Gathering Intelligence: Drifting Meaning and the Modern Surveillance Apparatus

Diana Lee, Paulina Perlin, & Joe Schottenfeld*

Introduction – Clapper's Library

Days after the Edward Snowden disclosures revealed the staggering scope of U.S. foreign intelligence surveillance, James Clapper, then Director of National Intelligence, sat down for an interview in which he attempted to reduce lingering uncertainty about the Intelligence Community's surveillance programs and practices. "A metaphor [that] I think might be helpful for people to understand this," Clapper explained, "is to think of a huge library with literally millions of volumes of books in it, an electronic library."[1] As Clapper described it, the library includes an unknown but enormous amount of internet traffic; like most libraries, only people with permission are allowed to view and make use of its contents.[2]

But unlike a real library, Clapper's electronic library contains information that is often the most private and immediate to ordinary individuals.[3] Rather than library-goers retrieving books, there are NSA analysts who are able to access and use this information. Where a real library has basic rules that are fairly transparent, the electronic library has intricate and labyrinthine procedures that determine what information is obtained, and how and when it can be combined – one of the most complex and sensitive facets of the U.S. intelligence framework. Further complicating Clapper's metaphor, there is not just one labyrinth of procedures. There are many. Over time, intelligence agencies have crafted their own internal manuals to guide and regulate intelligence gathering. These versions contain different definitions of the technical words that define the appropriate bounds of intelligence gathering. By focusing on when intelligence gathering begins – and, consequently, on three terms in these manuals: "collection," "acquisition," and "targeting" – we argue that three forces account for much of the structure of this system: discretion, dispersion, and drift.

Discretion refers to the wide latitude Executive Order 12333 affords to the executive to conduct foreign surveillance activities. Foreign signals intelligence, or

---

* Herbert J. Hansell Fellows at the Yale Center for Global Legal Challenges and J.D. Candidates at Yale Law School, class of 2019. Our deepest thanks to Oona Hathaway and David Kris for their guidance and input. We are also grateful to Laura Donohue, Timothy Edgar, Elizabeth Goitein, and our fellow students in Professor Hathaway's International Law & Foreign Relations seminar for their time and feedback.

1. Interview by Andrea Mitchell with James Clapper, Director, Office of Dir. of Nat'l Intelligence (June 8, 2013), https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2013/item/874-director-james-r-clapper-interview-with-andrea-mitchell.

2. *Id.*

3. *See* James Glanz, Jeff Larson & Andrew W. Lehren, *Spy Agencies Tap Data Streaming from Phone Apps*, N.Y. Times (Jan. 27, 2014), https://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html.

intelligence derived from electronic signals,[4] is constrained in at least one of two ways: by statutory authorization under the Foreign Intelligence Surveillance Act (FISA)[5] or by Executive Order 12333.[6] FISA and the 2008 amendments to the Act[7] apply to certain, specified facets of foreign intelligence activities, particularly those that affect U.S. persons.[8] Where FISA and its amendments apply, government surveillance is subject to limited judicial review. Everything else falls solely under Executive Order 12333 and the executive branch's broad ambit.

As a result, for the past forty years, as technology has changed to permit surveillance of a scope previously unimaginable, various components of the executive branch have revised and adapted the guidelines governing intelligence activities. Under Executive Order 12333, executive intelligence agencies have defined the key terms of surveillance,[9] established the compliance procedures regulating the foreign intelligence cycle,[10] and actually implemented surveillance practices.

Over time, the *dispersal* of power across the Intelligence Community (IC) has enhanced executive discretion.[11] Executive Order 12333 provides that each agency head "shall issue appropriate procedures and supplementary directives consistent" with the order's broad mandate.[12] During the past several decades, in accordance with Executive Order 12333, members of the Intelligence Community have each created and revised internal manuals to guide their foreign intelligence operations.

Dispersal has empowered particular actors: agency heads, the Attorney General, the Director of National Intelligence, and, at times, the President. Executive officials wield tremendous influence in determining the regulation of U.S. intelligence-gathering activities. Their seemingly minor alterations to often classified agency documents can significantly alter the structure and scope of U.S. surveillance. As we show, agencies have recently changed the definitions of technical terms, such as "collection," that are integral to determining the official commencement of intelligence gathering. In metaphor and reality, this is

4. *Signals Intelligence*, NAT'L SECURITY AGENCY (May 3, 2016), https://www.nsa.gov/what-we-do/signals-intelligence/.

5. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62 (2012)).

6. Exec. Order 12333, 3 C.F.R. § 200 (1982), as amended by Exec. Order No. 13284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No 13455, 69 Fed. Reg. 53593 (Aug. 27, 2004), Exec. Order No. 13470, 73 Fed. Reg. 45325 (Aug. 4, 2008) (reprinted as amended in 50 U.S.C. § 401 (2011)).

7. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2438 (2008) (codified as amended at 50 U.S.C. § 1881a).

8. *See infra* Section I.D.

9. *See infra* Part III.

10. *See infra* Part II.

11. *See, e.g.*, Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 651-58 (2016) (arguing that intelligence gathering is "[w]eakly [p]residentialized," as compared, for example, to covert action).

12. Exec. Order 12333, *supra* note 6, § 3.2.

Clapper's library – its contents are not only used, but determined by the intelligence agencies themselves.

Together, discretion and dispersal have wrought *drift* in the guidelines adopted by intelligence agencies.[13] The meanings of essential words, like "collection," vary considerably as executive actors define them. While the laws and regulations governing surveillance warn that the lay meanings of words may no longer apply,[14] the technical definitions of these terms are often neither clear nor fixed, changing both within and across agencies over time.

This variance in terminology is not just a matter of semantics. Agency terms such as "collection" determine the extent of the executive's intelligence-gathering authority – *when* surveillance, from the government's perspective, begins, and *which restrictions*, Executive Order 12333's or FISA's, apply.[15] Discretion, dispersal, and drift make it difficult to identify these boundaries. Few, either in Congress or the general public, are aware of the complex procedures governing foreign intelligence gathering, much less understand the technical definitions given to the terms that are used. This complexity, in turn, hinders democratic accountability, strains internal oversight, and even works against efforts by executive actors themselves to reform oversight.[16]

Since Snowden disclosed the U.S. government's secret surveillance programs in 2013, scholars and civil liberties advocates have called upon the government to strengthen and re-conceptualize the oversight regime governing its intelligence activities.[17] Indeed, agency officials themselves have recognized the necessity of

---

13. By "drift," we refer specifically to the shifting meaning of terms in agency manuals and not to the "bureaucratic drift" that political scientists have documented extensively. *See, e.g.*, Thomas H. Hammond & Jack H. Knott, *Who Controls the Bureaucracy: Presidential Power, Congressional Dominance, Legal Constraints, and Bureaucratic Autonomy in a Model of Multi-Institutional Policy-Making*, 12 L., ECON. & ORG. 119 (1996); Matthew D. McCubbins et al., *Administrative Procedures as Instruments of Political Control*, 3 J. L., ECON. & ORG. 243 (1987). We also do not refer to the "ideological drift" coined by Jack Balkin to describe shifts in the "political valence" underlying certain legal ideas. *See* J.M. Balkin, *Ideological Drift and the Struggle Over Meaning*, 25 CONN. L. REV. 869, 870 (1993).

14. As Clapper said of "collection," "there are honest differences on the semantics when someone says 'collection' to me, that has a specific meaning, which may have a different meaning to him." Interview by Andrea Mitchell with James Clapper, *supra* note 1.

15. *See* JENNIFER GRANICK, AMERICAN SPIES 27-40 (2017); Amos Toh, Faiza Patel & Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, BRENNAN CTR. FOR JUSTICE 15-19 (2016), https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf.

16. A recent report by the Privacy and Civil Liberties Oversight Board captures well the interaction between discretion, dispersal, and drift and the consequences that ensue: "The President issued PPD-28 to establish special requirements and procedures for the conduct of signals intelligence activities. PDD-28 does not define 'signals intelligence activities.' Nor did the ODNI. It was left to each IC element to determine how to apply PPD-28 to its respective activities. As a result, the application varies across the IC." PRIVACY & CIVIL LIB. OVERSIGHT BD., *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence*, 16 (Oct. 16, 2018), https://www.pclob.gov/reports/report-PPD28/ [hereinafter PCLOB Report on PPD-28].

17. *See, e.g.*, Rascoff, *supra* note 11; Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039 (2016); Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027 (2013); Margo Schlanger, *Intelligence*

updating Executive Order 12333's internal agency guidelines. In August 2013, the Privacy and Civil Liberties Oversight Board (PCLOB), a statutorily-created agency charged with providing oversight and advice on the executive branch's counterterrorism activities, wrote to then-DNI Clapper and Attorney General Eric Holder to express its concern that "key procedures that form [Executive Order 12333] guidelines . . . have not comprehensively been updated, in some cases in almost three decades, despite dramatic changes in information use and technology."[18] The Civil Liberties Protection Officer of the Office of the Director of National Intelligence assured the Board that "[t]he [Intelligence Community] has been working closely with the Department of Justice to review and update agency guidelines under EO 12333, as appropriate."[19] In August 2016, the Department of Defense released updated procedures to clarify the definition of key terms in its guidelines. The CIA followed suit in 2017, releasing updated procedures that largely align with those promulgated by the Department of Defense.[20]

The Intelligence Community's recent movement towards greater transparency and interagency coordination confirms the power of discretion, drift, and dispersal to sow confusion in the executive's intelligence-gathering efforts over the past forty years. While the Snowden disclosures have pushed the IC towards greater interagency coordination, these measures are reactive rather than prospective. Future technological changes will necessitate additional revisions to agency procedures.[21] Nothing currently precludes these agencies from falling back on entrenched patterns and failing to revise their guidelines consistently in the future.[22]

Legalism and the National Security Agency's Civil Liberties Gap, 6 HARV. NAT'L SEC. J. 112 (2015) [hereinafter Schlanger, *Intelligence Legalism*].

18. Letter from David Medine, Chairman, Privacy & Civil Liberties Oversight Bd., to Eric Holder, Jr., Att'y Gen. of the United States, and James R. Clapper, Dir., Office of the Dir. of Nat'l Intelligence (Aug. 22, 2013), https://www.dni.gov/files/documents/PCLOB_Letter.pdf.

19. IC ON THE RECORD, *Civil Liberties Protection Officer's Statement Regarding Privacy and Civil Liberties Oversight Board Guidelines Letter* (Aug. 26, 2013), https://icontherecord.tumblr.com/post/59418980452/civil-liberties-protection-officers-statement.

20. *See infra* note 132 and accompanying text. The immediate impetus for the DoD and CIA's updates to these procedures appears to be a provision of the Intelligence Authorization Act of 2015, Pub. L. No. 113-293, § 309, 128 Stat. 3990, 3998, that prohibits the retention of certain non-publicly-acquired U.S. person information for greater than five years, subject to a number of exceptions.

21. *See* Robert Litt, General Counsel, Office of the Dir. of Nat'l Intelligence, Prepared Remarks on Signals Intelligence at the Brookings Institution (Feb. 4, 2015), https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2015/item/1171-odni-general-counsel-robert-litt-s-as-prepared-remarks-on-signals-intelligence-reform-at-the-brookings-institute ("[T]o be effective, our signals intelligence activities have to take account of the changing technological and communications environment. Fifty years ago, we could more easily isolate the communications of our target: the paradigm of electronic surveillance then was two alligator clips on the target's telephone line. Today, digital communications are all mingled together and traverse the globe.").

22. As Timothy Edgar observed, "[t]he fact that a series of massively damaging leaks was needed to achieve such sensible reforms can only be described as a failure of leadership." TIMOTHY EDGAR, BEYOND SNOWDEN: PRIVACY, MASS SURVEILLANCE, AND THE STRUGGLE TO REFORM THE NSA 7 (2017).

We propose alternative solutions that provide a path forward for the Intelligence Community to properly constrain executive discretion, dispersal, and drift. First, we suggest that the executive issue a glossary of terms to standardize vital definitions across agencies. Second, we propose the creation of an external oversight body. Finally, we move outside the executive branch, recommending that Congress act to establish the meanings of key terms and concepts in a more durable way.

The debate over surveillance practices carries on, as demonstrated by the recent reauthorization of Section 702[23] and the questions and controversy surrounding the Foreign Intelligence Surveillance Court,[24] but Executive Order 12333 and the agency manuals that operationalize it remain poorly understood and largely out of sight. They are, however, critical to intelligence gathering.[25] In 2015, the Privacy and Civil Liberties Oversight Board finally proposed to review Executive Order 12333 practices;[26] it has not yet completed its report, leaving much unknown about essential programs and authorities.[27] Although we cannot fill these holes, we hope to chart a vital slice of the intelligence gathering landscape, identify systemic and complicated issues at the agency level, and propose possible avenues for reform. In doing so, we suggest new ways of understanding

23. Dustin Volz, *Senate Passes Bill Renewing Internet Surveillance Program*, REUTERS (Jan. 18, 2018), https://www.reuters.com/article/us-usa-congress-surveillance/senate-passes-bill-renewing-internet-surveillance-program-idUSKBN1F72JX.

24. *See, e.g.*, Daniel S. Alter, *The Nunes Memo Attacks the Legitimacy of the Foreign Intelligence Surveillance Court. It Should Act to Repair that Damage*, TIME (Feb. 6, 2018), http://time.com/5135266/nunes-memo-foreign-intelligence-surveillance-court/ ("The Nunes memo questions 'the legitimacy and legality of certain [Department of Justice] and FBI interactions' with the FISA Court and alleges 'a troubling breakdown of legal processes established to safeguard the American people from abuses related to the FISA process.'").

25. *See, e.g.*, David Kris, *Trends and Predictions in Foreign Intelligence Surveillance*, HOOVER INST. 2 (Aegis Paper Ser. No. 1601, 2016), https://www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf ("With one possible exception, concerning Executive Order 12333, [potential reforms] concern only incremental change and fit comfortably within existing legal and policy paradigms; although important, they are unlikely to have a profound effect on security or privacy.").

26. *See* Benjamin Wittes, *PCLOB Takes on Executive Order 12333 Surveillance*, LAWFARE BLOG (Apr. 9, 2015, 8:31 AM), https://www.lawfareblog.com/pclob-takes-executive-order-12333-surveillance (citing the PCLOB's statement that the "Board plans to issue a public report that explains [Executive Order 12333] at a high level, focusing on how the legal framework established by the executive order and its implementing procedures governs the collection, use, retention, and dissemination of information concerning U.S. persons.").

27. The PCLOB's report on Executive Order 12333 was stalled by the resignation of Chairman David Medine in 2016 and subsequent departure of two Board members in January 2017, depriving the Board of a quorum. The PCLOB regained a quorum in October 2018 after the Senate confirmed Chairman Adam Klein and Board Members Edward Felten and Jane Nitze. PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, *New PCLOB Board Members Release Joint Statement* (Oct. 18, 2018), https://www.pclob.gov/newsroom/2018/10/18/Board-Members-Release.html. In its budget request for Fiscal Year 2019, the PCLOB stated that it "will continue its extensive examination of [Executive Order 12333], focusing on in-depth examinations of two specific counterterrorism activities—one at the National Security Agency . . . and one at the Central Intelligence Agency." PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, *Fiscal Year 2019 Budget Justification*, 16 (2018), https://www.pclob.gov/library/CBJFY19Final.pdf.

how executive processes both determine and obscure the boundaries of intelligence activity and hinder transparency.

This Article proceeds in five parts. In Part I, we provide a brief history of Executive Order 12333 and the statutory landscape of the United States' surveillance architecture; we also describe the critical differences between the statutes and the executive order. The Foreign Intelligence Surveillance Act and the 2008 FISA Amendments Act not only govern certain, substantive aspects of foreign intelligence surveillance, limiting what is left to the responsibilities created by Executive Order 12333 – they instill a degree of clarity into the entire surveillance architecture that is absent from portions that fall under Executive Order 12333 guidance. In Part II, we introduce the agency manuals that implement Executive Order 12333 and examine the process whereby they may be altered and changed; in doing so, we demonstrate the dispersion of authority across the executive branch and show how actors within the executive branch are able to revise essential procedures, largely without notice. In Part III, we explore how these manuals have grappled with the key terms associated with the question of when surveillance begins; since the issuance of 12333, different elements of the IC have adopted specific understandings of when intelligence gathering begins that do not always cohere. In Part IV, we discuss reasons why political actors must reform the current process for updating and clarifying agency manuals. Although some executive- and legislative-led efforts have generated greater conformity in the guidelines, these efforts have not been consistent enough to solve the problem. Moreover, though some may argue that there are valid reasons for definitional inconsistency, we argue that circumstances specific to national security make the problem we describe particularly worrisome. Finally, Part V addresses what we see as the best means of injecting clarity into the 12333 guidelines.

I. THE ORIGINS AND EVOLUTION OF EXECUTIVE ORDER 12333

President Ronald Reagan issued Executive Order 12333 in 1981 to establish a framework for gathering intelligence on "the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents."[28] The third in a line of executive orders governing foreign intelligence activity, Executive Order 12333 affirmed that the executive branch would retain significant control over the foreign intelligence landscape.

This Part provides a brief history of foreign intelligence gathering and the development of the legal frameworks governing this activity, reviews the history of Executive Order 12333, and describes the order's relation to the general structure of intelligence authorities. The Snowden disclosures have only recently caused surveillance to capture the public's attention, but the problems of dispersal, discretion, and drift that afflict intelligence gathering under Executive Order 12333 today are tied to the framework that was established at its origins.

28. Exec. Order 12333, *supra* note 6, pmbl.

A. The Consolidation of Executive Foreign Intelligence Authority

Executive power has long been in tension with the practical difficulty of making executive efforts across the intelligence apparatus cohesive. As David Kris and J. Douglas Wilson explain, efforts to create consistency are "necessary – and difficult – principally because the President's power in this area, originally vested in him under Article II of the Constitution, has been dispersed among several different entities within the federal government."[29] Or, as Samuel Rascoff puts it, the Intelligence Community does not "march[] in lockstep with the White House."[30]

The modern intelligence community began to take shape in the form of the National Security Act of 1947, which Congress enacted "to provide a comprehensive program for the future security of the United States; [and] to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security."[31] Generally, the Act aimed to "coordinate" and "centralize" emerging U.S. intelligence efforts to better manage the Cold War threat.[32]

The Act took several steps to consolidate executive power over the burgeoning intelligence landscape that had emerged during World War II. First, it placed the Army, Navy, and Air Force under the single authority of the Secretary of Defense.[33] Second, the Act created a National Security Council (NSC) to advise the President on "the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the national security."[34] Third, the Act created the Central Intelligence Agency (CIA) and established the position of Director of Central Intelligence to oversee not just the CIA, but the Intelligence Community in general.[35] Today, the Director of National Intelligence (DNI), a position created in December 2004, has largely taken on the latter role.[36]

Although the National Security Act made some headway in consolidating intelligence-gathering power, it did not provide lasting, formal constraints on the newly formed Intelligence Community for at least three reasons. First, many of

29. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 1.2 (2d ed. 2012).

30. Rascoff, *supra* note 11, at 636.

31. National Security Act of 1947, Pub. L. No. 80-253, § 2, 61 Stat. 495, 495 (current version at 50 U.S.C. § 3021 (2012)).

32. RICHARD A. BEST, JR., CONG. RESEARCH SERV., RL32500, PROPOSALS FOR INTELLIGENCE REORGANIZATION, 1949-2004 (2004).

33. KRIS & WILSON, *supra* note 29, § 1:2.

34. Pub. L. No. 80-253, § 101(a), 61 Stat. 495, 496 (current version at 50 U.S.C. § 3021(b) (2012)). In practice, however, the NSC's structure has changed, and its power has waxed and waned, depending on each President's preferences and relationship with department leadership. KRIS & WILSON, *supra* note 29, § 1:3.

35. KRIS & WILSON, *supra* note 29, § 1:4.

36. *Id*.

the positions the Act created to consolidate power had little authority of their own. For example, the composition of the NSC has been historically subject to the prerogatives of each presidential administration.[37] Second, the Director of Central Intelligence had little budgetary control with which to enforce management decisions over the Intelligence Community.[38] Third, although already large in 1947, the size of the Intelligence Community has ballooned since the Act's enactment.[39] As a result, the weak structure created by the Act could not fully respond to the Intelligence Community's aggressive growth.

Indeed, in 1949, the Commission on Organization of the Executive Branch, chaired by President Hoover, issued a report on national security organization finding that the "National Security Organization, established by the National Security Act of 1947, is soundly constructed, but not yet working well."[40] The report criticized uncooperative tendencies among departments and recommended consolidation of intelligence power under the CIA. More than fifty years later, at the time that the DNI was established in 2004, a report to the President commented on the difficulties of the new office's mandate:

> The new intelligence law makes the DNI responsible for integrating the 15 independent members of the Intelligence Community. But it gives him powers that are only relatively broader than before. The DNI cannot make this work unless he takes his legal authorities over budget, programs, personnel, and priorities to the limit. It won't be easy to provide this leadership to the intelligence components of the Defense Department, or to the CIA. *They are some of the government's most headstrong agencies. Sooner or later, they will try to run around – or over – the DNI. Then, only your determined backing will convince them that we cannot return to the old ways*.[41]

These concerns over cooperation have persisted into the present day. As we elaborate in Part III, the dispersion of power to make decisions within each intelligence agency continues to enable discretion throughout the executive branch, with significant consequences for the conduct of foreign intelligence.[42]

---

37. *See id.* § 1:3 (noting that "the NSC has been a flexible institution, responding to the preferences of individual Presidents").

38. *Id.* § 1:5; *see also* Ctr. for Study of Intelligence, *Central Intelligence: Origin and Evolution*, CIA 7-8 (Michael Warner ed., 2001), http://www.dtic.mil/dtic/tr/fulltext/u2/a500075.pdf ("The DCI never became the manager of the Intelligence Community, his Agency never won the power to 'inspect' the departments' operational plans or to extract community-wide consensus on disputed analytical issues, and CIA never had authority over all clandestine operations of the US government.").

39. BEST, *supra* note 32, at 1.

40. *Id.* (quoting COMM'N ON ORG. OF THE EXEC. BRANCH OF THE GOV'T, TASK FORCE REPORT ON NATIONAL SECURITY ORGANIZATION, Appendix G, 3 (Jan. 13, 1949)).

41. Comm'n on the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction, Letter of Transmittal for the Report of the Commission 2 (Mar. 31, 2005) (emphasis added), *quoted in* KRIS & WILSON, *supra* note 29, § 1:5.

42. As Rascoff asserts, "a decentralized intelligence community that has proved adept at empire building and has been largely unconstrained by the political executive has revealed itself to be profoundly vulnerable to questionable intelligence-gathering practices." Rascoff, *supra* note 11, at 636.

B. Executive Order 12333's Origins

Although the National Security Act sets forth the overarching structure in which the Intelligence Community operates, Executive Order 12333, along with FISA and various directives, largely determine the scope of the IC's roles and responsibilities. In order to understand how executive dispersion has affected Executive Order 12333's implementation in the current era, we must first understand the order's origins – why it emanates from the executive branch and how it relates to congressional action in the intelligence-gathering arena.

Executive Order 12333 emerged from a "crisis of confidence" in the federal government's intelligence agencies.[43] In the early 1970s, media reports disclosed a series of domestic abuses by the FBI and CIA. The Nixon administration had interpreted a provision of the 1968 Omnibus Crime Control and Safe Streets Act[44] to permit the "conduct [of] extensive wiretapping and other forms of electronic surveillance of U.S. citizens without probable cause or prior judicial approval."[45] In 1973, the *New York Times* reported that the CIA had pursued a "massive, illegal domestic intelligence operation . . . against the antiwar movement and other dissident groups in the United States," including "break-ins, wiretapping, and the surreptitious inspection of mail."[46]

In response to these revelations, Congress formed a Senate committee to review the government's intelligence activities, commonly referred to as the Church Committee after the committee's chair, Senator Frank Church.[47] The Church Committee investigated federal intelligence agencies during 1975 and 1976 and found that the CIA had repeatedly spied upon American citizens within the United States.[48] According to one account, the agency's operation "CHAOS had amassed some 10,000 intelligence files on American citizens and groups and

---

43. This phrase is borrowed from President Carter's speech addressing the nation's deep moral and spiritual crisis arising from its economic troubles. President Jimmy Carter, Address to the Nation on Energy and National Goals (July 15, 1979), http://www.presidency.ucsb.edu/ws/?pid=32596.

44. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (current version at 18 U.S.C. § 2511 (2012)).

45. SURVEILLANCE IN AMERICA: AN ENCYCLOPEDIA OF HISTORY, POLITICS, AND THE LAW 174 (Pam Dixon ed. 2016).

46. Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES (Dec. 22, 1974), https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html; *see generally* KRIS & WILSON, *supra* note 29, §§ 2:1-2:7.

47. *See* S. Res. 21, 94th Cong. (1975) (establishing a "select committee of the Senate to conduct an investigation and study of governmental operations with respect to intelligence activities and of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government"), https://www.senate.gov/artandhistory/history/common/investigations/pdf/ChurchCommittee_SRes21.pdf.

48. Among other activities, the CIA had run covert chemical and biological experiments on Americans, secretly inspected American citizens' mail, and implemented a secret intelligence operation that, though originally directed towards "anti-American foreign elements," eventually broadened to encompass the "domestic activities of Americans protesting the Vietnam War." *Executive Order on Intelligence Activities: Hearing Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 97th Cong. 12 (1981) (statement of Hon. Frank Church, former U.S. Senator from Idaho).

indexed 300,000 names of Americans in CIA computer records, all without establishing the foreign connection for which it . . . presumably searched."[49] But "[p]erhaps the largest electronic surveillance program" in the twentieth century was "conducted by the NSA or its predecessor organizations."[50] The Church Committee reported that from 1974 to 1975, the NSA had "received copies of most international telegrams leaving the United States" in what was "probably the largest governmental program affecting Americans ever undertaken."[51]

Based upon these findings, the Church Committee "proposed a charter for the intelligence community aimed at restricting the intelligence community."[52] Specifically, the committee introduced "ninety-six recommended reforms to the [executive's] intelligence-gathering operations"[53] that would "replace the National Security Act of 1947 with more specific lines of responsibility and authority,"[54] including more "effective Congressional oversight"[55] to curb executive discretion in the foreign intelligence realm. These proposals marked the "dawning of 'intelligence law' and a first-time focus on the President's authority for national security surveillance."[56]

Despite calls to reform the government's intelligence activities, the Church Committee's charter for the intelligence community never got off the ground. Before Congress could act, "President Ford quickly sought to displace [the committee's] proposals by issuing Executive Order 11905, which implemented many of the Church Committee recommendations."[57] In addition to establishing a "lengthy list of restrictions on intelligence activities," Executive Order 11905 attempted to facilitate interagency cohesion by "encourage[ing] the DCI to devote more energy to the supervision and direction of the Intelligence Community."[58] Because Executive Order 11905 addressed the primary issues identified by the Committee, the Committee's most ambitious legislative proposals withered thereafter.[59]

Subsequent executive orders have adjusted the IC's organization and the scope of its intelligence activities at the President's discretion. In 1978, President

---

49. *Id*. at 15 (statement of Hon. Church); *see also* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 5 (2016).

50. KRIS & WILSON, *supra* note 29, § 2:3.

51. Church Report Book III 765, *quoted in* KRIS & WILSON, *supra* note 29, § 2:3.

52. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 34 (2000).

53. Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 61, 79 (2014).

54. Banks & Bowman, *supra* note 52, at 34 n.250.

55. S. REP. NO. 94-755, bk. I, at 13 (1976) ("The leaders of the United States must devise ways to meet their respective intelligence responsibilities, including informed and effective congressional oversight, in a manner which brings secrecy and the power that secrecy affords within constitutional bounds.").

56. Banks & Bowman, *supra* note 52, at 34.

57. *Id*. at 35.

58. *Central Intelligence: Origin and Evolution*, *supra* note 38, at 9 (internal quotation marks omitted).

59. *Id*.

Jimmy Carter replaced Ford's Executive Order 11905 with Executive Order 12036. In addition to imposing a number of restrictions intended to protect U.S. persons,[60] the order also attempted to centralize control of the Intelligence Community by vesting in the DCI "full and exclusive responsibility for approval of the National Foreign Intelligence Program Budget."[61]

Three years later, President Reagan replaced Carter's order with Executive Order 12333, the intelligence charter that remains in effect today.

C. Executive Order 12333's Guiding Principles and Structure

As its history suggests, Executive Order 12333 broadly serves as a charter for the U.S. government's foreign intelligence activity. The order contains three notable features. First, Executive Order 12333 lays out the U.S. government's justification for intelligence gathering: to obtain "[t]imely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents" in order to render "informed decisionmaking in the areas of national security, national defense, and foreign relations."[62] The order provides that the executive will balance the "vigorous" and "innovative" pursuit[63] of this "essential information" with the "protection of individual interests" consistent with U.S. law and the Constitution.[64] This balancing act between civil liberties, on the one hand, and foreign intelligence gathering, on the other, suffuses the intelligence law manuals implementing Executive Order 12333.[65]

Second, Executive Order 12333 sets forth the Intelligence Community's structure and responsibilities. In accordance with statutory requirements, the order specifies that the DNI "shall serve as the head of the Intelligence Community" and "act as the principal adviser to the President, to the [National Security Council], and to the Homeland Security Council for intelligence matters related to national security."[66] Section 1.7 delineates the scope of each IC element's duties. The order specifies, for example, that the CIA may conduct foreign intelligence activity "without assuming or performing any internal security functions within the United States," but permits the FBI to gather foreign intelligence

60. For example, the order prohibited the CIA from conducting electronic surveillance inside the United States, and restricted all agencies except the FBI from "conduct[ing] any unconsented physical searches within the United States." Exec. Order No. 11905, 41 Fed. Reg. 7703 (Feb. 18, 1976).

61. *Central Intelligence: Origin and Evolution*, *supra* note 38, at 10.

62. Exec. Order 12333, *supra* note 6, § 2.1.

63. *Id.*

64. *Id.* ("Collection of such information . . . will be pursued in a . . . responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.").

65. *See infra* Sections III.B.2, V.A.

66. Exec. Order 12333, *supra* note 6, § 1.3. In this capacity, the DNI has access to "all information and intelligence relevant to the national security," *id.* § 1.5(a); establishes the "objectives" and "priorities" of the IC, *id.* § 1.3(b); enters into intelligence agreements with foreign powers, *id.* § 1.3(b)(4); and "develop[s] guidelines for how information or intelligence is provided to or accessed" by the intelligence agencies, *id.* § 1.3(a)(2).

within the United States if it is not "otherwise obtainable" abroad.[67] With limited exceptions, Executive Order 12333 also allocates to the NSA exclusive responsibility for collecting, analyzing, and disseminating signals intelligence.[68]

Third, and most importantly for our purposes, Executive Order 12333 authorizes the heads of the IC elements to establish procedures, subject to the Attorney General's approval after consultation with the DNI, governing the collection, retention, and dissemination of information concerning U.S. persons.[69] Although the order identifies broad categories of information that may be gathered and the techniques that the IC may use, intelligence agencies retain significant discretion to determine how and to what extent to gather foreign intelligence.

D. Congressional Action in the Foreign Intelligence Realm

Although Ford's executive order limited congressional interference in the foreign intelligence realm, "Congress did not become quiescent after the failure of charter legislation."[70] In 1978, the same year that Carter issued Executive Order 12036, Congress passed the Foreign Intelligence Surveillance Act (FISA). The Act contains two key characteristics: it delineates permissible physical and electronic surveillance of U.S. persons, and it grants jurisdiction to a Foreign Intelligence Surveillance Court (FISC) to authorize foreign intelligence activity conducted pursuant to the statute.[71]

Intelligence agencies conducting foreign intelligence activity are bound by both Executive Order 12333 and FISA's constraints. FISA's regulatory scope is largely determined by its definitions of electronic surveillance and physical search. To the extent that foreign intelligence activity constitutes FISA electronic surveillance or a physical search, intelligence agencies must comply with the Act's requirements. For example, before conducting electronic surveillance, agencies typically[72] must submit an application to the FISC that specifies the identity of the "specific target of the electronic surveillance,"[73] "each of the facilities or places at which the electronic surveillance is directed,"[74] and "the period of time for which the electronic surveillance is required to be maintained."[75] The

67. *Id.* § 2.3(b).
68. *Id.* § 1.7(c).
69. *Id.* § 2.4; *see also id.* § 1.3(b)(9)(B).
70. Banks and Bowman, *supra* note 52, at 35 n.254.
71. 50 U.S.C. §§ 1803-1805 (2010).
72. FISA permits intelligence authorities to conduct foreign intelligence activity without judicial approval if the activity meets certain specifications. *See, e.g.*, 50 U.S.C. § 1802 (providing that the Attorney General may authorize electronic surveillance without a court order to acquire foreign intelligence information for up to one year if the electronic surveillance is directed solely at "the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers" and "there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party," subject to minimization procedures).
73. 50 U.S.C. § 1805 (c)(1)(A) (2012).
74. § 1805(a)(2)(B).
75. 50 U.S.C. § 1804(a)(9) (2012).

FISC, in turn, issues an order approving the electronic surveillance if the government's application satisfies FISA's requirements.[76] If, on the other hand, the foreign intelligence activity does not trigger FISA's protections, then the Intelligence Community is generally bound only by Executive Order 12333 and its implementing procedures.

This distinction between Executive Order 12333 and FISA is significant, for FISA establishes a complex definition of "electronic surveillance" that excludes significant portions of foreign intelligence activity from its reach.[77] FISA defines "electronic surveillance" as: (1) the intentional acquisition of wire or radio communications sent to or from a U.S. person within the United States;[78] (2) the domestic acquisition of the contents of any wire communications to or from a person in the United States;[79] (3) the intentional acquisition of domestic radio communications;[80] and (4) the installation or use of monitoring devices, such as GPS location trackers and microphones, in the United States.[81] In 2008, Congress amended FISA to permit the Attorney General and the DNI to jointly authorize, for a period of up to one year, the targeting of non-U.S. persons "reasonably believed to be located outside the United States to acquire foreign intelligence information,."[82] The government has relied upon this provision to authorize "the collection, use, and dissemination of electronic communications content stored by U.S. internet service providers (such as Google, Facebook, and Microsoft) or traveling across the internet's 'backbone' (with the compelled assistance of U.S. telecom providers such as AT&T and Verizon)."[83] By contrast, the FISA Amendment Act requires agencies to obtain an individualized FISC order to target a U.S. person "reasonably believed" to be abroad, regardless of whether the acquisition occurs inside or outside the United States.[84]

As these provisions suggest, the extent to which FISA applies to foreign intelligence gathering depends on several factors, including: the location of the target of the surveillance, whether the target is a U.S. person or a non-U.S. person, and the type of communication – wire, radio, or neither – surveilled. FISA's definition

76. § 1805(a).

77. As James Baker, the FBI's General Counsel, has explained, FISA's definition of electronic surveillance "subject[s]" certain types of "collection to [a] statutory regime": "If you change the definition of electronic surveillance so that you can carve out certain types of communication, then somebody else other than the FISA court could approve that. It could be the president; it could be the attorney general; could be somebody down at the FBI office or at the NSA – wherever the determination is made that this is the appropriate official to do [so]." *Spying on the Home Front* (PBS television broadcast May 15, 2017), http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/baker.html (interview with James Baker).

78. 50 U.S.C. § 1801(f)(1).

79. *Id*. § 1801(f)(2).

80. *Id*. § 1801(f)(3).

81. *Id*. § 1801(f)(4).

82. 50 U.S.C. § 1881a(a), (j) (2012).

83. *Section 702: What It Is and How It Works*, CTR. FOR DEMOCRACY & TECH. (Feb. 15, 2017) https://cdt.org/insight/section-702-what-it-is-how-it-works/.

84. 50 U.S.C. §§ 1881b, 1881c.

of "electronic surveillance" would not cover, for example, the acquisition of radio communications between individuals located outside the United States or between an individual in the United States and an individual overseas, provided that a U.S. person is not targeted.[85] Nor would FISA govern the overseas acquisition of stored information, such as address book contacts and draft emails, of non-U.S. persons located outside the United States.[86] These activities would be conducted exclusively under 12333. "Similarly, to the extent that social network information, such as Instagram postings, fall outside FISA's definition of electronic surveillance or stored communications, regardless of whether a U.S. person is located inside or outside the country, collection would be governed by the weaker restrictions of Executive Order 12333."[87] As Laura Donohue and others have noted, this form of surveillance could "potentially yield significant amounts of information," including "e-mail address books for most major webmail companies"[88] that contain "hundreds of millions of contact lists from personal e-mail and instant messaging accounts around the world."[89]

Parsing the overlap between Executive Order 12333 and FISA thus requires close attention to where, how, and against whom surveillance is conducted. Although FISA imposes additional limitations on the government, considerable foreign intelligence activity lies outside the statute's reach and is governed exclusively by Executive Order 12333. Furthermore, although Executive Order 12333 provides a basic framework for what foreign intelligence activity is and is not allowed, the actual implementation of surveillance programs, and the internal oversight and compliance mechanisms that apply, revolve around far more technical considerations by agencies within the executive branch. In the next Part, we explore these technical considerations and trace the dispersal and drift that accompany them.

II. IMPLEMENTING EXECUTIVE ORDER 12333: PRESIDENTIAL GUIDANCE AND AGENCY MANUALS

While Executive Order 12333 serves as a high-level charter for the Intelligence Community's foreign intelligence gathering activities, the guidelines issued by each intelligence agency determine the substance and scope of these efforts. As with any administrative agency's guidance, these manuals provide intelligence agencies with ground-level instructions on how, precisely, to conduct foreign intelligence surveillance. In order to do so, the guidelines must determine the *scope* of foreign intelligence gathering. Yet, despite these manuals'

85. Toh et al., *supra* note 15, at 14.

86. Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 152 (2015).

87. *Id.*

88. *Id.*

89. *Id.* (citing Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html).

importance, little attention has been paid to their substance, as well as the definitional inconsistencies that permeate manuals both within a single agency and across the Intelligence Community.

Much attention has been paid instead to *presidential* efforts at reform. In 2014, for example, President Obama issued Presidential Policy Directive-28 (PPD-28) – an unprecedented step following the Snowden disclosures that aimed to reassure the United States' foreign counterparts of its commitment to protecting the privacy of Americans and foreigners alike. The directive rings with lofty language describing the role of American values in surveillance activities.[90] The equivalent of an executive order,[91] the directive extended protections to foreigners, established new reporting requirements, and signaled greater transparency.[92]

Two years later, the Department of Defense released an updated version of the agency manual that it relies on to implement Executive Order 12333.[93] It did so to little fanfare.[94] But, in many ways, revisions to the manual may have altered U.S. intelligence-gathering practices more concretely than President Obama's more heralded PPD-28.

This Part shows how Executive Order 12333 contemplates and enables executive dispersal by granting agencies a broad ambit to implement the order. We

---

90. For example, the directive states that "[p]rivacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities." PRESIDENTIAL POL'Y DIRECTIVE 28 – SIGNALS INTELLIGENCE ACTIVITIES (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28].

91. Memorandum from Randolph D. Moss, Acting Assistant Att'y Gen., to the Counsel to the President on Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order (Jan. 29, 2000), https://fas.org/irp/offdocs/predirective.html [hereinafter Moss Memo]. Executive orders represent a subset of presidential directives. President Obama, for instance, used a presidential policy directive to begin the process of restoring relations with Cuba. *See, e.g.*, *Presidential Policy Directive on Cuba*, N.Y. TIMES (Oct. 14, 2016), https://www.nytimes.com/interactive/2016/10/14/world/americas/document-Presidential-Policy-Directive-on-Cuba.html. Except "[i]n the event of an attack or threatened attack," executive orders must be published in the Federal Register; other forms of presidential directives may be published, but need not be. 44 U.S.C. § 1505(a)-(c) (2012). Presidents may alter all forms of presidential directives, including executive orders, at any point, but, unless explicitly repealed by presidential action, directives remain in force beyond the end of an administration. *See* Moss Memo, *supra*.

92. For how the directive extends protections to foreigners, see section 2 of PPD-28. *See also* Jack Goldsmith, *Three Years Later: How Snowden Helped the U.S. Intelligence Community*, LAWFARE BLOG (June 6, 2016, 9:32 AM), https://lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community (noting that "PPD 28 does not have sharp teeth and, while it has reportedly been a pain to implement, will not likely have a material impact on U.S. collection practices. Like many post-Snowden reforms, it imposes process and oversight constraints and forces NSA to be more prudent in its collection practices. . . [It also] has the side-benefit that the United States can now proudly and truthfully claim to have the most robust protections for non-citizens of any signals collection agency in the world."). For a more granular review of PPD-28's effects, see the Privacy and Civil Liberties Oversight Board's recent review of the implementation of PPD-28. PCLOB Report on PPD-28, *supra* note 16.

93. DEP'T OF DEF., 5240.01-M, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES FACT SHEET (Aug. 8, 2016), https://www.documentcloud.org/documents/3010006-DOD-Guidelines-Fact-Sheet-08-08-2016-FINAL-1120.html [hereinafter DOD FACT SHEET 5240.01-M].

94. One of the few, if only, places to cover the change was *Lawfare*. *See* Cody M. Poplin, *Pentagon Releases New Procedures for Intelligence Collection*, LAWFARE BLOG (Aug. 10, 2016, 10:35 AM), https://www.lawfareblog.com/pentagon-releases-new-procedures-intelligence-collection.

illustrate this phenomenon by focusing on two federal entities, the Department of Defense and the NSA, and the procedures promulgated by each. Despite congressional and executive efforts to make Intelligence Community programs cohere,[95] the rules and procedures governing foreign intelligence activity today vary throughout the executive branch. This dispersion, in turn, facilitates drift – both across different agencies and temporally within individual agencies – that is critical to the conduct and scope of foreign intelligence surveillance.[96]

A. Executive Order 12333 Delegation

Executive Order 12333 broadly authorizes the Intelligence Community to collect, retain, and disseminate foreign intelligence information. While the order provides the general parameters governing the types of information that may be gathered, as well as the surveillance techniques that agencies may use,[97] the specific rules and procedures that implement these constraints are crafted by the intelligence agencies themselves.

Executive Order 12333 specifies that agencies may conduct foreign intelligence activity only in conformity with procedures developed by each agency head.[98] Intelligence Community elements therefore retain substantial discretion to determine *when* foreign intelligence gathering begins, *how long* communications are retained, and *with which entities* and *in what form* information may be shared."[99] Prior to the implementation of the procedures, the Attorney General must approve the agency procedures, after consultation with the DNI, to ensure compliance with both the executive order and the Foreign Intelligence Surveillance Act.[100]

The agency manuals that emerge from this process provide detailed instructions for how intelligence agencies must interpret the surveillance programs they are allowed to operate and the oversight mechanisms they must establish.[101] The

95. *See supra* Part I.A.

96. *See infra* Part III.

97. For example, intelligence agencies must use "the least intrusive techniques feasible" against U.S. persons, Exec. Order 12333, *supra* note 6, § 2.4, and, with limited exceptions, may not engage in the physical surveillance of Americans abroad on foreign intelligence grounds, *id*. § 2.3.

98. *Id*. § 2.3.

99. As Daphna Renan explains, "[w]hat we have are programs of surveillance, grounded in a range of legal authorities and implemented under parameters that govern collection, access, sharing, use, and retention. These parameters are generally underspecified in the underlying legal authority. Elaborated at the administrative level, they can engage a web of interacting administrative actors," who, in turn, adopt disparate interpretations that "determine[] the scope of the executive's surveillance power." Renan, *supra* note 17, at 1053-55 (internal citation omitted). Renan calls this phenomenon "programmatic surveillance," and is principally concerned with its relationship to conventional Fourth Amendment jurisprudence.

100. Exec. Order 12333, *supra* note 6, § 3.2 ("No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director [of National Intelligence]."); *see also id*. § 2.5 (delegating to the Attorney General the authority "to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act.").

101. The manuals fall into an interesting category of executive issuance. Although they do not go through notice and comment, they may still have more legal force than does, for example, a similar

manuals are both easily changed – at least in comparison to other forms of intelligence regulations like statutes or Executive Order 12333 itself – and the site of intense internal contestation over how to balance intelligence gathering needs and legal and policy requirements.[102]

As a result, bureaucratic stagnation is only rarely punctuated by wholesale change. In theory, an agency's procedures should respond to technological advancements that affect the scope of foreign intelligence gathering. Yet, as David Medine, the Former Chairman of the Privacy and Civil Liberties Oversight Board, wrote in a letter encouraging then-DNI Clapper and Attorney General Eric Holder to update all of the agency manuals, "guidelines . . . have not been updated, in some cases in almost three decades, despite dramatic changes in information use and technology."[103] At the same time, an agency's procedures may be revised and re-released without attracting significant attention. Few outside the Intelligence Community noted the release of the Department of Defense's manual implementing Executive Order 12333 in 2017, or the CIA's release of its own manual in January 2018.[104]

B. Agency Manuals

1. DoD 5240.1-R

The DoD Manual implementing Executive Order 12333 is the consummate example of both the slowness with which manuals are updated, and the consequences of such change. For more than thirty years, the Department of Defense consolidated its procedures for implementing Executive Order 12333 in DoD Manual 5240.1-R.[105] In addition to defining key terms, such as "foreign intelligence" and "collection,"[106] 5240.1-R specified restrictions on intelligence agencies' methods and types of foreign intelligence activity. Procedures 2 through 4, for example, governed the collection, retention, and dissemination of information about U.S. persons, respectively.[107] Subsequent sections imposed limitations on the government's conduct of electronic surveillance, in accordance with FISA,[108]

---

manual from the U.S. Department of Health and Human Services, due to the fact that Section 553 of the Administrative Procedure Act specifically allows foreign affairs materials to carry weight even without passing through notice and comment. 5 U.S.C. § 553(a)(1) (2012).

102. For an example of the process by which Attorney General-approved guidelines governing the National Counter-Terrorism Center's retention of U.S. citizen information were approved, see Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53, 88-92 (2014) [hereinafter *Offices of Goodness*]; *see also* Schlanger, *Intelligence Legalism*, *supra* note 17, at 130-32.

103. Letter from David Medine, *supra* note 18.

104. *See* discussion *infra* Section II.B.

105. *See* DEP'T OF DEF., DIR. 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (Dec. 1982), https://biotech.law.lsu.edu/blaw/dodd/corres/pdf/52401r_1282/p52401r.pdf [hereinafter DoDD 5240.1-R]. DoDD 5240.1-R, in turn, implemented more general guidance in DoD 5240.1 implementing Executive Order 12333 and FISA. https://biotech.law.lsu.edu/blaw/dodd/corres/pdf/d52401_042588/d52401p.pdf.

106. *See infra* Part IV.

107. DODD 5240.1.R, *supra* note 105, §1.1.2.

108. *Id*. at C5.

as well as concealed monitoring,[109] physical searches,[110] and searches and examination by mail.[111] While 5240.1-R outlined procedures in its main text, the DoD also relied on a classified annex to the manual, which contained even more specific guidance governing the conduct of foreign intelligence.[112]

2. DoD 5240.01

During the three decades that 5240.1-R was in effect, the nation witnessed sea changes in the structure of the Intelligence Community, the statutory constraints on Executive Order 12333 imposed by the FAA, and intelligence agencies' technological capabilities.[113] And yet, it was not until August 2016 that the Department of Defense released an updated version of the manual, titled 5240.01.[114]

Like its predecessor, DoD 5240.01 serves two broad purposes: to establish rules protecting civil liberties in accordance with Executive Order 12333, and to authorize intelligence gathering within that framework of protection.[115] To determine how to strike this balance, the manual relies on both the executive order and FISA, and contains procedures governing the collection, retention, and dissemination of information, as well as the conduct of electronic surveillance.[116]

3. USSID 18

Although DoD 5240.01 governs the DoD's subordinate agencies, including the NSA, the NSA also follows its own agency-specific guidelines, compiled in the United States Signals Intelligence Directive 18 (USSID 18). USSID 18 was issued in January 2011, but not officially released to the public until November 2013, following the revelation of its existence as a part of the Snowden leaks.[117] Part of the directive remains classified.

---

109. *Id*. at C6.

110. *Id*. at C7.

111. *Id*. at C8.

112. DEP'T OF DEF., 5240.01-M, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES (Aug. 8, 2016), http://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887 [hereinafter DoD 5240.01-M].

113. *See* DOD FACT SHEET 5240.01-M, *supra* note 93 ("The manual was last issued in 1982. In the intervening decades, there have been significant changes in technology, law, and intelligence practices: The information technology revolution has significantly affected intelligence collection and analysis capabilities and raised new issues regarding privacy and civil liberties.); *see also supra* Part I.D.

114. Not to be confused with "DoD Directive 5240.01," which the Department issued in 2007 and contains high level guidance for intra-agency collaboration and assigns specific roles to Department officials. *See* DODD 5240.1.R, *supra* note 105.

115. DOD 5240.01-M, *supra* note 112, at 1.

116. For example, as the procedure for "electronic surveillance" describes, "[a] Defense Intelligence Component may conduct electronic surveillance for an intelligence purpose in accordance with FISA or [Executive Order 12333] and this procedure." *Id*. § 3.5(a), at 23.

117. The 2011 version replaced one from 1993, underscoring how long the gap may be between versions. *See* NAT'L SECURITY AGENCY, USSID 18, LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES (2011), https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

In general, the manual describes the compliance mechanism that "the NSA uses to ensure that its signals intelligence (SIGINT) operations accord with the Fourth Amendment."[118] On an organizational level, USSID 18 broadly mirrors the updated DoD Manual. The NSA manual contains guidelines that apply to the collection, processing, retention, and dissemination of information. Moreover, USSID 18 contains an annex that incorporates FISA's provisions on electronic surveillance.

In terms of substance, however, DoD 5240.01 and USSID 18 diverge. While the DoD and NSA manuals should, in theory, complement each other, we show below that highly technical and precise definitions of essential words vary across the two.[119] Complicating matters further, DoD 5240.01 and USSID-18 each rely on classified annexes. DoD 5240.01 acknowledges this complexity and openly encourages intelligence officers engaging in surveillance activities to check in with lawyers regularly:

> The authorities governing electronic surveillance are complex and subject to change. This procedure addresses the situations that most frequently arise and, even for those situations, only describes some of the legal requirements. Accordingly, Defense Intelligence Component personnel should seek the guidance of legal counsel when planning and conducting electronic surveillance.[120]

This distinction between the NSA and the DoD's 12333 procedures has particular consequences for the scope of each element's intelligence activity.

III. DEFINITIONAL INCONSISTENCIES

The Intelligence Community's latitude to gather foreign intelligence often turns on how specific terms are defined. As the foregoing demonstrates, in addition to FISA, the NSA relies on a complex assortment of statutes, executive orders, directives, and agency manuals in order to determine where, when, and how it may carry out surveillance activities. These authorities and guidelines, however, ascribe ambiguous and inconsistent definitions to many key terms, which, in turn, determine what legal structures apply. To demonstrate how definitional variances dramatically alter the oversight mechanisms and procedures triggered by foreign intelligence surveillance, this Part focuses on three terms integral to information gathering: collection, acquisition, and targeting.

In the context of foreign intelligence gathering, these terms are ubiquitous, influential, and almost invariably used or defined inconsistently. Sometimes they

118. Jane Chong, *The November NSA Trove VII: The 2011 U.S. SIGINT Directive*, LAWFARE BLOG (Nov. 26, 2013, 1:53 PM), https://www.lawfareblog.com/november-nsa-trove-vii-2011-us-sigint-directive/. As the preface to USSID-18 establishes, "[s]everal themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection . . . to protect the Fourth Amendment rights of U.S. persons." *See* USSID 18, *supra* note 117, § 1.3.

119. *See infra* Part III.

120. DOD 5240.01-M, *supra* note 112, § 3.5(a)(1), at 23.

are treated as terms of art; sometimes they are used loosely. What results is a tangled web, with lingering uncertainty over whether the types of intelligence gathering described fall under the oversight mechanisms established by FISA and Section 702, or the internal oversight of Executive Order 12333. For example, in a joint statement delivered to Congress in 2013, representatives of the Intelligence Community and the section of the Department of Justice charged with overseeing the NSA used all three of the terms in a single sentence in the midst of a discussion of the FISC's potency: "[T]he FISC denied in part the Government's requests [to conduct intelligence gathering] because of its concerns about the rules governing the retention of certain non-targeted Internet communications acquired through NSA's upstream collection."[121]

Jargon-filled as it is, this language is representative of far more than just the technical thicket that shrouds the space of surveillance. As we show below, differing definitions of each of these three terms – collection, acquisition, and targeting – determine what form of authority bounds the intelligence gathering described, with consequences for the oversight and protections that apply.

A. Collection

As a rough heuristic, Executive Order 12333 and PPD-28 refer repeatedly to "intelligence collection,"[122] while FISA and Section 702 rely on "acquisition"[123] to describe the activities governed under each authority. Although "collection" and "acquisition" are often used interchangeably,[124] especially in lay contexts, in the Intelligence Community the former generally includes more activity than the latter. "Collection" may refer to activities beyond "electronic surveillance."[125]

As described below, what qualifies as "collection" is determined not by presidential guidance, but by the implementing manuals of the various agencies that gather information under Executive Order 12333's guidance. And, in the manuals themselves, the definition of the term has varied considerably over time and across agencies.

---

121. *Hearing on FISA Amendments Act Reauthorization Before the H. Permanent Select Comm. on Intelligence*, 112th Cong. 7 (2011) (joint statement of Lisa O. Monaco, Assistant Att'y Gen. for National Security; John C. Inglis, Deputy Director, National Security Agency; Robert S. Litt, General Counsel, Office of Director of National Intelligence), https://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf.

122. The most important use may be in Section 1.7 of Executive Order 12333, which establishes that the Director of the NSA "control[s] signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders." Exec. Order 12333, *supra* note 6, § 1.7.

123. James Baker once said, "[t]he FISA law talks in terms of acquisition of communications, and it differs." Interview with James Baker, *supra* note 77; KRIS & WILSON, *supra* note 29, § 7:9.

124. Toh et al., *supra* note 15, at 4 ("In our view, 'collection,' 'interception,' 'acquisition,' 'gathering,' and 'obtaining' of information all mean the same thing.").

125. For example, "collection" may also refer to gathering human intelligence. A more complicated example: according to DoD 5240.01's definition of collection, "[c]ollected information *includes* information *obtained or acquired* by any means, including information that is volunteered to the Component." DOD 5240.01-M, *supra* note 112, Annex G.2, at 45 (emphasis added).

1. Executive Order 12333

Despite referring repeatedly to "collection," neither Executive Order 12333 nor PPD-28 provides its own definition of the term. Executive Order 12333 establishes that "[i]ntelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President."[126] Beyond this, 12333 contemplates "collection" as one phase of a multi-part intelligence cycle. The responsibilities of the Director of National Intelligence, for example, include "establish[ing] objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective *collection*, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived."[127] Under the order, each director or head of an IC component is to "[c]ollect . . ., analyze, produce, and disseminate foreign intelligence and counterintelligence."[128] This accords roughly with what might be expected: the IC collects information, analyzes that information, and then disseminates the information to relevant actors.

Similarly, and more importantly for our purposes, Executive Order 12333 contemplates three actions that can occur to U.S. persons' information in a manner that would require oversight: collection, retention, and dissemination.[129] Although vague, the framing affirms that, under 12333, collection of information is the first act that triggers oversight.

PPD-28 provides more specific high-level interpretative guidance. The directive establishes four general principles that limit "[s]ignals intelligence collection": that collection be properly authorized by executive order or statute and not violate the Constitution; that collection respect privacy and civil liberties and only occur when there is a "foreign intelligence or counterintelligence purpose"; that foreign trade secrets only be collected for national security purposes; and that collection be "tailored as feasible."[130]

In establishing these principles, PPD-28 employs the term consistently with 12333's use, but, as discussed below, differently from intelligence agencies' procedures implementing the executive order. As a report on Executive Order 12333 issued by the Brennan Center for Justice argues, "PPD-28 deepens the 'collection' conundrum: There is some indication that the Directive relies on the common sense meaning of the word."[131] As a result, the Brennan Center treats

126. Exec. Order 12333, *supra* note 6, § 1.1.

127. *Id.* § 1.3 (emphasis added).

128. In general, the intelligence process under Executive Order 12333 follows the collect-analyze-produce-disseminate framework. *See, e.g.*, *id.* § 1.7 ("The Director of the Central Intelligence Agency shall. . .Collect. . .analyze, produce, and disseminate.").

129. *Id.* § 2.3; *see also*, Letter from David Medine, *supra* note 18, ("Under section 2.3 of the Executive Order, intelligence agencies can only collect, retain, and disseminate information about U.S. persons if the information fits within one of the enumerated categories under the Order and if it is permitted under the agency's implementing guidelines approved by the Attorney General after consultation with the Director of National Intelligence.").

130. PPD-28, *supra* note 90, § 1.

131. Toh et al., *supra* note 15, at 18.

"collection" under the directive as being akin to all forms of "information gathering."

Although Executive Order 12333 and PPD-28 offer a rough sketch of the term, neither provides insight into when, exactly, an agency begins collecting information.

2. DoD Manual

For the most part, the task of defining collection has fallen to the Department of Defense and the NSA, both of which have generated their own specific definitions of the term.[132] In the DoD's case, the definition of collection changed dramatically with the release of DoD 5240.01 in 2016.

The evolution of "collection" in the DoD's parlance provides a meaningful case study for executive components' capacity to interpret 12333 as opposed to FISA or Section 702. Until last year, DoD 5240.1-R, which was released in 1982, provided the most up-to-date public guidance on the Department of Defense's understanding of "collection."[133] The manual established that

> [i]nformation shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component *officially accepts*, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been *processed into intelligible form*.[134]

Under this definition, 5240.1-R requires information to be processed such that it is "intelligible" and "accepted for use" to constitute "collection." "Collection" occurs at a point after the gathering or, for lack of a word that is not a term of art, initial interaction with the information. As the Intelligence Law Handbook characterized this definition of collection, "'collecting" therefore involves 'more than

132. The CIA released an updated version of its "Attorney General Guidelines" in January 2017 ("CIA manual"); its definition of collection is almost an exact replica of that from the DoD's recently updated manual. As defined by the CIA's manual, "[c]ollection means the receipt of information by the CIA for official purposes, whether or not the information is retained . . . not including information that has been disseminated by other elements of the Intelligence Community." CIA, CENTRAL INTELLIGENCE AGENCY INTELLIGENCE ACTIVITIES: PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 §12 (Jan. 18, 2017), https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf [hereinafter CIA INTELLIGENCE ACTIVITIES]

133. There is lingering uncertainty surrounding which version of the manual previously created the backdrop for various agencies' definitions. As the Brennan report notes, "[w]hile [the 1988] version was retracted, the [Intelligence Law] handbook's general point that the definition of 'collection' has a multi-layered and highly technical meaning applies equally to the version of DoD 5240.1-R that is in place today, as discussed *infra*. Moreover, despite the retraction, the NSA's definition of 'collection' under USSID 18 appears consistent with the definition contained in the 1988 directive." Toh et al., *supra* note 15, at 48 n.91.

134. DODD 5240.1-R, *supra* note 105, C2.2.1, at 15 (emphasis added).

"gathering" – it could be described as 'gathering, plus.'"[135] This "plus" allowed the government significant leeway to conduct activities prior to "collection." For example, the requirement that data be rendered intelligible before constituting "collection" would allow the U.S. government to gather encrypted data without having to worry about any of Executive Order 12333's safeguards, such as a limit on the amount of time the data could be stored.[136]

The manual, however, no longer contains that definition. The Department of Defense released DoD 5240.01 in August 2016, formally cancelling much of 5240.1-R other than the classified annex and rewriting the definition of "collection." Whereas in the past, 5240.1-R required information to be "officially accepted" or "processed into intelligible form" to constitute "collection," now, 5240.01 defines "collection" as beginning much earlier:

> Information is collected *when it is received* by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence or other purposes. Collected information includes *information obtained or acquired by any means*, including information that is volunteered to the Component.[137]

The switch to "upon receipt" has considerable practical implications. Consider, for example, the manual's description of procedures to be followed when dealing with the incidental collection of U.S. personal information [USPI]:

> In the course of authorized collection activities, a Defense Intelligence Component may incidentally collect USPI . . . All such information may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with Procedures 3 and 4.[138]

In the context of bulk surveillance, 5240.01's updated definition of collection ensures that these retention safeguards apply far earlier. Previously, under 5240.1-R, "collection" would have occurred long after the actual gathering of the information, presumably meaning that U.S. personal information could have been permanently retained without evaluation.

Although collection under 5240.01 begins earlier, there are still surveillance activities that the term might be expected to cover that fall outside its purview. Under 5240.01, collection explicitly does not include information that only momentarily passes through a computer system of an intelligence component; information on the internet or in an electronic forum or repository outside the

135. DEFENSE INTELLIGENCE AGENCY, INTELLIGENCE LAW HANDBOOK, DEFENSE HUMINT SERVICE, CC-0000-181-95 §§ 3-5 (Aug. 2004), https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf; *see also* Toh et al., *supra* note 15, at 15.

136. Toh et al., *supra* note 15, at 15.

137. DoD 5240.01-M, *supra* note 112, Annex G.2, at 45 (emphasis added).

138. *Id.* § 3.2(d), at 13.

component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner;[139] information disseminated by other Components or elements of the Intelligence Community; or information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes.[140] As a result, even the new definition of "collection" leaves open broad swathes of information that might be gathered or viewed outside of the framework of 12333 and therefore unprotected by any safeguards.

3. USSID 18

Although the NSA is a subordinate agency to the Department of Defense, the new, 2016 DoD definition has not altered the NSA's interpretation as it pertains to information gathering.[141] Prior to the update, the NSA had developed its own definition of "collection," separate from the one established by DoD 5240.1-R.[142] That definition persists through today. According to the DoD Fact Sheet describing 5240.01's release, USSID 18 remains untouched.[143]

USSID 18 defines "collection" as occurring at an even later moment than 5240.1-R: "COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record."[144] What 5240.1-R defines as "collection," USSID 18 instead classifies as "interception": "INTERCEPTION means the acquisition by the [U.S. SIGINT System] through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of the communication into an intelligible form."[145]

This distinction between "collection" and "interception" matches Clapper's library metaphor. As Clapper explained in a 2013 interview, "[G]oing back to my metaphor, what I was thinking of is looking at the Dewey Decimal numbers of those books in the metaphorical library. To me collection of U.S. Persons data would mean taking the books off the shelf, opening it up and reading it."[146] Where 5240.1-R started the "collection" clock when the data is intelligible, and 5240.01 now begins it once the information is received, the NSA appears to

139. Although vague, this may allow members of the IC to monitor forums like chat rooms without having to go through formal oversight mechanisms.

140. DoD 5240.01-M, *supra* note 112, § 3.2(d), at 13 (emphasis added).

141. DoD FACT SHEET 5240.01-M, *supra* note 93. Additionally, DoD Manual 5240.01 establishes that "DoD Component heads may issue implementing instructions for the conduct of authorized missions or functions consistent with the procedures in this issuance. In developing such instructions, the DoD Component heads should consult with their respective privacy and civil liberties officials." DoD 5240.01-M, *supra* note 112, § 2.2, at 7.

142. *See* USSID 18, *supra* note 117, § 9.2.

143. DoD FACT SHEET 5240.01-M, *supra* note 93.

144. USSID 18, *supra* note 117, § 9.2.

145. *Id*. § 9.11; *see also* Toh et al., *supra* note 15, at 16-18.

146. Interview by Andrea Mitchell with James Clapper, *supra* note 1.

require that someone actually be *reading* that data for collection to have commenced.

For now, the NSA's definition under USSID 18 remains intact, with significant implications for when oversight mechanisms kick in for intelligence-gathering activities.

B. Acquisition

In 2014, the Privacy and Civil Liberties Oversight Board convened a public hearing on Section 702 of FISA. In response to the Snowden disclosures, the PCLOB had undertaken an extensive overview of Section 702 and agreed to prepare a public report on programs operating under that provision.[147] During the hearing, the Board asked Rajesh De, then General Counsel of the FBI, to explain his use of the terms acquisition and collection. De responded:

> There's no parsing between acquisition or collection. So there are some theories out there that when the government receives the data it doesn't count as collection or acquisition. That is incorrect. Acquisition and collection *for these purposes* are the same thing.[148]

De's explanation, though clarifying in its context, does not shed much light on the ambiguous picture presented by FISA, Executive Order 12333, and the agency manuals. Indeed, in the context of the question presented and the hearing itself, De's reference to "these purposes" appeared to limit his response to the NSA's understanding of these terms under Section 702. Moreover, the PCLOB hearing did not clarify the meaning of "acquisition" itself, a term that neither FISA nor Executive Order 12333 and DoD 5240.01 define. This Section examines varying uses of "acquisition" and their relation to "collection" beyond the FAA. While both FISA and agency regulations tend to use acquisition in the context of FISA electronic surveillance, the definition of acquisition itself is unclear, creating uncertainty as to Executive Order 12333's constraints.

1. Executive Order 12333 and DoD 5240.01

Construed most narrowly, acquisition refers to FISA electronic surveillance. Although FISA, as amended, never explicitly defines acquisition, it exclusively regulates the "acquisition" rather than the "collection" of foreign intelligence. As discussed in Part I, FISA uses acquisition in its complex definition of "electronic surveillance."[149] The FISA Amendments Act refers to "acquisition" similarly: the

147. For the full report *see* PRIVACY & CIVIL LIB. OVERSIGHT BOARD, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

148. PRIVACY & CIVIL LIB. OVERSIGHT BOARD, *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 38 (Mar. 19, 2014) https://www.pclob.gov/library/20140319-Transcript.pdf (emphasis added) [hereinafter *Public Hearing Regarding Section 702*].

149. 50 U.S.C. § 1801(f); *see supra* Part I.D.

Act itself is entitled "An Act to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain *acquisitions* of foreign intelligence, and for other purposes." Notably, neither the original nor the amended statute employs the term "collection" once.

Executive Order 12333 appears to confirm the close connection between acquisition and FISA electronic surveillance. For the most part, the executive order uses "collection" rather than "acquisition," suggesting a distinction between the two terms. However, Executive Order 12333's definition of electronic surveillance uses "acquisition" instead: electronic surveillance is the "*acquisition* of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication."[150] This definition suggests that FISA electronic surveillance and acquisition are intertwined and distinct from 12333 "collection."[151]

As in Executive Order 12333, DoD 5240.01 uses acquisition only in the context of FISA electronic surveillance. DoD 5240.01 defines electronic surveillance as "the *acquisition* of a nonpublic communication by electronic means,"[152] and specifies that "[e]lectronic surveillance is also defined in FISA, and where these procedures reference that definition, FISA should be consulted."[153] Consistent with these provisions, the manual appears to distinguish between Executive Order 12333 collection and FISA acquisition: "This procedure specifies the general criteria governing the *collection* of [U.S. Person Information]. Only paragraphs 3.2f and 3.2g apply to the *acquisition* of information in accordance with . . . the "Foreign Intelligence Surveillance Act (FISA)."[154]

These authorities indicate that "acquisition" signals not only where, when, and against whom intelligence agencies may conduct foreign intelligence activity, but also whether they are constrained by FISA and the FAA. Where agency manuals use "collection" rather than "acquisition," intelligence agencies may understand these activities to fall outside the statute's scope.

2. USSID 18

Although Executive Order 12333 and DoD 5240.01 consistently employ acquisition in the context of electronic surveillance, neither indicates *when* acquisition begins. Unlike 12333 and the DoD manuals, USSID 18 defines "acquisition"; in doing so, the manual demonstrates the ambiguity of acquisition itself.

---

150. Exec. Order 12333, *supra* note 6, § 3.5 (emphasis added).

151. Consistent with this interpretation, Executive Order 12333 expressly incorporates FISA's provisions governing electronic surveillance. *Id*. § 2.5.

152. DoD 5240.01-M, *supra* note 112, at 48.

153. DoD 5240.01-M, *supra* note 112, at 48; *see also id*. at 24 ("A Defense Intelligence Component may conduct electronic surveillance targeting a person in the United States only for foreign intelligence or CI purposes. FISA governs such activities, except in very limited circumstances and in accordance with this procedure.").

154. DoD 5240.01-M, *supra* note 112, at 10 (emphasis added).

USSID 18 at first reiterates 12333's definition of electronic surveillance as the "acquisition" of a "nonpublic communication without the CONSENT of the person who is a party to the communication."[155] The NSA manual also appears to understand "acquisition" to refer to FISA electronic surveillance. Annex A to the manual, which implements FISA, specifies that "[t]hese procedures apply to the *acquisition*, retention, use, and dissemination of non-publicly available information concerning United States persons."[156]

However, USSID 18 also uses "acquisition" and "collection" interchangeably, blurring 12333 and DoD 5240.01's distinctions between the two. For example, Annex A defines "acquisition" as the "*collection* by the NSA of a nonpublic communication to which it is not a party."[157] In another provision, the manual switches the order of the two terms: "The purpose of the COLLECTION is to *acquire* significant FOREIGN INTELLIGENCE information."[158] Whereas the former suggests that acquisition occurs before collection, the latter indicates the reverse.

USSID 18 supports both competing interpretations. For example, the manual prohibits "[s]electing through the use of a SELECTION TERM" communications to, from, or about a U.S. person unless (1) "[t]he COLLECTION is directed against . . . [c]ommunications to or from U.S. PERSONS outside the UNITED STATES"; (2) these individuals have been "approved for targeting in accordance with the terms of FISA"; and (3) the Attorney General has authorized the collection.[159] Under this provision, U.S. person information may only be "collected" through use of a "selection term" if the individual has been "targeted" in accordance with FISA, suggesting that "acquisition" occurs prior to "collection."

By contrast, the manual also provides that "[i]nformation to, from or about U.S. PERSONS *acquired* incidentally *as a result* of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and 6 of this USSID," indicating that the NSA first "collects" information that is subsequently "acquired."[160]

This ambiguity could implicate the scope of the NSA's foreign intelligence activities. Assume, for example, that the NSA adheres to USSID 18's definition of collection as the intentional selection of information from a database – in Clapper's analogy, the physical act of opening and reading a book. If acquisition occurs prior to collection, then FISA's minimization procedures governing electronic surveillance apply before the selection of information from the database. If, however, acquisition occurs after collection, then FISA's more stringent requirements would not apply until a much later stage.

155. *See* USSID 18, *supra* note 117, § 9.7.
156. *Id.* Annex A (emphasis added).
157. *Id.* (emphasis added).
158. *Id.* § 4.1(b)(3) (emphasis added).
159. *Id.* § 4.1(b).
160. *Id.* § 4.3 (emphasis added).

Alternatively, it is possible, and we think likely, that USSID 18 fails to consistently distinguish between "acquisition" and "collection." Unlike DoD 5240.01, which uses acquisition only in the context of electronic surveillance, the NSA manual does not appear to have been crafted with the same level of attention to the definitions of the two terms.

C. Targeting

Intelligence agencies do not just "collect" or "acquire" information. They often conduct "targeted collection" or "targeted acquisition." Like collection and acquisition, targeting provides another lens through which to examine the interaction between Executive Order 12333 and FISA. Poorly defined, targeting assumes a variety of meanings across FISA, Executive Order 12333, and the order's implementing manuals, further complicating when foreign intelligence begins and the scope of the surveillance itself.

1. Targeted Acquisition

FISA does not define "targeting." The statute suggests, however, that "targeting" precedes "acquisition" in the conduct of electronic surveillance. Traditionally, FISA's definition of electronic surveillance refers to information that is "acquired" by "intentionally targeting."[161] Similarly, Section 704 prohibits the government from "intentionally target[ing]" a U.S. person "for the purpose of acquiring" foreign intelligence information.[162] According to the NSA's procedures governing Section 702 surveillance, the NSA "targets" an individual when it "tasks" a selector, such as an email address or telephone number.[163] The information retrieved is considered "acquired" for retention, analysis, and

161. *See, e.g.*, 50 U.S.C. § 1801(f); 50 U.S.C. § 1881a(b).

162. 50 U.S.C. § 1881c(2).

163. *NSA Director of Civil Liberties and Privacy Office Report: NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, NSA 4-5 (Apr. 16, 2014), https://fas.org/irp/nsa/clpo-702.pdf. *See also* Glenn Greenwald & James Ball, *The Top Secret Rules That Allow NSA To Use US Data Without a Warrant*, GUARDIAN (June 20, 2013, 5:59 EST) (according to the NSA's Office of Privacy and Civil Liberties, targeting occurs when: "an NSA analyst [identifies] a non-U.S. person located outside the U.S. who has and/or is likely to communicate foreign intelligence information as designated in a certification. . . .Once the NSA analyst has identified a person of foreign intelligence interest who is an appropriate target under one of the FISC-approved Section 702 certifications, that person is considered the target. The NSA analyst attempts to determine how, when, with whom, and where the target communicates. Then the analyst identifies specific communications modes used by the target and obtains a unique identifier associated with the target—for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address). Next the NSA analyst must verify that there is a connection between the target and the selector and that the target is reasonably believed to be (a) a non-U.S. person and (b) located outside the U.S. This is not a 51% to 49% "foreignness" test. Rather the NSA analyst will check multiple sources and make a decision based on the totality of the information available. If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.").

dissemination. In short, FISA electronic surveillance cannot occur without targeting. All FISA "acquisition" is "targeted."

Executive Order 12333 by contrast, never mentions the word "target," except briefly in a provision unrelated to foreign intelligence gathering.[164] This suggests that "target" is closely linked to FISA acquisition. DoD 5240.01 supports this interpretation. The manual uses "target" exclusively to refer to electronic surveillance.[165]

2. Targeted Collection

"Target," however, has a different meaning in the context of USSID 18, where the term appears to refer to the beginning of collection, not acquisition. Unlike Executive Order 12333, the NSA pins its definition of "targeting" to "collection." In fact, USSID 18's definition of "target" redirects readers to "collection."[166] As explained above, the NSA manual defines collection as the "intentional tasking or SELECTION" of information for "subsequent processing."[167] USSID 18 defines "selection" as "the intentional insertion of a [redacted] telephone number, email address, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing."[168] Read together, these definitions suggest three features of "targeting."

First, "targeting" involves some form of selection, although it is not clear what precisely selection entails.[169] Unlike Executive Order 12333 and FISA, the NSA's definition of collection implies that selection occurs *after* data has already been gathered. However, the NSA's Supplemental Procedures to USSID 18, developed in response to PPD-28, state that "[w]henever practicable, collection [of non-US persons' information] will occur through the use of one or more SELECTION TERMS in order to focus the collection on specific foreign intelligence targets . . . or topics."[170] This phrase implies that selection can occur before "collection" as well. The NSA's manual thus confounds when selection must occur for foreign intelligence gathering to qualify as "targeted," adding temporal ambiguity to uncertainty over what specifically "selection" entails.

---

164. Exec. Order 12333, *supra* note 6, § 2.3(d).

165. *See, e.g.*, DOD 5240.01-M, *supra* note 112, § 3.5(c), at 24.

166. USSID 18, *supra* note 117, § 9.16.

167. *Id.* § 9.2.

168. *Id.*

169. While part of the definition is redacted, the NSA seems to define "selection" more narrowly than the DoD, focusing, for example, on telephone numbers and email addresses instead of entire countries or agencies.

170. U.S. NAT'L SECURITY AGENCY, USSID SP0018: SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF NON-UNITED STATES PERSONS § 4.2 (Jan. 12, 2015), https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/assets/files/PPD-28.pdf.

Second, USSID 18's definition explicitly ascribes intent to "targeting." In other words, for information gathering to be "targeted," the government must introduce selection terms on purpose. While this point may be somewhat obvious, USSID 18 is the only authority that makes it explicit.

Finally, by requiring "collection" to be targeted, USSID 18 substantially differentiates the meaning of "collection" from how PPD-28 defines it. As we discuss below, PPD-28 refers to "bulk collection" – impossible in the NSA's phrasing. It thus becomes even more important to understand how the NSA defines "collection" in light of post-2014 changes to other legal sources.

3. Bulk Collection

Information collected under 12333 and not FISA may be gathered in "bulk." PPD-28's attempt to define the limits of bulk collection further complicates the meaning of targeting. Assuming a dichotomy between "bulk" collection and "targeted" information gathering, a footnote in PPD-28 suggests that "targeting" involves selection prior to "acquisition": "References to signals intelligence collected in 'bulk' mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g. specific identifiers, selection terms, etc.)."[171]

This language implies that unlike collection in "bulk," "targeted" signals intelligence is acquired *with* "the use of discriminants," although the footnote does not clearly define what constitutes a discriminant. A committee convened by the Director of National Intelligence to explore alternatives to bulk collection reached a similar conclusion that "collection is targeted if it is not bulk."[172] However, the committee notes that "PPD-28 defines 'discriminant' only by example, so it does not provide a precise definition of either bulk or targeted collection. Nor are these terms defined precisely anywhere in law or policy."[173]

D. Summary of Terms

As with "collection" and "acquisition," it is problematic that several sources rely on "targeting" to set their procedures without defining the term consistently with other authorities – or simply without defining the term at all. The following chart summarizes the ambiguities among each of the three terms within the Department of Defense and NSA 12333 manuals.

Agencies throughout the executive branch use language in precise and technical ways. But in the context of foreign intelligence, considerable ambiguity surrounds key terms that significantly affect the scope of the government's foreign intelligence activity. The Intelligence Community's tendency towards discretion,

171. PPD-28, *supra* note 90, § 2 n.5.

172. COMMITTEE ON RESPONDING TO SEC. 5(D) OF PRESIDENTIAL POL'Y DIRECTIVE 28, BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS 2 (2015), http://www.nap.edu/read/19414/chapter/1 [hereinafter SECTION 5(D) REPORT].

173. *Id.*

	DoD 5240.01 (2016)	**DoD 5240.1-R (1982)**	**USSID 18**
Collection	Information is collected when it is *received*, which includes information that is *obtained* or *acquired* by any means.	Information is collected when it is *officially accepted* for use and *processed into an intelligible form.*	Information is collected when it is *intentionally tasked* ("selected") for *subsequent processing*.
Acquisition	Ties "collection" to Executive Order 12333 and "acquisition" to FISA, but never explicitly defines "acquisition."	N/A	Defined in Annex A as "the *collection* by the NSA of a nonpublic communication to which it is not a party."
Targeting	Never explicitly defined. Used to refer to "acquisition," not collection. In military dictionary, selectors can include entire countries.	N/A	Definition redirects to "collection." Selection terms include telephone numbers and email addresses.

dispersal, and drift, in turn, makes it more difficult to bolster government accountability and transparency in an already highly classified sphere. In the next two Parts, we discuss in greater depth the normative reasons for counteracting these forces and propose solutions to ensure enduring change.

IV. NORMATIVE REASONS FOR ACTION

Skeptics of our argument may point to a series of reasons why the effects of discretion, dispersion, and drift are not overly troubling. In this Part, we explain the normative justifications for counteracting discretion, dispersion, and drift, while addressing a number of potential objections in turn.

First, although Executive Order 12333 and the IC's regulatory framework establish a number of actors charged with agency oversight, these actors focus primarily on compliance with existing regulations and lack the capacity to implement widespread change. Second, although the executive can and has attempted to implement reform, executive efforts to clarify and publicize the IC guidelines have, so far, often contributed to the confusion surrounding these documents while failing to lay the groundwork for enduring reform.

Third, while the intelligence manuals are meant for a specific audience – agency employees, not the general public – they are key to ensuring effective oversight over the executive branch's foreign intelligence activity. Fourth, and relatedly, the intelligence manuals are one of the few means to obtain visibility into intelligence activity.

Finally, reporting requirements to Congress, as well as legislation curtailing domestic surveillance, have failed to sufficiently limit executive discretion and minimize dispersion in the meanings of key technical terms.

A. The Inefficacy of Internal Compliance Checks

The foreign intelligence realm is chock-full of regulations. These regulations, in turn, are largely overseen by what Stewart Baker once called the "army of second-guessers"[174] – agency inspectors general, general counsels, and a multitude of lawyers tasked with regulating intelligence activity under Executive Order 12333. DoD 5240.01, for example, instructs "Defense Intelligence Component Counsel" to "assess the reasonableness of collection and restrictions on the retention and dissemination of USPI to ensure protection of Fourth Amendment rights and, when necessary, [to] consult with Defense Intelligence Component privacy and civil liberties officials and the Department of Justice."[175] The manual also establishes regular audits to ensure that U.S. person information is gathered in "compliance" with the manual.[176]

The Intelligence Community's complex rules make regular audits and close supervision, particularly by lawyers, necessary to carrying out foreign intelligence activities. But those tasked with ensuring compliance have limited means to change the regulations themselves. Rather than evaluating a program's efficacy or the degree to which it successfully protects constitutional guarantees, these agency overseers' efforts focus on ensuring that the IC adheres to its own rules.[177]

More generally, compliance does not involve ensuring or generating consistency across agencies. Nor is it typically elastic enough to respond to technological change over time.[178] As a result, although the compliance architecture that Executive Order 12333 and agency manuals rests upon is a necessary component for regulating intelligence activities, it has limited utility in redressing the problems we have identified.

B. Ad-Hoc Executive Reform

Due to the discretion granted it, the executive branch has the power to resolve and redress issues arising from inconsistency and confusion. Indeed, following

174. *Oversight Hearing on FISA Surveillance Programs* (2013) (statement of Stewart A. Baker), https://fedsoc.org/commentary/publications/stewart-a-baker-oversight-hearing-on-fisa-surveillance-programs-committee-on-the-judiciary-united-states-senate.

175. DOD FACT SHEET 5240.01-M, *supra* note 93, at 23.

176. *Id.* at 18.

177. *See* Schlanger, *Intelligence Legalism*, *supra* note 17, at 133-58.

178. *See, e.g.*, Sinnar, *supra* note 17 (examining the compliance function of offices of inspector general); Schlanger, *Intelligence Legalism*, *supra* note 17 (describing the limits of compliance).

the Snowden disclosures, the Obama Administration embarked on a series of wide-ranging intelligence reforms. Although the debate over the general efficacy of these reforms is beyond the scope of this Article, three executive efforts stand out for their efforts to clarify and publicize the government's foreign intelligence practices: (1) the attempts by intelligence agencies and, in particular, the newly constituted NSA Civil Liberties Office to clarify intelligence collection processes; (2) the Obama Administration's promulgation of PPD-28; and, most importantly, (3) the IC's recent attempt to make consistent the definitions of certain terms by updating a number of agency manuals.

In general, these efforts show that executive authorities have the capacity to respond to dispersion and drift. The question, however, is whether that capacity can be matched by the necessary conviction to ensure that consistency is sustained over time. This is far from certain: until recently, many agencies had not revised their manuals for nearly 40 years, and some have still not done so. As we demonstrate below, intermittent political will is not enough to meaningfully constrain these forces.

1. Public Facing Documents

Following the Snowden disclosures, the Obama Administration embarked on efforts to provide greater access to the classified materials amassed by the IC. Most notably, in 2013, the Office of the Director of National Intelligence, acting upon President Obama's direction, created IC on the Record, a Tumblr account dedicated to providing access to previously declassified information.[179] The site has served as a forum through which the IC has released FISC decisions, compiled speeches and testimony, and hosted primers authored by IC officials.

At the same time (and often in conjunction with IC on the Record), agencies have begun to declassify or generate their own documents to promote transparency. In 2014, for example, the NSA's Civil Liberties and Privacy Director – a position created in the summer of 2013[180] – released a civil liberties report on signals intelligence gathering under Executive Order 12333.[181] The report acknowledged that the classification of material made full transparency and direct participation by the public impossible. Instead, "NSA overseers provide surrogate

179. *See, e.g.*, Timothy Edgar, *The Good News About Spying*, FOREIGN AFF. (Apr. 13, 2015), https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying ("[The files on IC on the Record] are not decades-old files about Cold War spying, but recent slides used at recent NSA training sessions, accounts of illegal wiretapping after the 9/11 attacks, and what had been highly classified opinions issued by the Foreign Intelligence Surveillance Court about ongoing surveillance programs.").

180. *NSA Announces New Civil Liberties and Privacy Officer*, NSA (Jan. 29, 2014), https://perma.cc/2B2Z-W9TE (announcing the appointment of Rebecca Richards and noting that Obama announced the creation of the office in the summer of 2013); *see also* Schlanger, *Intelligence Legalism*, *supra* note 17, at 141.

181. Rebecca J. Richards, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333*, NSA CIVIL LIB. & PRIVACY OFF. 11 (Oct. 7, 2014), https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_clpo_report_targeted_EO12333.pdf [hereinafter *NSA Civil Liberties Report*].

means" for ensuring adequate protection. To inform the public about signals intelligence practices, the report provided lay definitions of key technical terms.[182]

These efforts, however, have at times added to the ambiguity surrounding the intelligence manuals. The NSA's civil liberties report, for example, describes the intelligence cycle as beginning with "acquisition" – a term typically associated with FISA rather than Executive Order 12333. The report notes that "[w]hile there are a variety of ways to describe the intelligence cycle, the report focuses on the following major components: Acquire, Analyze, Retain and Disseminate."[183]

Moreover, the report's definition of these terms confounds their meaning. In the report, data is "processed" after it is "collected": "Collection is the means by which NSA obtains SIGINT mission data on targets likely to produce foreign intelligence. Processing refers to the functions necessary to make that data usable for analysis and dissemination."[184]

This definition appears to conform to 5240.01's updated definition of "collection" as the moment when information is gathered. It diverges, however, from USSID 18's understanding of collection. Whereas USSID 18 describes "collection" as occurring only *after* information has been rendered intelligible, the NSA civil liberties report splits this conception into "collection" and "processing." Borrowing again from Clapper's metaphor, under the NSA civil liberties report, targeting would cover the scanning and selection of the book titles, collection would describe the choosing of the books, and processing might involve something like the translation of the book into a readable language.

As this discrepancy between the NSA civil liberties report and the Department of Defense manual demonstrates, unilateral executive efforts to declassify and make more intelligence procedures transparent may reveal, rather than resolve, confusion in the meaning of terms.

2. Presidential Direction

The Obama Administration's attempts to increase transparency extended beyond agency explainers. In 2014, the President issued PPD-28, which, unlike the civil liberties report, had the legal force to effect change. In fact, to date, PPD-28 represents one of the President's most significant direct efforts to clarify the scope of the IC's signals intelligence activities, reassure foreign allies by expanding the IC's privacy and civil liberties protections, and strengthen signals intelligence gathering oversight.

---

182. As the report begins, "This report was prepared by the National Security Agency (NSA) Civil Liberties and Privacy Office (CLPO) as part of its responsibilities to enhance communications and transparency with the public and stakeholders . . . .The intent of this . . . report is to continue to build upon a common understanding and foundation for future discussions about NSA's civil liberties and privacy protections." *Id.*

183. *Id.*

184. *Id.*

However, while PPD-28 unambiguously extends basic civil liberty protections to foreigners, its success in resolving ambiguity for the purposes of transparency or effective oversight remains uncertain.

For example, in an effort to promote transparency, PPD-28 appears to assign a lay definition to "collection," which would accord with the definition provided in DoD 5240.01.[185] In the preamble, PPD-28 provides that "[t]he collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm."[186] But in a footnote, PPD-28 combines all of the relevant terms we have introduced in a way that uses "collect" very differently from what the text of the document suggests: "The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection."[187] Rather than defining collection as the point of first interaction with the data, as in DoD 5240.01, the footnote suggests that collection may occur *after* acquisition and through the use of targeting. Some of this may be semantics. But the added layer of confusion undermines PPD-28's aims.

More broadly, in a report assessing PPD-28, the PCLOB noted that uncertainty has pervaded the IC's efforts to implement PPD-28 and advised the President to clarify the directive's scope. The Board cautioned that while "[i]t is not unusual for individual IC elements to apply different procedures to similar types of data, . . . the lack of a common understanding as to the activities to which PPD-28 applies has led to inconsistent interpretations and could lead to compliance traps, especially as IC elements engage in information sharing."[188]

Uncertainty has also undermined efforts undertaken pursuant to PPD-28 to establish new oversight. Section 5(d) of PPD-28 authorizes the DNI to create a new committee to author a "report assessing the feasibility of creating software that would allow the Intelligence Community more easily to conduct targeted information acquisition rather than bulk collection [of signals intelligence]."[189] In 2015, the aptly named 5(d) Committee released a report that demonstrates the barriers to effective oversight of the intelligence manuals:

> PPD-28. . . does not provide a precise definition of either bulk or targeted collection. Nor are these terms defined precisely elsewhere in law or policy. Moreover, the PPD-28 description of bulk collection is problematic because it says that (1) with a broad discriminant, such as "Syria," collection is targeted, even though it captures a large volume of information and covers vast numbers of people who are not of intelligence value; and (2) if the signal itself contains only the traffic of a single individual, collection is bulk if there is no

185. *See supra* Part III.A.
186. PPD-28, *supra* note 90, at pmbl.
187. *Id*. § 2 n.5.
188. Report on PPD-28, *supra* note 16, at 13-14.
189. SECTION 5(D) REPORT, *supra* note 172, at 1.

> discriminant. Both of these results are inconsistent with the plain meaning of the words bulk and targeted.[190]

Regarding "target," the committee noted, "Presidential Policy Directive 28 (PPD-28) asks whether it is feasible to create software that could replace 'bulk collection' with 'targeted collection.' This section attempts to explain this distinction, which, unfortunately, is quite unclear."[191] Rather than adopt the Intelligence Community's definitions, the committee often chose to create its own.[192] But the definitions generated by the committee are not always clearer than the IC's. More importantly, the definitions have no legal purchase. The committee's report therefore confirms the consequences of the executive branch forces we have described.

3. Agency Revision

The most significant effort to corral drifting meanings of terms has occurred at the agency rather than presidential level. Perhaps as a response to the Snowden disclosures, technological advances,[193] or congressional mandates,[194] the CIA

---

190. *Id*. at 2.

191. *Id*.

192. Specifically, the 5(d) Committee describes "[t]argeted collection" as "tr[ying] to reduce, insofar as possible, items about parties with no past, present, or future intelligence value," which is "achieved by using discriminants that narrowly select relevant items to store." *Id*. at 33 (blurring lines of how much selection is necessary to constitute "targeted" data, emphasizing that "if a discriminant is broadly crafted, the filter may retain such a large proportion of data on people of no intelligence value that the collection cannot be called 'targeted.'").

In addition to defining the term "targeting," the Committee defines the term "target" as "[a] subject of interest in an intelligence investigation" and notes that "[t]his term is used liberally by the Intelligence Community to denote an identifier or person that is the subject of interest or surveillance." *Id*. at 36. The Committee describes the phrase "subject of interest" with equal imprecision, defining it as "[a]n identifier of a party (person, group) that may have intelligence value and is likely to be part of an intelligence investigation." *Id*. Thus, in effect, the Committee does little to clarify the Department of Defense's broad conception of what constitutes a "target" and, if anything, muddles the already vague definition of "targeting."

However, the Committee does distinguish between two types of targets: (1) a "seed (target)," which is "[a]n initial target used to start an intelligence investigation" and (2) a "RAS target," which is "[a] target for which there is a reasonable, articulable suspicion (RAS) that it is associated with a foreign terrorist organization." *Id*. Notably, however, this is a distinction that stems from FISA, not Executive Order 12333. While this distinction's consequences for surveillance under Executive Order 12333 are not entirely clear, one might imagine RAS targets to allow more intrusive collection, particularly if this structure mirrors FISA's. *See* Jon Greenberg, *Are Americans Being 'Targeted' for Surveillance?*, POLITIFACT (July 2, 2013, 2:49 PM), http://www.politifact.com/truth-o-meter/article/2013/jul/02/are-americans-being-targeted-surveillance/.

193. *See, e.g*., John Reed, *The CIA's New Guidelines for Handling Americans' Information*, JUST SECURITY (Jan. 18, 2017), https://www.justsecurity.org/36482/cia-announces-revisions-executive-order-12333/ ("The rules announced today lay out several new requirements to deal with the fact that 'inherently, there's going to be more incidental collection' of Americans' data, CIA Privacy and Civil Liberties Officer Ben Huebner said.").

194. *See* discussion *infra* Section V.C.

and DoD have each recently revised their manuals, and other IC elements appear to be in the midst of doing so.[195]

The potential for agency correction is supported by the initial results of the manual revisions. The updated CIA and DoD manuals have conforming definitions of collection – both start the clock before information has been decrypted.

The substantive results recently achieved are supported by the nature of the process whereby the manuals are revised. Although these manuals are agency-issued, Executive Order 12333 requires both Department of Justice and ODNI participation.[196] Acting in a concerted manner, the input from DOJ and the ODNI could minimize the effects of dispersion and contain drift by considering the needs of the entire IC ecosystem. The ODNI, for example, which did not exist when agencies first began issuing their manuals, has catalogued and made public a single table documenting the status of all agency manual revisions.[197]

We are not convinced, however, that the roles played by DOJ and the ODNI, even substantiated by the new consistency of the revised manuals, are a sufficient reason to believe that the intelligence agencies can limit disruption on their own. DOJ and ODNI participation requires intelligence agencies to undertake the laborious process of updating and revising the manuals. Given the labor required to update the manuals, and their vital role for agencies, there is no guarantee the agencies will choose to commence an update without an exogenous shock along the lines of the Snowden disclosures. When they do, individual agencies may choose to act while others wait, as happened between the initial generation of manuals following President Reagan's issuance of Executive Order 12333 and the recent round of revisions. The powerful incentives for individual agencies to prioritize their own functioning remains. Moreover, agency interests vary administration by administration. It may not be a coincidence that the CIA released its new manual just days before President Obama – and CIA Director John Brennan – left office.

Finally, when agencies do update their manuals, implementation of these revisions is often uncoordinated and inconsistent. For example, an OIG report following the FBI's updates to its manual in May 2002 "found numerous instances where agents were not timely informed of Guidelines' requirements."[198] It also reported that a majority of Division Counsel considered manual guidance

195. *See* IC ON THE RECORD, *supra* note 19; *see also* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATUS OF ATTORNEY GENERAL APPROVED U.S. PERSON PROCEDURES UNDER EXECUTIVE ORDER 12333 (May 16, 2017), https://www.dni.gov/files/CLPT/documents/Chart-of-EO-12333-AG-approved-Guidelines_May-2017.pdf [hereinafter TABLE OF EO 12333 PROCEDURES].

196. The CIA manual, for example, states, "Executive Order 12333 directs that the CIA collect, retain, and disseminate intelligence information concerning U.S. persons in accordance with Procedures . . . approved by the Attorney General, after consultation with the Director of National Intelligence." CIA INTELLIGENCE ACTIVITIES, *supra* note 132, at 4.

197. TABLE OF EO 12333 PROCEDURES, *supra* note 195.

198. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, *How the FBI Implemented the May 30, 2002, Revisions to the Attorney General's Investigative Guidelines*, *in* THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES 279, 279 (Sept. 2005), https://oig.justice.gov/special/0509/final.pdf [hereinafter Special Report].

"not clear" in various sections.[199] Even after training to familiarize agents with the new FBI Guidelines, the OIG's "survey of FBI personnel revealed significant gaps and inconsistencies in the sufficiency and effectiveness of Guidelines training."[200] The FBI's experience suggests that even when individual agencies take the initiative to update their manuals, mere revisions are not enough without sufficient implementation oversight.

C. Manuals' Audience

While an initial set of counterarguments posits that the executive has the capacity to resolve any issues presented by variance in key meanings, another might focus on the nature of the documents themselves. These manuals are not designed to facilitate academic studies, the argument might go, but rather to create specific *operational guidance* for agents. Moreover, critics may argue that high-level documents such as PPD-28 and ground-level manuals will inevitably define terms in diverse ways. This issue is compounded by the scope of the topic: intelligence gathering is a broad category. Accordingly, some of these differences in definitions of terms between levels of hierarchy or across agencies may be appropriate.

But the manuals' role and intended audience are not reasons to sacrifice clarity or consistency. As we have argued above, the technical terms defined in the intelligence law manuals often play a critical role in determining the scope of intelligence gathering. As a result, they are also key to enabling effective internal and external oversight over the government's foreign intelligence activities. Absent clear and consistent definitions of these terms, legislators, judges, and even internal agency boards may struggle to assess the legality of intelligence gathering programs. Furthermore, the manuals themselves indicate that internal employees also struggle to make sense of definitional and regulatory ambiguity. The DoD manual, for example, encourages employees to check in with government lawyers at every opportunity.[201]

D. Definitional Dispersion and Drift Is Typical of Law

Another counterargument might point to a factor more intrinsic to law: words always matter. Definitional inconsistencies are not unique to intelligence gathering. On the contrary, there are inevitable differences of approach across *any* body of law. Understanding the tax code revolves around highly technical definitions of key words. The definition of "terrorism" or "employee" varies across federal agencies.

While definitional dispersion is not unique to the intelligence community, several factors that *are* unique make inconsistency especially troubling in the intelligence context. First, as discussed in Part I, the Intelligence Community has

199. *Id.*
200. *Id.*
201. DoD 5240.01-M, *supra* note 112, § 3.5(a)(1), at 23.

proven particularly unwieldy and difficult to unify.[202] Definitional inconsistencies thus both reflect and amplify the heightened dispersal in the underlying organizational structure.

Second, and more importantly, unlike tax determinations or typical agency determinations (be they rules or adjudications), the results of the manuals – the programs they operationalize – are often classified. An SEC determination to classify a security in a new way is visible, perceptible to the brokers involved in trading that security. Beyond the manuals, there is often no such visibility into the particulars of intelligence gathering activities. These definitional inconsistencies therefore limit external checks on the executive's intelligence gathering practices in the form of both congressional oversight and informed public debate.

E. Congressional Oversight

To date, Congress's repeated efforts to oversee foreign intelligence activities have not sufficiently promoted internal agency consistency or clarity. In the 1970s, Congress established the House and Senate Intelligence Committees to receive classified briefings from the Intelligence Community.[203] Congress later placed statutory responsibility upon, first, the heads of intelligence agencies, then, in 1991, the President to keep the congressional intelligence committees "fully and currently informed" of all U.S. intelligence activities, "including any significant anticipated intelligence activity and any significant intelligence failure."[204] Jack Goldsmith, former Special Counsel to the General Counsel to the Department of Defense, argues that intelligence agencies "take this duty seriously," both because they have experienced repercussions for "underreporting" and "because [they gain] political and legal cover (and comfort) from reporting."[205] And members of the intelligence committees –most notably Senator Ron Wyden and former Senator Mark Udall – have criticized the Intelligence Community for improperly using its surveillance powers, presumably in reliance on these reports.[206]

---

202. KRIS & WILSON, *supra* note 29.

203. National Security Act of 1947, Pub. L. No. 102-88, § 437(b), 105 Stat. 429 (1991) (codified as amended at 50 U.S.C. § 3091(a)(1) (2012)).

204. *Id.* § 3091(a)(1).

205. Jack Goldsmith, *Skepticism About Supposed White House and Intelligence Committee Ignorance About NSA Collection Against Allied Leaders*, LAWFARE BLOG (Oct. 29, 2013, 12:01 PM), https://www.lawfareblog.com/skepticism-about-supposed-white-house-and-intelligence-committee-ignorance-about-nsa-collection; *see also* KRIS & WILSON, *supra* note 29, § 2:7.

206. *See, e.g.*, Letter from Ron Wyden, U.S. Sen., & Mark Udall, U.S. Sen., to Eric Holder, Attn'y Gen. (Mar. 15, 2012), https://www.documentcloud.org/documents/325953-85512347-senators-ron-wyden-mark-udall-letter-to.html (criticizing the government's attempt to seek dismissal of two Freedom of Information Act lawsuits concerning its surveillance practices under Section 215 of the PATRIOT Act, and noting that "there is now a significant gap between what most Americans *think* the law allows and what the government *secretly claims* the law allows"); Ron Wyden, *Wyden Gets NSA's Top Lawyer to Confirm Secret Interpretations of Surveillance Laws*, YOUTUBE (July 26, 2011), https://www.youtube.com/watch?v=DERehlOPt3I; *see also* Julian Sanchez, *Ron Wyden Lights the Batsignal*, JUST SECURITY (June 26, 2017), https://www.justsecurity.org/42341/ron-wyden-lights-batsignal/?print (describing a Senate Intelligence Committee hearing on Section 702 of the FISA Amendments Act, in

In recent years, Congress has supplemented this duty to disclose by imposing additional statutory constraints on foreign intelligence practices. In 2014, the Senate Intelligence Committee included a provision in the Intelligence Authorization Act, codified in Section 309, that limits intelligence agencies to retaining non-publicly-acquired U.S. person information for a maximum of five years.[207] This provision may have played a role in encouraging the IC agencies to update their internal guidelines to comport with the retention requirement, including the definition of "collection" adopted by the Department of Defense.[208]

Although Section 309 suggests that Congress may have the capacity to address these forces, it has ultimately failed to do so. Despite their engagement with the Intelligence Community, Senators Wyden and Udall are outliers rather than the norm – most members of Congress simply do not have the incentive to develop the expertise necessary to effectively oversee the foreign intelligence cycle.[209] The high-level classification and technical complexity of intelligence activities pose significant barriers to acquiring sufficient knowledge for oversight. And, despite public concerns over civil liberties spurred by disclosures such as the 2013 Snowden leaks, foreign intelligence gathering oversight does not hold much political cache.[210] As the dispersion and drift of terms central to foreign intelligence gathering further complicate the intelligence landscape, they also prevent members of Congress from understanding the IC's foreign intelligence efforts, strengthening the disincentives for Congress to act.

Pointing to Congress as an effective overseer also fails to account for the twin concerns of transparency and government accountability, which are exacerbated by inconsistencies in the intelligence agency guidelines. Absent congressional action, the public has little opportunity to become aware of, much less respond to, agency determinations that ultimately determine the scope of intelligence gathering.[211] Although intelligence agencies brief the congressional intelligence committees, their meetings occur behind closed doors and before few members of

---

which Senator Wyden signaled, through questioning, that the government may be using Section 702 "to collect communications that it knows are entirely domestic.").

207. Intelligence Authorization Act of 2015, Pub. L. No. 113-293, § 309, 128 Stat. 3990, 3998.

208. The Intelligence Authorization Act requires "each head of an element of the intelligence community [to] adopt procedures approved by the Attorney General" within two years of the Act's enactment. *Id.* § 309(b)(1).

209. *See* Schlanger, *Intelligence Legalism*, *supra* note 17, at 179; Rascoff, *supra* note 11, at 698.

210. Schlanger, *Intelligence Legalism*, *supra* note 17, at 179 (citing AMY B. ZEGART, EYES ON SPIES: CONGRESS AND THE UNITED STATES INTELLIGENCE COMMUNITY 10-11 (2011) ("Congress has collectively and persistently tied its own hands in intelligence oversight for a very long time. Two institutional weaknesses are paramount: rules, procedures, and practices that have hindered the development of *legislative expertise* in intelligence, and committee jurisdictions and policies that have fragmented Congress's *budgetary power* over executive branch intelligence agencies. . . .Ten years after 9/11, the United States has an intelligence oversight system that is well-designed to serve the re-election interests of individual legislators and protect congressional committee prerogatives, but poorly designed to serve the national interest.")).

211. *See supra* Section IV.D (discussing effect of classified intelligence agency manuals on informed public debate).

Congress.[212] Members who do not sit on the intelligence committees are not privy to these conversations. Indeed, in the 1980s, frustrated by these institutional barriers, the House Subcommittee on Civil and Constitutional Rights for the Committee on the Judiciary held televised hearings on Executive Order 12333 after President Reagan excluded much of Congress from reviewing the order.[213] These concerns have persisted into the present day. Following the Senate Intelligence Committee's late addition of Section 309 to the Intelligence Authorization Act, a House representative objected to the "troubling" new provision that was "rushed to the floor for a vote" with little opportunity for review by the full body.[214] Even the congressional intelligence committees themselves have, at times, expressed frustration with the extent and quality of the IC's reports.[215]

In sum, the inadequacy of congressional oversight reemphasizes the point: rather than mitigate definitional confusion, the counterarguments we identify here underscore the reasons for action. The status quo, both in the executive and Congress, calls for measures to incentivize and regularize the process of revising the intelligence agency guidelines. These revisions, in turn, should ensure conformity within and across agencies, and appropriately account for technological advancements that enhance the government's surveillance capabilities. The normative critiques we identify here simultaneously indicate potential solutions to discretion, dispersion, and drift. While Congress and the executive have so far been ineffective, they each have the capacity to implement significant reforms. We turn to these solutions in Part V.

V. SOLVING THE INTELLIGENCE GATHERING PUZZLE

Scholars and the government itself have long recognized the dispersion of power among national security entities within the executive branch as a problem. In response, the government has attempted to implement solutions, such as the creation of the ODNI. However, few have undertaken serious efforts to establish interagency cohesion on granular issues, such as internal agency definitions.

Congress and various components of the executive branch have the capacity to address this confusion – the problem is that they do not consistently do so. As the

212. "In practice the intelligence communities brief only eight lawmakers and usually only after the fact. Edward Luce, *The Shifts in U.S. National Security Policy Since 9/11*, FIN. TIMES (Nov. 7, 2014), https://www.ft.com/content/21b69fca-6428-11e4-8ade-00144feabdc0 (reviewing MICHAEL J. GLENNON, NATIONAL SECURITY AND DOUBLE GOVERNMENT (2014)). In past years, slightly more than half of House Permanent Select Committee on Intelligence hearings and the vast majority of the Senate Select Committee on Intelligence have been closed to the public. https://intelligence.house.gov/calendar/?EventTypeID=215; https://www.intelligence.senate.gov/hearings.

213. *Executive Order on Intelligence Activities: Hearing Before the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 97th Cong. 12 (1981).

214. Justin Amash, FACEBOOK (Dec. 10, 2014), https://www.facebook.com/justinamash/posts/812569822115759.

215. As Representative Norman Mineta, who served on the House Intelligence Committee during the Reagan years, colorfully observed, "We are like mushrooms. . ..They keep us in the dark and feed us a lot of manure." Rascoff, *supra* note 11, at 699.

IC's current push to update its procedures demonstrates, intelligence agencies have, at times, initiated internal reforms. And, as Section 309 suggests, Congress itself may take action to check the executive branch's foreign intelligence activities. These efforts, however, began only after precipitating events, such as the Snowden disclosures.[216] As Carrie Cordero explains, while "presidential . . . involvement in reviewing intelligence-collection priorities has likely ebbed and flowed over the decades, . . . that does not mean that there was not an institutional process available to those participants, if they had chosen to engage deeply with it. Instead, . . . priorities across and within presidential administrations shift and . . . it sometimes takes a crisis to mobilize attention and prompt action."[217] While Cordero focused in particular on presidential involvement in foreign intelligence affairs, her claim applies more broadly to the executive and Congress. Even absent a crisis such as the Snowden leaks, both institutions have the *ability* to counter the IC's discretion in crafting its internal agency guidelines and the inconsistency that results.

A note of caution: although there are vital normative reasons for Congress to react to the intelligence gathering puzzle, it is equally essential that it does not *over*react. From a constitutional standpoint, Article II places much control over national security, and by extension, foreign intelligence activity, within the executive branch's powers.[218] Although we argue that some congressional action is preferable as an external accountability and regulatory mechanism, we believe that the executive must retain adequate discretion. Moreover, given the political difficulties of reforming the system, we suggest that incremental reforms are far more realistic than efforts to implement sweeping structural changes.

A. Executive Standardization of Terms

We first propose a novel means for the executive to address the problems of dispersal and drift: issuing a glossary, generated by an interagency process, that clarifies and standardizes vital intelligence terms. Although a glossary of this sort would leave executive discretion unperturbed, it would guarantee interagency consistency of definitions, enabling both internal and external oversight actors to better understand how intelligence surveillance works, and thus to better evaluate its legality. Importantly, we argue this glossary should emanate from the executive to build on IC expertise and encourage individual agencies to "own" the

---

216. *See* EDGAR, BEYOND SNOWDEN *supra* note 22, at 3-4 ("The Snowden revelations forced the NSA to take painful steps to open up. Before Snowden, basic information such as the number of targets affected by court-ordered surveillance was a closely guarded secret, obscuring important facts such as how much surveillance could be authorized by a single court order. Today the head of the intelligence community publishes an annual transparency report, revealing that one such order authorized surveillance of more than 100,000 foreign targets, and that data about Americans collected under that order were queried more than 30,000 times, among other details. This new transparency would not have happened without Snowden.").

217. Carrie Cordero, *A Response to Professor Samuel Rascoff's Presidential Intelligence*, 129 HARV. L. REV. F. 104, 106 (2016) (emphasis added).

218. KRIS & WILSON, *supra* note 29, § 1:2.

process and product, rather than view it as a congressional imposition on their duties and domain.

An executive glossary would have a number of advantages over simply allowing agencies to define terms on a manual-by-manual basis, as they currently do now, with Attorney General approval and consultation with the Director of National Intelligence. Most simply, collecting the terms would provide clarity and enhance oversight efforts.[219] Overseers, whether in Congress or at the Department of Justice or even within the intelligence agencies themselves, would be able to consult with glossary definitions when interpreting agency manuals or checking programs. Rather than just adding unnecessary paperwork, this could help make the manuals themselves more legible and their use more efficient.

Perhaps more importantly, an interagency process to issue the glossary would increase the stickiness of the definitions. While the issuance of the agency manuals brings individual agencies together with the Department of Justice and the ODNI, we believe that the initial issuance of the glossary should involve participation from agencies across the IC, in a process convened by the National Security Council. While this would require substantial upfront and coordinated effort, it would ensure that at least initial agency needs are reflected ex ante, as opposed to addressed ex post through manual revisions. To the extent that agencies have specific or unique needs, different words can be introduced and defined. As time passes, and intelligence gathering changes, NSC officials – or even officials at ODNI or DOJ – would be well placed to determine whether the glossary itself should be modified. With the White House at the helm, updates or modifications to the glossary would alter the entire fabric of the definitions of intelligence gathering simultaneously.

Additionally, although the glossary would emanate solely from the executive, a notice-and-comment like process – without the legal requirements that comments be meaningfully addressed – would both enhance the glossary's legitimacy and provide a much-needed outlet for public discourse. Since terms would be integral to, but reasonably divorced from and not revealing of, classified operations, the general conversation over definitions would serve well to help determine the nature of the balance between privacy interests and surveillance needs. As a result, although the glossary would not limit discretion, it could further democratic accountability both by rendering the manuals more accessible to all forms of oversight and by offering another point at which to consider general values.

Of course, any future presidential administration could simply discard (or disregard) the glossary. This, though, is true of Executive Order 12333 itself, which

219. Of course, the next logical question might be: Which terms? Based on our previous analysis, "collection" and "targeting" are critical to define, but, as we have stated before, these terms are merely two gnarls in a broad field of definitional confusion. We believe that the same process whereby the terms would be issued could also be used to identify which terms merit inclusion: At a minimum, they should have some technical or legal significance and be general enough to cover more than a single agency's activity.

persists due to the IC's reliance on it. Likewise, the advantages of a glossary for all parties would likely ensure its staying power.

B. Independent Oversight Body

Much as Congress formalized the role of the PCLOB, it could similarly establish an independent clearinghouse to review terms *prior* to their adoption by each agency. An external oversight body would prevent drift in the use and interpretation of key terms by centralizing the dispersion of power across the Intelligence Community, as well as potentially expediting the long – sometimes arduous – process by which an agency revises its own definitions.

The benefits of an external oversight body have been discussed at length.[220] Centralized overseers have access to highly classified documents that are not available to most members of Congress, let alone the public.[221] These institutions are therefore best situated to assess the consistency, and efficacy,[222] of the use of agency terms. As bodies external to the Intelligence Community, independent overseers are also uniquely positioned to ensure the consistent interpretation of terms *throughout* the Intelligence Community.[223] And they can do so freed from the exigencies of the intelligence apparatus.[224] In the context of Executive Order 12333, a central oversight institution would, for example, supplement the Attorney General by serving as an additional check on intelligence agencies. As others have argued, the Attorney General's role as the final, and often sole, authority on intelligence agency procedures has been diminished by that office's increasing involvement in intelligence and national security operations.[225]

The PCLOB offers the best example of a central oversight institution in the foreign intelligence realm. Formed in 2004 and reconstituted in 2007, the PCLOB is an independent bipartisan agency within the executive branch responsible for reviewing the executive's counterterrorism activities to ensure that they appropriately weigh privacy and civil liberties concerns.[226] Unlike the independent overseer envisioned in this Article, the PCLOB focuses on assessing surveillance programs after their initiation, as opposed to the contemporaneous development and implementation of the agency procedures themselves.[227] But the PCLOB exhibits many of the qualities described above. Its report on Section 702

220. *See, e.g.*, Zachary K. Goldman, *The Emergence of Intelligence Governance*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 207-34 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016); Schlanger, *Offices of Goodness*, *supra* note 102, at 92-101.

221. Goldman, *supra* note 220, at 223; *see also* Renan, *supra* note 17, at 1121.

222. Renan, *supra* note 17, at 1118-23.

223. As Renan notes in the context of the Fourth Amendment, "[c]entralized review enables a more synoptic expertise—that is, visibility into how overlapping and interconnected administrative policies (designed by different actors) in combination create systemic privacy risks or safeguards." *Id.* at 1114.

224. Goldman, *supra* note 220, at 226-28.

225. Renan, *supra* note 17, at 1118.

226. 42 U.S.C. § 2000ee(c) (2012).

227. Note that nothing in the statute prevents the PCLOB from focusing on the development of the procedures themselves. *See id.*

of FISA,[228] for example, draws from classified information to form a fuller and more informed picture of the surveillance programs operated by the government.[229]

At a minimum, these characteristics could enable the PCLOB or a similarly situated institution to examine the executive's agency procedures as they are developed pursuant to Executive Order 12333. Indeed, the Board began reviewing the Executive Order 12333 intelligence programs in 2015.[230] However, the PCLOB also illustrates the hazards of relying upon an institution within the executive branch to review agency activity. All but one of the PCLOB's members resigned or retired prior to President Trump's inauguration, depriving the Board of a quorum sufficient for it to continue examining Executive Order 12333 for over a year.[231] The Board recently regained a quorum in October 2018 but has not yet released its 12333 report.[232]

C. Congressional Legislation

Although the solutions above would add further internal oversight and centralize the generation of key elements in the architecture of foreign intelligence gathering – corralling dispersion and drift – neither would address the fundamental question of the President's discretion in the realm of foreign intelligence gathering. As discussed above, Executive Order 12333 and its implementing manuals are primarily executive branch-created. For reasons ranging from the difficulty of intelligence oversight to a lack of motivation and deference to the executive,[233] Congress has consistently proved cautious, at best, when engaging with the intelligence-gathering apparatus, choosing only to enact legislation governing domestic intelligence gathering or in tightly delimited scenarios, like the FISA Amendments Act. Still, we argue that congressional remedies are available.

Congress could, for example, pass legislation clarifying when intelligence gathering begins. For that matter, it could define – or require the executive to

228. *Public Hearing Regarding Section 702*, *supra* note 148.

229. Renan, *supra* note 17, at 1121-22 (noting that the PCLOB's Section 702 report "sets out for the first time how the various pieces of the section 702 program fit together, how and when the rules from different agencies interconnect, and what the hard and open legal and policy questions of program design and implementation look like"). For a critique of the executive's surveillance activities by a former PCLOB member, see Rachel Brand, *Memo to NSA: Stop Saying You Apply the FIPPs*, LAWFARE BLOG (Nov. 25, 2014, 11:51 AM), https://www.lawfareblog.com/memo-nsa-stop-saying-you-apply-fipps.

230. *See PCLOB Examination of Executive Order 12333 Activities in 2015*, PRIVACY & CIVIL LIB. BOARD, https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf.

231. Paul Rosenzweig, *Near-Death of the PCLOB*, LAWFARE BLOG (Dec. 21, 2016, 5:32 PM), https://www.lawfareblog.com/near-death-pclob.

232. *See supra* note 27.

233. Goldman, *supra* note 220, at 222-225. As Amy Zegart has written, "Intelligence is in many respects the worst of all oversight worlds: It concerns complicated policy issues that require considerable attention to master, deals with highly charged and controversial policies that are fraught with political risk, requires toiling away in secret without the promise of public prestige, and provides almost no benefit where it counts the most, at the polls." AMY B. ZEGART, EYES ON SPIES at 115-16, *cited in* Rascoff, *supra* note 11, at 639.

regularly update the definitions of - the terms for *all* key phases of the intelligence cycle. Section 309 of the Intelligence Authorization Act demonstrates that such a solution is possible. In limiting the retention of intelligence on U.S. persons to five years, Congress passed its first statutory constraint on Executive Order 12333 non-statutory activity. While the legislative history does not reveal the impetus behind Section 309, the provision likely encouraged intelligence agencies to reevaluate and subsequently revise their intelligence agency guidelines as a whole. Most notably, the CIA has updated its definition of "collection" to accord with the DoD's; other Intelligence Community elements will likely release updated definitions as well.[234] As we have previously noted, the meaning of this term had not been clarified since the 1980s.

Rather than indirectly compel agencies to revise their intelligence-gathering procedures from the back end, we argue that Congress can affirmatively require interagency coordination to update foreign intelligence guidelines at regular intervals and thereby prevent dispersion and drift. Such action would not affect individual operations at a programmatic level, nor would it directly superimpose additional, difficult to administer, congressional oversight; it would, however, limit ambiguity and curtail executive dispersal, drift, and, in a narrowly tailored manner, discretion. The meanings of "electronic surveillance" and "intercept," defined in FISA and the federal wiretap act,[235] respectively, have endured in roughly their original form, even as the words have often become the sites of significant contestation.[236]

Legislation would have the further advantage of inviting greater democratic attention to and debate over how surveillance and intelligence gathering function. Additionally, any legislation could be worded so as to give the FISC a slender jurisdictional hook into Executive Order 12333 oversight: rather than overseeing particular programs of foreign intelligence gathering conducted under Executive Order 12333, the FISC could be asked to serve as a final review of the use of defined terms in agency manuals and classified annexes, to ensure that new developments comply with the statute. This process would constitute a more relaxed form of FISA written justifications for procedural changes.[237]

Any congressional action would, of course, be fraught. The NSA has typically opposed congressional incursions that would limit flexibility. Moreover, due to the technicality of intelligence terms, meaningful congressional action comes at a high upfront cost – one that members of Congress have typically chosen to avoid. Finally, terms might need to be updated over time, and, as debates over the expiration of Section 702 have shown, this could be a difficult political enterprise for Congress.[238]

---

234. *See supra* note 195 and accompanying text.

235. 18 U.S.C. § 2510 *et seq*. (2012).

236. *See, e.g*., Huff v. Spaw, 794 F.3d 543 (6th Cir. 2015).

237. *See* Schlanger, *Intelligence Legalism*, *supra* note 17, at 131-32.

238. Jason Pye & Sean Vitka, *Congress Poised to Jam Through Reauthorization of Mass Surveillance*, THE HILL (Nov. 27, 2017, 6:20 AM), http://thehill.com/opinion/cybersecurity/361875-congress-poised-to-jam-through-reauthorization-of-mass-surveillance.

CONCLUSION

In the five years since the Snowden disclosures, much attention has been paid to efforts to reform the modern surveillance apparatus. President Obama's promulgation of PPD-28, the IC's movement towards greater transparency, and, in 2017, congressional debates over the reauthorization of Section 702, reflect governmental efforts to reconsider appropriate constraints on the executive's intelligence apparatus and the effectiveness of agency overseers. But few have trained attention on inconsistencies in the agency guidelines – the "ecosystem of interacting agency protocols"[239] – that ultimately determine the scope of the executive's intelligence activities. We argue that they should. The definitions of collection, acquisition, and targeting are critical to the initiation of the foreign intelligence cycle. Discretion, dispersion, and drift thus threaten to undermine the efficacy of agency guidelines intended to constrain surveillance of U.S. persons. It is only after foreign intelligence gathering has officially "begun" that the attendant procedural protections apply.

By focusing on specific terms, we do not intend to obscure the broader import of these forces. The problems we document here are not limited to the beginning of the intelligence cycle; discretion, dispersal, and drift in agency guidelines pervade the national security realm. Unlike other agencies, the particular sensitivity and classification of foreign intelligence activities means, in practice, that comparatively few corrective measures exist outside the executive branch. As the Intelligence Community itself has recognized, clarifying intelligence agency guidelines is necessary to facilitate public awareness of its foreign intelligence activities.

The Intelligence Community's recent and forthcoming updates to its Executive Order 12333 guidelines represent an important step towards reform. But a massive disclosure of intelligence practices such as the Snowden leaks should not be the impetus for change. Rather, the solutions we outline here aim to regularize and institutionalize the process of reviewing and updating intelligence agency guidelines, both within and across agencies. Such measures are particularly important in light of technological advancements that will likely continue to expand the government's surveillance capabilities. By establishing mechanisms to counteract discretion, dispersal, and drift, the IC can avoid falling into the "isolated echo chambers of the agency itself."[240]

239. Renan, *supra* note 17, at 1041.
240. Dalal, *supra* note 53, at 84.

***