).

When I was in government, we spent a great deal of time updating these procedures. Our goal was to bring them into the modern era while harmonizing protections and using consistent terminology where possible. President Bush updated the order in 2008 to make it consistent with the organizational changes wrought by the Intelligence Reform and Terrorism Prevention Action of 2004 (most notably, the creation of the DNI). The changes are described in this CLPO Information Paper.

There is much more to say about this order, but again, due to space constraints, I will refrain from doing so.

Executive Order 14086

In October of 2022, President Biden signed out Executive Order 14086 on Signal Intelligence Activities (EO 14086). This order enhances privacy safeguards for United States signals intelligence activities, and unquestionably breaks new legal ground for the Intelligence Community. The team I lead on Privacy Across Borders at the Tech, Law and Security Program has been digging into this new executive order and we will have much more to say about it in the near future. For now, here are some of the reasons why I find this order (and the instrument it replaced and expanded upon, Presidential Policy Directive 28) to break new ground for the Intelligence Community.

First and foremost, it extends key privacy safeguards to cover all individuals, regardless of nationality. The legal instruments the U.S. put in place after the Church Committee responded to the abuses of that era, when intelligence agencies improperly sought to conduct surveillance on (and in some cases influence) Americans exercising their First Amendment freedoms, thus threatening to subvert the democratic process. Not surprisingly, the major reforms that followed—such as FISA and EO 12333—aimed to prevent such abuses in the future, and thus focused their protections on domestic activities and the rights of U.S. persons.

We now live in a very different world, one that is bound together tightly by a web of communications carrying personal information of people from around the globe. U.S. companies run much of this infrastructure. It should come as no surprise, then, that our foreign partners are concerned about the safeguards that U.S. intelligence agencies will apply to their citizens' data. EO 14086 answers those concerns emphatically by protecting the privacy of both U.S. and non-U.S. persons.

Second, the order delineates 12 legitimate objectives that can be pursued through signals intelligence activities. It also lays out four prohibited objectives (such as suppressing free speech) and declares that collection of foreign private commercial information to afford a US company with a competitive advantage is not a legitimate objective. The order goes on to include the CLPO in the process of setting intelligence priorities to ensure that each priority advances a legitimate objective. It then provides that signal intelligence activities may be conducted "only following a determination … that the activities are necessary to advance a validated intelligence priority" and that they are conducted "only to the extent and in a manner that is proportionate" to that priority.

Third, the order's most dramatic innovation is the creation of a new redress mechanism. This two-tier process directs the CLPO to receive and investigate complaints, creating a complete record of the investigation at its conclusion. The CLPO is empowered to direct agencies to remedy any violations (including destroying improperly collected information) and is granted independence when performing these functions. Importantly, the order establishes a Data Protection Review Court within the Department of Justice, composed of experts from outside government who are guaranteed independence and have binding authority to direct agencies to remediate violations.

This process neatly addresses the twin challenges involved with judicial redress: standing and secrecy. Claimants must provide certain information to the CLPO in submitting their complaints but need not show that they have been the targets of surveillance. In addition, the CLPO and the DPRC will have full access to classified information to carry out their activities.

Interestingly, in a reversal of what our foreign partners have previously expressed concerns about, this is a redress process where non-U.S. persons may enjoy greater access than U.S. persons. The mechanism applies to data that has been transferred to the U.S. from a "qualifying state" (presumably a member state of the European Union). While there is no nationality limitation, if an American who has not traveled abroad wishes to submit a claim, they will not be able to avail themselves of this process.

Oversight—A system of many layers with many players

It is not enough to have rules. Particularly for secret intelligence, oversight is a vital element of the national security legal framework. In the U.S., we have what I like to call a system of many layers with many players. Within the executive branch, agencies have civil liberties and privacy offices, office of general counsel, compliance organizations, and offices of inspectors general. The Department of Justice provides granular oversight over FISA, shapes EO 12333 procedures, and serves as the chief legal officer of the executive branch. In addition, the Intelligence Oversight Board receives and assesses reports from the IC of potential violations of laws, executive orders, and directives.

A key oversight institution is the Privacy and Civil Liberties Oversight Board (PCLOB), which provides advice and oversight regarding counterterrorism and other activities (such as those relating to Executive Order 14086). This is an independent agency composed of a full-time chair and four part-time members from outside government. It published a landmark report on Section 702 which is cited to this day (*see, e.g.*, *United States v. Hasbajrami*, 945 F.3d 641, 649 n.4 (2d Cir. 2019) (noting that its discussion of Section 702 "is drawn in large part" from the PCLOB report)). I had the privilege of working closely with the Board in its various iterations during my tenure and am a strong believer in the vital oversight role that it plays.

As discussed above, Congress and the FISC also conduct vital oversight; I will not reiterate their roles here.

Intelligence Transparency

I end this whirlwind tour of key developments with the subject of intelligence transparency, something that I was privileged to work extensively on during my time at the ODNI. Early on, I realized that we needed to enhance transparency. According to a Wall Street Journal profile on me in April 2006: "'One of the things I've tried to champion is finding ways to draw the circle around the secret a little more tightly,' says Mr. Joel. By doing that, he says, there are things related to a program that can be discussed to ameliorate concerns without giving up its essence." I was not alone in this view in the IC, but dramatic progress came only after the Snowden disclosures in 2013. The crisis of confidence that ensued prompted the IC to launch a far-reaching transparency initiative, one that continues to bear fruit to this day. We adopted the

Principles of Intelligence Transparency for the IC, followed up with an implementation plan, established IC on the Record as a platform to post documents about our surveillance authorities, worked with FOIA offices to lean forward on releasing requested records with fewer and fewer redactions, created transparency reports, and released large amounts of information about Section 702 as well as about other intelligence activities (some of which are posted in the "Intel Vault").

During my time at ODNI and in my work since then, I have engaged with national security officials from around the world. Many countries have made important strides in enhancing transparency, but I can confidently say that this is an area where the United States continues to lead the way.

Where do we go from here?

Looking back, I see a resilient and flexible framework that sustained shocks to the system and adapted to change. I am proud of that framework and the role I played in it. That said, it is not perfect. Our framework faces the same fundamental challenge that all laws and policies face: it is, in essence, reactive rather than proactive. It can dynamically respond to a crisis but does not readily anticipate change. As a result, we have a framework shaped by prior events—momentous ones, to be sure—more so than mindfully designed for the future.

And more change is coming, that is certain. Technological advances far outpace the ability of our legal system to keep up. Threats morph with increasing speed. New opportunities bring new risks. What to do? I do not believe there is a single magical answer. There are, however, several practical steps we can take right now that will better position the system to both authorize and constrain the intelligence agencies in a time of constant change.

Invest

As stated at the beginning, a legal framework must both authorize and constrain. But that framework is not self-sustaining. One cannot write a rule, flip a switch, and then move on. The rule needs to be interpreted, understood, and followed. The rule, to be effective, requires investment, both in its creation and its ongoing implementation. And that investment must bear a relationship to the scope of activity that is subject to that rule.

In one of its lesser-known recommendations, the Church Committee called for the strengthening of the roles of general counsels at inspectors general as a safeguard against illegality and abuse (p. 332). But other organizations play a key role in the multifaceted task of ensuring that rules are properly designed, interpreted, and followed. These include privacy and civil liberties offices, compliance organizations, and oversight bodies such as the Privacy and Civil Liberties Oversight Board. In my experience, these entities are staffed with highly dedicated and expert professionals, but they are substantially under-resourced. The impact they have on enhancing the trust that is so necessary for agencies to do their work cannot be underestimated and requires a corresponding investment.

The same is true for transparency. A relatively small number of professionals must work to meet FOIA requests, conduct obligatory declassification reviews, and surge limited resources on an ad

hoc basis to review and release information of pressing public interest (e.g., Section 702 reauthorization). The overclassification problem is widely recognized, and the burden on declassification and release officials is increasing exponentially with the explosion of records that is the inevitable byproduct of the digital era. The key task of transparency requires significant new investments in both people and technology.

How does this help cope with change? It may be impossible to predict exactly what will come at us in the future, but we can predict that we will need to constantly adapt. It is, therefore, imperative that we have a well-resourced framework with dedicated and trained professionals ready to assess and adjust as change comes our way.

Align Roles

A system of many layers with many players can be robust and comprehensive, as I believe ours is, but can also create unnecessary friction and complexity, especially when new circumstances arise that challenge settled ways of handling issues. The roles of the various players (e.g., the Intelligence Oversight Board vis-à-vis the Privacy and Civil Liberties Oversight Board) should be studied and adjustments made to avoid unnecessary overlap and ensure comprehensive coverage.

Update and Harmonize Rules

This is a never-ending process that we must recognize as such. This means that as new legal documents are created, we must take care to ensure that they will stand the test of time. Where possible, they should be technology neutral, and should apply across a range of related activities. To the extent different agencies and mission domains are involved, the rules should be consistent in goals, principles, and terminology. Processes should be put in place to monitor how well those rules work for their intended purposes given constantly changing circumstances.

These rules should not be developed in closed silos, but rather should emerge after robust engagement and consultation within and outside of government. This not only includes interagency discussion, but crucially, also includes engagement with civil society and international partners.

In a world tied closely together by technology, where national security activities can intrude on the privacy of people around the world, it is more important than ever to develop a common understanding among like-minded democracies of what the legal framework should authorize and what it should constrain. The Organization for Economic Cooperation and Development has already taken the most important first step, adopting in December 2022 the Declaration on Government Access to Personal Data held by Private Sector Entities. This effort involved the hard work of data protection and national security officials from member countries, coming together over many months to work out the principles their legal frameworks hold in common for law enforcement and national security access to personal data in private sector hands.

First Principles

How to achieve all this? Start with first principles. Or, more practically put, "first, start with principles." Reach a general understanding of key principles, and then move out from that core to develop and update the rules, oversight, and transparency necessary to carry out those principles. This is the model we followed with transparency, which has stood the test of time. We started with the transparency principles, followed with an implementation plan, ensured we had buy-in at all levels, and based our work on carrying out those principles.

These principles should include technology neutrality; the need for consistency, clarity, and broad coverage; a recognition that the enormous volumes of data in today's digital age must be treated with great care; effective redress mechanisms; and an unwavering commitment to the protection of privacy and the promotion of transparency.

Ultimately, we must invest the time, energy, and resources necessary to ensure we have a legal framework that is both robust and flexible enough to adapt to change.

The views expressed in this publication are the author's and do not imply endorsement by the Office of the Director of National Intelligence, the Intelligence Community, or any other U.S. Government agency.