SECRECY AND NATIONAL SECURITY INVESTIGATIONS

Nathan Alexander Sales[*]

> The necessity of procuring good Intelligence, is apparent and need not be further urged. All that remains for me to add is, that you keep the whole matter as secret as possible. For upon secrecy, success depends in most Enterprises of the kind, and for want of it, they are generally defeated, however well planned and promising a favourable issue.
>
> George Washington, July 26, 1777[1]

> They may carry on the most wicked and pernicious of schemes under the dark veil of secrecy. The liberties of a people never were, nor ever will be, secure, when the transactions of their rulers may be concealed from them. The most iniquitous plots may be carried on against their liberty and happiness.
>
> Patrick Henry, June 9, 1788[2]

Secrecy has been part of national security operations for as long as there has been a nation to secure. And it has been problematic ever since.

July 26, 1777, dawned with the Continental army encamped eight miles east of Morristown, New Jersey, and with its Commander in Chief, General George Washington, baffled about the intentions of his British rival. Sir William Howe had spent the spring trying, unsuccessfully, to goad Wash-

* This Article was written when I was John M. Olin Fellow at Georgetown University Law Center. The standard disclaimers apply. The views expressed are mine and mine alone. Neither they, nor any mistakes, should be attributed to those who offered comments on drafts of this Article, and for whose assistance I am grateful: Jonathan H. Adler, Kristi L. Bowman, Julie Cohen, David Cole, Elisebeth Cook, Viet D. Dinh, Fr. Robert F. Drinan, Orin S. Kerr, Heather Mac Donald, Brent J. McIntosh, Louis Michael Seidman, and participants in faculty workshops at Brooklyn Law School, George Mason University School of Law, Georgetown University Law Center, and the University of Nebraska College of Law.

1. Letter from George Washington to Col. Elias Dayton (July 26, 1777), *in* 8 THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745-1799, at 479 (John C. Fitzpatrick ed., 1931) [hereinafter WRITINGS OF GEORGE WASHINGTON].

2. THE DEBATES IN THE CONVENTION OF THE COMMONWEALTH OF VIRGINIA ON THE ADOPTION OF THE FEDERAL CONSTITUTION, *in* 3 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 170 (Jonathan Elliot ed., J.B. Lippincott Co., 2d ed. 1941) (1836) [hereinafter ELLIOT'S DEBATES].

ington's smaller army into a general engagement in the New Jersey countryside,[3] while Washington had used the previous months to develop an extensive network of spies.[4] Now he meant to use it. Washington had just learned that Howe's army had sailed from New York City.[5] With the words reproduced above, he dispatched one of his regimental commanders to Staten Island, not only to see if a skirmish there were practicable but more generally "to obtain intelligence of the Enemy's situation and numbers, What kind of Troops they are, and what Guards they have, their strength and where posted."[6] Washington was in the dark, and he was frustrated.[7] Would Howe head up the Hudson River and join forces with General John Burgoyne, then leading a campaign near Lake Champlain? Would he lay siege to Boston, the seedbed of revolutionary fervor? Or would he sail south and menace the capital city of Philadelphia?

Washington had to wait a month for a definitive answer, and his efforts to gain intelligence proved no more successful than the immediate campaign it was meant to support. After a lengthy perambulation in the Atlantic, Howe's army finally landed at the northern tip of the Chesapeake in late August and began its march to Philadelphia.[8] The outnumbered Continentals suffered a bitter defeat at Brandywine creek—on September 11, 1777—in large part because of intelligence failure.[9] Seven days later, a young Washington aide-de-camp named Alexander Hamilton urged Congress to evacuate Philadelphia; Howe captured the infant nation's capital eight days after that.[10]

Though secrecy and intelligence have walked hand in hand since the nation's infancy, the going has not always been easy. Consider the problems that arise when the government uses third parties to gather intelligence about national security threats. Telephone companies, Internet service providers, banks, and other entities accumulate vast repositories of data in their

3. *See* JOHN E. FERLING, THE FIRST OF MEN: A LIFE OF GEORGE WASHINGTON 198-203 (1988); 4 DOUGLAS SOUTHALL FREEMAN, GEORGE WASHINGTON: A BIOGRAPHY 427-34 (1951).

4. *See* G.J.A. O'TOOLE, HONORABLE TREACHERY: A HISTORY OF U.S. INTELLIGENCE, ESPIONAGE, AND COVERT ACTION FROM THE AMERICAN REVOLUTION TO THE CIA 37-40 (1991); *see also* NATHAN MILLER, SPYING FOR AMERICA: THE HIDDEN HISTORY OF U.S. INTELLIGENCE 5 (1989) ("George Washington was America's first spymaster. Probably no American military commander since has surpassed him in the attention given to intelligence operations.").

5. *See* 4 FREEMAN, *supra* note 3, at 445; O'TOOLE, *supra* note 4, at 41.

6. Letter from George Washington to Col. Elias Dayton, *supra* note 1, at 479.

7. *See* 1 HARRISON CLARK, ALL CLOUDLESS GLORY: THE LIFE OF GEORGE WASHINGTON 328 (1995) ("This was one of the more peculiar periods of the war and totally nerve-wracking for Washington and his army. From July 23 until August 25, the greater part of the British army rolled around the Atlantic Ocean and Chesapeake Bay. Washington could never be sure of what would happen, whether Howe would turn north again or go farther south.").

8. *See* JOSEPH J. ELLIS, HIS EXCELLENCY: GEORGE WASHINGTON 102 (2004); 4 FREEMAN, *supra* note 3, at 467.

9. Washington attributed Brandywine to his having received "[a] contrariety of Intelligence, in a critical and important point." Letter from George Washington to Brig. Gen. Thomas Nelson (Sept. 27, 1777), *in* 9 WRITINGS OF GEORGE WASHINGTON, *supra* note 1, at 272; *see also* 4 FREEMAN, *supra* note 3, at 471-89 (chapter describing Brandywine entitled "The Intelligence Service Goes Astray").

10. *See* 1 CLARK, *supra* note 7, at 335; BURKE DAVIS, GEORGE WASHINGTON AND THE AMERICAN REVOLUTION 224 (1975).

day to day operations. Investigators often want access to that information to monitor the communications, travels, and finances of suspected terrorists and spies. Examining third party records can be a helpful investigative technique, but it also carries a risk: the danger that a third party will compromise an operation by publicizing the government's request. Investigators therefore will want to impose "gag rules"—secrecy requirements that bar outside entities from revealing anything about the government's activities. And there's the rub. Not only are third parties effectively conscripted into participating in the government's national security operations, but they also will find themselves forbidden from speaking about their interactions with investigators. And those restrictions put a real strain on free speech, privacy, and other constitutional values.

The problems posed by investigative secrecy won't go away anytime soon. The principal tools used by the FBI (the United States' chief domestic intelligence agency[11]) to gather information in U.S. based operations—the Foreign Intelligence Surveillance Act of 1978 (FISA) and the several National Security Letter (NSL) statutes—generally bar third parties from revealing that the government sought information from them. And since the terrorist attacks of September 11, 2001, investigators have sharply increased their use of FISA and NSLs, along with their attendant secrecy requirements.[12] Academics and advocates alike have denounced these secrecy rules as poor public policy, not to mention affronts to various constitutional guarantees.[13] Courts haven't lagged far behind. Recently, two federal district courts independently invalidated an NSL statute's secrecy rule, concluding that it was an unconstitutional restriction on the recipient's rights of free speech.[14]

---

11. Unlike, say, the United Kingdom, which has separate agencies for criminal law enforcement (Scotland Yard) and domestic intelligence gathering (MI5), *see* MARK RIEBLING, WEDGE 460, 474 (2002), the United States has assigned both law enforcement and national security responsibilities to the FBI, *see* Exec. Order No. 12,333, § 1.14, 46 Fed. Reg. 59,941, 59,949 (Dec. 8, 1981), *reprinted as amended in* 50 U.S.C. § 401 (2000).

12. *See* Dan Eggen & Susan Schmidt, *Data Show Different Spy Game Since 9/11; Justice Department Shifts Its Focus to Battling Terrorism*, WASH. POST, May 1, 2004, at A1 (reporting that "[t]he number of FISA warrants filed in 2003 was an 85 percent increase over the total in 2001," and that "[t]he volume of secret wiretaps has grown so rapidly over the past two years that the Justice Department has fallen behind in processing applications"); Barton Gellman, *The FBI's Secret Scrutiny; In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A1 (reporting that since 2001, the "FBI now issues more than 30,000 national security letters a year, . . . a hundredfold increase over historic norms").

13. *See, e.g.*, Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1359-60 (2004); ANN BEESON & JAMEEL JAFFER, ACLU, UNPATRIOTIC ACTS: THE FBI'S POWER TO RIFLE THROUGH YOUR RECORDS AND PERSONAL BELONGINGS WITHOUT TELLING YOU 8 (2003), http://www.aclu.org/FilesPDFs/spies_report.pdf.

14. *See* Doe v. Gonzales, 386 F. Supp. 2d 66, 82 (D. Conn. 2005), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006); Doe v. Ashcroft, 334 F. Supp. 2d 471, 525-26 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006). The Second Circuit dismissed the former case as moot and vacated the latter, in light of the fact that Congress subsequently made substantial revisions to the NSL's secrecy rules. *See Gonzales*, 449 F.3d at 418-19 (citing USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006); and USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278).

Not to put too fine a point on it, the existing investigative secrecy regime is a mess. This Article, the first systematic account of the secrecy rules used in national security investigations,[15] aims to explain these shortcomings and suggest what may be done about them.

Part I begins by discussing the various competing interests implicated by investigative secrecy: the Executive Branch's operational interests in maintaining the confidentiality of its intelligence sources and methods, preventing disruption to ongoing investigations, and averting diplomatic embarrassment; the respective interests of investigative targets and third party witnesses in privacy and free speech; the public interest in obtaining the information needed to check government abuses and to participate meaningfully in democratic decisionmaking; and the congressional interests in effective oversight of the Executive. No one set of interests is decisive. Whether secrecy is justified at all, and the appropriate scope of a secrecy requirement, will be a function of the interplay among them. Part I.B then describes the range of policy choices that would have to be made if one were building a secrecy regime from the ground up. For example, what type of information is to be protected against disclosure? Should a secrecy obligation be imposed automatically or only upon a special showing by the government? How long should a nondisclosure requirement persist?

Part II describes how the existing investigative secrecy regime operates. It begins with a brief history of FISA, which was born in the late 1970s out of widespread revulsion at abuses by the Executive Branch of its information gathering authorities—in particular, warrantless wiretapping of dissident groups and the political rivals of incumbent statesmen. It then explains the requirements of the various secrecy rules, discussing which of the intersecting options from Part I.B's menu of policy choices have been implemented. Special attention is paid to FISA's four subchapters, which govern electronic surveillance; pen registers and trap and trace devices; physical searches; and orders to produce business records and other tangible things. This Part also examines NSLs, a form of administrative subpoena that enables the government to collect certain documentary information without prior court approval. Instructive contrasts are drawn to each of these authorities' counterparts from the world of garden variety criminal investigations.

Part III explores how the existing secrecy regime measures up to ideal rules as informed by Part I. The answer is: Not well. First, almost without exception, investigative secrecy rules only forbid third parties from disclos-

15. The law review literature recently has begun to examine the secrecy rules associated with particular investigative techniques. *See, e.g.*, Swire, *supra* note 13, at 1359-60 (analyzing the FISA business records nondisclosure obligation); Zachary D. Shankman, Note, *Devising a Constitutional National Security Letter Process in Light of* Doe v. Ashcroft, 94 GEO. L.J. 247 (2005) (analyzing the ECPA NSL's nondisclosure obligation); Brett A. Shumate, Comment, *Thou Shalt Not Speak: The Nondisclosure Provisions of the National Security Letter Statutes and the First Amendment Challenge*, 41 GONZ. L. REV. 151 (2006) (same). But at present, no sustained synthesis of the issues that cut across the various investigative secrecy requirements yet exists.

ing that the government is conducting an investigation; they generally impose no limitations on revealing the underlying information the government seeks to collect. Yet sometimes releasing those "underlying facts" is just as damaging as disclosing "investigative facts." The system therefore needs a mechanism by which secrecy may be imposed as to exceptionally sensitive underlying facts. Second, some of the secrecy rules associated with investigative techniques where information is gathered in real time (such as electronic surveillance) are weaker than their retrospective counterparts (such as the collection of documents and records). This has it backwards because real time intelligence gathering presents a risk not present when other investigative techniques are used—namely, the danger that the target's awareness of the monitoring will prevent the information sought from being created at all. The current regime's weak secrecy rules for certain real time surveillance methods should be strengthened. Third, many nondisclosure rules are imposed automatically, without any requirement that the government make a special showing of the need for secrecy. But an investigation conducted in secrecy implicates a greater range of interests than one conducted openly: not just target privacy interests but also third party speech interests and public and congressional oversight interests. The existing rules therefore should be changed so the Executive ordinarily has to demonstrate the need for a nondisclosure requirement on a case by case basis; we should be buying secrecy retail, not wholesale. And fourth, the Executive's operational interests tend to diminish over time, while those of other stakeholders only grow stronger. Hence, the secrecy rules, most of which currently are perpetual in fact or by presumption, should be amended to include both dates certain on which secrecy presumptively will lapse and review mechanisms by which secrecy may be lifted before its natural expiration.

The point of this exercise is not so much to argue that this or that aspect of the existing secrecy rules is or is not constitutional. Rather, my purpose is to identify the competing values that underlie the law of secrecy (Part I), to trace how current law chooses among and implements those values (Part II), and to recommend improvements that would more closely calibrate the secrecy requirements to the values they implicate (Part III).

A few clarifications are needed to help situate this Article within the larger debates about governmental secrecy. My ambitions are modest. This Article only addresses what may be called "investigative," or "first order," secrecy rules—the restrictions designed to maintain the confidentiality of the manner by which the government collects intelligence. It does not address in detail the issues raised by what we may call "possessory," or "second order," secrecy requirements—laws that govern the dissemination of sensitive information in the government's possession,[16] such as the Freedom of Information Act.[17] Nor do I spill much ink on "evidentiary," or "third

16. *See, e.g.*, Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131 (2006).

17. *See* 5 U.S.C. § 552(b)(1) (2000) (providing that an agency's general obligation to release re-

order," secrecy rules, which come into play when the government seeks to use sensitive information in legal proceedings while simultaneously shielding it from public view.[18] The Classified Information Procedures Act[19] is an example. Even the limited class of first order secrecy rules must be further subdivided. I focus almost entirely on the secrecy requirements in the surveillance tools (such as FISA and the NSLs) the FBI uses in domestic intelligence operations. Only in passing will the Article touch on the investigative secrecy rules typically associated with foreign operations (such as the Intelligence Identities Protection Act[20]). A broader focus, one fears, would test both the skill of the author and the patience of the reader.

I. THE INTERESTS AND TAXONOMY OF SECRECY: A CONCEPTUAL FRAMEWORK

Any account of government secrecy must begin with the presumption that, in the American constitutional system, transparency and openness is the general rule to which secrecy is the occasional exception.[21] "Democracies die behind closed doors,"[22] and "[s]unlight is said to be the best of disinfectants."[23] Yet although openness and transparency are heavily favored, they do not invariably carry the day. Since the founding, it has been recognized that the need for secrecy is more acute in matters of foreign policy, military affairs, and other national security functions.[24] This Part surveys the

---

cords to the public does not apply to matters that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order").

18. *See, e.g.*, Note, *Secret Evidence in the War on Terror*, 118 HARV. L. REV. 1962 (2005).

19. *See* 18 U.S.C. app. 3, § 4 (2000) (authorizing the government, "upon a sufficient showing," to "delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove").

20. 50 U.S.C. § 421(a) (2000) (making it a crime to disclose information that identifies certain covert operatives).

21. *See* Anthony Lewis, *Introduction* to NONE OF YOUR BUSINESS: GOVERNMENT SECRECY IN AMERICA 3, 9 (Norman Dorsen & Stephen Gillers eds., 1974) [hereinafter NONE OF YOUR BUSINESS] ("[S]ecrecy in government is *not* as American as apple pie. It has occurred, it may be defended in particular circumstances, but it must always be regarded as an exception.").

22. Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002).

23. Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WEEKLY, Dec. 20, 1913, at 10, *reprinted in* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92, 92 (Frederick A. Stokes Co. 1914).

24. *See* CIA v. Sims, 471 U.S. 159, 169 (1985) (invoking "the practical necessities of modern intelligence gathering" to justify occasional national security secrecy); Chi. & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are not and ought not to be published to the world."); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936) ("[The President] has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials. Secrecy in respect of information gathered by them may be highly necessary, and the premature disclosure of it productive of harmful results."); Totten v. United States, 92 U.S. 105, 106 (1876) ("[The President] was undoubtedly authorized during the war, as Commander-in-Chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources and movements of the enemy . . . ."); THE FEDERALIST NO. 64, at 392-93 (John Jay) (Clinton

wide array of interests implicated by these rules, including those of the Executive Branch, investigative targets, third parties, Congress, and the public. Part I.B then identifies five issues one must grapple with when crafting a secrecy regime from the ground up (e.g., Should secrecy be available automatically or only upon a special showing? How long should secrecy last?), and it locates the possible answers on a set of intersecting axes. With this analytical framework in hand, we will be prepared to make sense of the policy calls the present secrecy regime has made (in Part II); we also will be able to critique those choices and recommend improvements that ensure a neater fit between the underlying values and the positive requirements of secrecy law (in Part III).

A. The Interests of Secrecy

Secrecy in national security investigations affects a wide array of competing interests. It serves the Executive Branch's operational interests in gathering intelligence effectively. It helps ensure that intelligence sources and methods are not compromised and that ongoing investigations of enemy agents are not disrupted. But secrecy comes at a price, often steep. It undermines the privacy interests of targets by preventing them from judicially challenging the surveillance. It harms the interests of third party witnesses in speaking about their experiences. It prevents the general public from checking government abuses of power and participating in democratic deliberation over the optimal national security policies. And it frustrates Congress's interests in engaging in effective oversight of the Executive Branch.[25]

The stew is even richer than this, for secrecy can interact with stakeholders' interests in unexpected ways. Those for whom secrecy ordinarily is anathema sometimes can find their interests vindicated by secrecy requirements, and vice versa. For instance, the Executive Branch's need to mount effective national security operations can actually be undermined by secrecy to the extent that such rules tend to foster bureaucratic rivalries and thus discourage cooperation. In the same way, sometimes a target's privacy interests can be vindicated by secrecy. It can prevent those who are suspected

Rossiter ed., 1961) ("There are cases where the most useful intelligence may be obtained, if the persons possessing it can be relieved from apprehensions of discovery. . . . The convention have done well, therefore, in so disposing of the power of making treaties that although the President must, in forming them, act by the advice and consent of the Senate, yet he will be able to manage the business of intelligence in such a manner as prudence may suggest.").

25. Efforts to protect national security at the expense of targets and third parties may be thought of as a wealth transfer from those groups to the public at large. In effect, a tax is levied that takes the form of burdens on privacy and speech interests, and the public reaps that tax's benefits in the form of the absence of deadly attacks. In many cases (i.e., where they are not complicit in the planned attacks the government seeks to foil), the targets and third parties themselves can be said to benefit from the tax, though probably not at a rate proportional to their contributions. *Cf.* Fuchs, *supra* note 16, at 151 (suggesting that "secrecy is most dangerous when the government targets small groups that lack the political clout to keep information in the public's hands").

of involvement in espionage or terrorism, but who later turn out to be innocent, from suffering public opprobrium and vigilante violence. And the bedrock public interest in acquiring the information necessary for democratic participation can give way to the still more fundamental interest members of the public have in not becoming victims of a foreign attack due to a harmful disclosure of sensitive information.

1. Executive Branch Operational Interests

Secrecy requirements implicate the Executive Branch's interests in conducting successful national security operations. These operational interests may be further subdivided into at least three categories. First, secrecy helps preserve what the Supreme Court has dubbed "the heart of all intelligence operations"[26]: the Executive's intelligence sources and methods, or information about the manner in which the government collects intelligence. Sources and methods—the who, when, where, and how of intelligence gathering—can include the name of a covert CIA operative, whether working at a desk in Langley or having infiltrated a hostile terrorist group overseas. The term also includes data about the identities of the targets who are under surveillance, technical details about devices used to intercept targets' communications, and many other types of information.

The compromise of sources and methods can have devastating consequences. Disclosure of the techniques used to gather information about foreign powers enables those entities to evade detection.[27] Revelation of sources and methods thus makes it more difficult for the United States to strike hostile foreign powers[28] and makes it easier for enemies to plot assaults against American interests.[29] One celebrated example of these harms occurred in the summer of 1942, when the *Chicago Tribune* and other newspapers broke the story that American cryptanalysts had broken a principal operational code of the Japanese Navy (known as "JN25b").[30] The

26. *Sims*, 471 U.S. at 167; *see also* United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) (stating that there is a "need to maintain the secrecy of lawful counterintelligence sources and methods" (quoting S. REP. NO. 95-701, at 15 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3983) (internal quotation marks omitted)); Swire, *supra* note 13, at 1367 ("The sources and methods used in foreign intelligence investigations are generally sensitive and require secrecy.").

27. *See* O'TOOLE, *supra* note 4, at 1 ("Obviously, such sources and methods must be protected by a cloak of secrecy if they are to continue to supply needed intelligence.").

28. *See* Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 933 (D.C. Cir. 2003) (emphasizing that disclosure of surveillance could enable hostile foreign powers to determine "which cells had been compromised," which in turn could enable them to draw "conclusions as to how [to] more adequately secure their clandestine operations in future terrorist undertakings"); Detroit Free Press v. Ashcroft, 303 F.3d 681, 706 (6th Cir. 2002) ("This information could allow terrorist organizations to alter their patterns of activity to find the most effective means of evading detection.").

29. *See* N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 218 (3d Cir. 2002) (indicating that publication of information about the entry of suspected terrorists into the United States "would allow [a terrorist organization] to tailor future entries to exploit weaknesses in the United States immigration system").

30. *See* MILLER, *supra* note 4, at 258, 262; Matthew M. Aid, *"Not So Anonymous": Parting the Veil of Secrecy About the National Security Agency*, *in* A CULTURE OF SECRECY: THE GOVERNMENT VERSUS

resulting intelligence was a key reason the United States prevailed at the Battle of Midway; American forces knew the details of Japan's attack plans and therefore were able to surprise and devastate the Japanese fleet, sinking four aircraft carriers.[31] But after the newspapers ran their stories, the Japanese high command switched to a different, unbroken cipher ("JN25c").[32] American cryptanalysts did not succeed in breaking the new code until early 1943.[33] The intervening months saw a string of defeats for the Pacific Fleet, and some historians blame those losses, at least in part, on the new difficulties the United States faced at listening in on Japanese communications.[34]

The Executive's interests in secrecy are even more compelling when the sources and methods at issue involve covert operatives. The Supreme Court has adverted to "the grim consequences facing intelligence sources whose identities became known."[35] That's putting it mildly. Spies who are detected by the powers they infiltrate face incarceration, interrogation, torture, and death.[36] It is estimated that Aldrich Ames, a CIA official who sold secrets to the Soviet Union, contributed to the deaths of at least ten American agents in the U.S.S.R.[37] Not only does the revelation of covert operatives' identities compromise their effectiveness as a source of intelligence for the United States (thereby undermining the government's operational interests), it also threatens those individuals with grave bodily harm or death (thereby implicating the government's interests in the well-being of its agents, not to mention the interests of those agents in their own lives).

Spectacular breaches of secrecy, like publishing an account of American cryptanalytic successes or leaking a spy's identity, are not the only ways to compromise sources and methods. Even seemingly innocuous disclosures can frustrate the Executive's operational interests. A fact that appears insignificant to the casual observer can reveal a great deal to a sophisticated intelligence agent well practiced in the art of espionage.[38] This is especially

---

THE PEOPLE'S RIGHT TO KNOW 60, 69 (Athan G. Theoharis ed., 1998) [hereinafter CULTURE OF SECRECY].

31. *See* CHARLES D. AMERINGER, U.S. FOREIGN INTELLIGENCE: THE SECRET SIDE OF AMERICAN HISTORY 142-43 (1990); MILLER, *supra* note 4, at 260-62. Admiral Chester W. Nimitz, commander of the Pacific Fleet, claimed that Midway "was essentially a victory of intelligence." *Id.* at 262.

32. *See* Aid, *supra* note 30, at 69.

33. *See* MILLER, *supra* note 4, at 289.

34. *See* Aid, *supra* note 30, at 69, 80 n.30.

35. CIA v. Sims, 471 U.S. 159, 172 (1985); *see also* Snepp v. United States, 444 U.S. 507, 512 (1980) ("The continued availability of these foreign sources depends upon the CIA's ability to guarantee the security of information that might compromise them and even endanger the personal safety of foreign agents."); Detroit Free Press v. Ashcroft, 303 F.3d 681, 705 (6th Cir. 2001) (indicating that public knowledge of the identity of informants may "eliminat[e] valuable sources of information for the Government and impair[] its ability to infiltrate terrorist organizations"); Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980) (explaining that "disclosure of the identity of [a covert agent] might expose him to adverse action from hostile powers").

36. *See, e.g.*, Matthew Cooper, *The Blameless World of Official Washington*, U.S. NEWS & WORLD REP., Oct. 10, 1994, at 6.

37. *Id.*; *see also* Fred Hiatt, *Russian Agent's Widow: A Shattered Life*, WASH. POST, Dec. 17, 1994, at A1.

38. *See Sims*, 471 U.S. at 178 ("Foreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identi-

true when an apparently trivial piece of information is coupled with others in the foreign power's possession. "[B]its and pieces of data 'may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself.'"[39] The risk is that a foreign power will be able to discern from the individual tiles the larger intelligence "mosaic."[40] (The mosaic theory of intelligence collection is hardly a modern innovation. George Washington embraced it during the Revolutionary War.[41])

Second, besides preserving the confidentiality of sources and methods, secrecy can prevent diplomatic embarrassment. It is only prudent that nations collect information about foreign governments, and not just the ones they count as enemies. Such surveillance is a way of acquiring intelligence about hostile nations in the possession of allied governments; it also helps officials plan for the contingency that a heretofore friendly nation will have a change of heart.[42] Public knowledge that such surveillance is taking place could jeopardize the relationship between those nations.[43] The dangers are even more acute when the target is a foe. Revelation that surveillance has taken place could furnish pretext for the country to take action against the United States' interests, such as expelling American citizens from its territory, initiating a trade embargo, or worse. America suffered severe embarrassment, and a summit between Khrushchev and Eisenhower was ruined,

---

ties of intelligence sources from seemingly unimportant details."); United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989) (warning that fragments of information may "make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods").

39. *Sims*, 471 U.S. at 178 (quoting *Halperin*, 629 F.2d at 150).

40. *See Detroit Free Press*, 303 F.3d at 706 ("The Government describes this type of intelligence gathering as 'akin to the construction of a mosaic,' where an individual piece of information is not of obvious importance until pieced together with other pieces of information." (quoting J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 604 (D.C. Cir. 1996))); *J. Roderick MacArthur Found.*, 102 F.3d at 604 (explaining that "intelligence gathering is 'akin to the construction of a mosaic;' to appreciate the full import of a single piece may require the agency to take a broad view of the whole work" (quoting *In re* United States, 872 F.2d 472, 475 (D.C. Cir. 1989)) (citation omitted)); United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) ("The significance of one item of information may frequently depend upon knowledge of many other items of information. What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."). *See generally* David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

41. *See* Letter from George Washington to Lord Stirling (Oct. 6, 1778), *in* 13 WRITINGS OF GEORGE WASHINGTON, *supra* note 1, at 39, 39 (John C. Fitzpatrick ed., 1936) ("Every minutiae should have a place in our collection, for things of a seemingly triffling [sic] nature when conjoined with others of a more serious cast may lead to very valuable conclusions.").

42. *See* Seymour M. Hersch, *Why Pollard Should Never Be Released*, THE NEW YORKER, Jan. 18, 1999, at 26, 27 ("Officials are loath to talk publicly about it, but spying on allies is a fact of life: the United States invests billions annually to monitor the communications of its friends. . . . The goal is not only to know the military and diplomatic plans of our friends but also to learn what intelligence they may be receiving and with whom they share information.").

43. *See Halperin*, 629 F.2d at 148 ("Exposure of a CIA operative in a foreign country can further lead to embarrassment for the United States and disruption of relations with foreign countries."); Swire, *supra* note 13, at 1323 ("Prudent foreign policy may suggest keeping tabs on foreign agents who are in the United States, but detailed disclosure of the nature of that surveillance could create embarrassing incidents or jeopardize international alliances.").

after a Soviet surface to air missile downed Francis Gary Powers's U-2 spy-plane over Sverdlovsk in 1960.[44]

Investigative secrecy also helps prevent the diplomatic embarrassment that can result when a foreign government or other entity is revealed to be cooperating with the United States. Secrecy enables foreign officials to assist American investigators when, for reasons of domestic anti-U.S. sentiment or other political considerations, they would prefer not to be seen publicly as aiding this country. Disclosure of such cooperation both would embarrass allies and dissuade them from assisting in the future. For instance, after American media organs in 2006 revealed that a European banking consortium was helping the United States track the financial transactions of suspected terrorists, numerous complaints were filed with E.U. member states charging the consortium with violating European data privacy laws.[45]

Third, secrecy furthers the Executive Branch's operational interests by preventing disruption to ongoing investigations. If a target discovers he is under surveillance, he might flee or go into hiding.[46] He might destroy evidence that implicates him in the plot or intimidate witnesses who have observed his malfeasance.[47] This in turn could prevent the government from learning the identities of other participants, as well as compromise its ability to bring criminal charges against the target. The target might create false evidence to throw investigators off his trail. The target might accelerate his plot, striking the intended target before the government is able to intercept him.[48] Responsibility for a planned attack might be shifted to another cell, perhaps a cell of which the government is not yet aware.[49] Finally, the target might alert his co-conspirators and cause them to take any of these measures.

Though secrecy is typically thought to advance the Executive Branch's operational interests, there are several ways in which it can harm the government's interests. Secrecy—both specific rules and the broader culture of secrecy they tend to foster—can result in individual and interagency rival-

---

44. *See* JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY: FROM THE COLD WAR THROUGH THE DAWN OF A NEW CENTURY 43-55 (2001); RIEBLING, *supra* note 11, at 155.

45. *See* Dan Bilefsky, *Rights Unit Challenges U.S. Over Bank Data*, INT'L HERALD TRIB., June 28, 2006, at 1.

46. *See* Katz v. United States, 389 U.S. 347, 355 n.16 (1967) (warning that a target's knowledge of surveillance could "provoke the escape of the suspect").

47. *See id.* (reasoning that disclosure could "provoke . . . the destruction of critical evidence"); Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 929 (D.C. Cir. 2003) ("A terrorist organization may even seek to hunt down detainees (or their families) who are not members of the organization, but who the terrorists know may have valuable information about the organization."); N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 203 (3d Cir. 2002) (cautioning that investigative targets might "obstruct or disrupt pending proceedings by destroying evidence [or] threatening potential witnesses").

48. *See Ctr. for Nat'l Sec. Studies*, 331 F.3d at 923 ("[R]elease of the information could endanger the public safety by making terrorist attacks more likely . . . ."); *N. Jersey Media Group*, 308 F.3d at 218 (warning that a foreign power "may accelerate the timing of a planned attack, thus reducing the amount of time the government has to detect and prevent it").

49. *See N. Jersey Media Group*, 308 F.3d at 218 ("If acceleration is impossible, it may still be able to shift the planned activity to a yet-undiscovered cell.").

ries that prevent national security players from sharing data and coordinating with one another. As Max Weber recognized, a principal mission of bureaucracies, and of officials within those entities, is to maintain and expand their own powers.[50] Secrecy is a means to that end. Persons who possess sensitive information will seek to preserve the secrecy of those data as a way of enhancing their standing in the eyes of their supervisors vis-à-vis other agency employees. The same is true of the bureaucracy writ large. An agency will refrain from sharing sensitive information with sister agencies, even when doing so is not unlawful, to ensure that decisionmakers regard it as the indispensable source of such information. Secrecy thus can precipitate a form of informational turf war.[51] This danger is especially acute in the national security context, in which various agencies (such as the FBI, CIA, and NSA) have overlapping responsibilities and thus have reason to regard one another as competitors.[52]

Recent history is replete with examples of when bureaucratic pride born of secrecy has dissuaded government officials from sharing information and coordinating their efforts. In the early 1990s, during the first stages of the Aldrich Ames investigation, the FBI asked CIA's Berlin station chief for access to files about Soviet moles that recently were acquired from the old East German security apparatus. The station chief—who was christened with the derisive nickname "the poison dwarf"—refused, and the FBI briefly flirted with seeking obstruction of justice charges against him.[53] And in early 2001, CIA failed to share with the FBI its knowledge that a man named Khalid al-Mihdhar—who was believed to have ties to the mastermind of the 2000 USS *Cole* bombing—held a U.S. visa and had traveled within the country.[54] Months later, al-Mihdhar would help hijack American Airlines Flight 77 and crash it into the Pentagon.

---

50. *See* MAX WEBER, *Bureaucracy*, *in* FROM MAX WEBER: ESSAYS IN SOCIOLOGY 196, 233-34 (H.H. Gerth & C. Wright Mills eds., trans., 1946) ("Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret."); *see also* DENNIS C. MUELLER, PUBLIC CHOICE II 250 (1989) ("Bureaucratic man pursues power. Economic man pursues profit. . . . Thus, there is a close link between the economic theory of profit and the political theory of power. Both exist owing to uncertainty; both accrue to the possessors of information.").

51. *See* DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 73 (1998) ("Departments and agencies hoard information, and the government becomes a kind of market. Secrets become organizational assets, never to be shared save in exchange for another organization's assets."); *see also* BAMFORD, *supra* note 44, at 384 (recounting the belief of a top CIA official that the National Security Agency "regularly and deliberately" withheld information "in order 'to make itself look good'").

52. *See* JAMES Q. WILSON, BUREAUCRACY 188-90 (1989) (describing natural rivalry between agencies that perform similar functions). *See generally* RIEBLING, *supra* note 11 (recounting antagonism between the FBI and CIA). Interagency antagonism is not without its benefits. Such rivalries can produce enhanced protection of civil liberties. In 1970, the NSA developed a plan to intercept, without a judicial warrant or probable cause, the international communications of American citizens who were anti-war activists. J. Edgar Hoover got wind of NSA's proposal and, fearing that the agency was encroaching on his turf, convinced the Nixon Administration to nix the plan. *See* BAMFORD, *supra* note 44, at 428-31.

53. *See* RIEBLING, *supra* note 11, at 414.

54. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 266-67 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf [hereinafter 9/11 COMMISSION REPORT]; *see also id*. at 181-82.

Secrecy threatens to harm the Executive Branch's operational interests in a second way. It can fuel conspiracy theories that breed distrust of government officials, thereby sapping public support for the Executive Branch's national security or foreign policy initiatives. "The government's obsession with secrecy creates a citizens' obsession with conspiracy."[55] If the Executive Branch indulges in secrecy too readily, it will find it more difficult to persuade citizens of the wisdom of a particular policy, for the public will doubt the government's veracity.

2. Targets' Privacy Interests

While secrecy can be essential to the success of national security investigations, it is no less true that secrecy can impose severe burdens on the interests of stakeholders other than the Executive Branch. For example, the privacy interests of investigative targets. Individuals have a basic interest in withdrawing into a private sphere where they are free from government observation. Those privacy interests are even stronger when they are coupled with interests in free speech—that is, when the investigation is based in part on the target's political or religious beliefs, or threatens to chill their expression.[56] The crucial point is not so much that the monitoring itself triggers privacy concerns, though that certainly is true. The point is that the secrecy attendant upon such surveillance imposes an even greater burden on the target's privacy interests. By preventing targets from learning that the government is gathering information about them, secrecy denies them the opportunity to contest the legality of the surveillance in court. It also prevents them from modifying their conduct and acting in a way that is not subject to observation. A target may not learn until years after the surveillance was undertaken that the government was watching him. If a secrecy rule is perpetual, and if the government ultimately decides not to initiate

55. Eleanor Randolph, *Is U.S. Keeping Too Many Secrets?*, L.A. TIMES, May 17, 1997, at 1 (quoting Paul McMasters); *see also* James X. Dempsey, *The CIA and Secrecy*, *in* CULTURE OF SECRECY, *supra* note 30, at 37, 37 ("Secrecy has a corrosive effect on the popular trust necessary for democracy to function."); Thomas M. Franck & Edward Weisband, *Introduction* to SECRECY AND FOREIGN POLICY 3, 8 (Thomas M. Franck & Edward Weisband eds., 1974) (identifying as a "cost of secrecy" the "loss of public support for government policy, such as occurs when there is a real or imagined 'credibility gap' based on evidence of frequent non-disclosure by a government"); Richard Gid Powers, *Introduction* to MOYNIHAN, *supra* note 51, at 58 ("What secrecy grants in the short run—public support for government policies—in the long run it takes away, as official secrecy gives rise to fantasies that corrode belief in the possibilities of democratic government.").

56. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313 (1972) (emphasizing that national security investigations "often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime"); *id.* at 320 (indicating that "[s]ecurity surveillances are especially sensitive because of . . . the temptation to utilize such surveillances to oversee political dissent"); *id*. at 314 ("Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs."); *cf.* Employment Div., Dep't of Human Res. of Or. v. Smith, 494 U.S. 872, 881-82 (1990) (recognizing that "hybrid" free exercise claims—i.e., where a free exercise claim is coupled with another claim, such as free speech or free association—are more forceful than unadorned free exercise claims).

public legal proceedings on the basis of the information acquired, the target might never learn about the intrusion.

Though privacy interests are implicated any time the government surveils a target, the Supreme Court has held that the precise strength of such interests depends on the relative intrusiveness of the investigative technique used to gather the information. Physical searches and electronic surveillance implicate privacy interests of the highest order. For centuries, searches via physical invasion, especially of the home, have triggered strong privacy concerns.[57] Physical intrusions are by no means the only types of searches that implicate privacy values,[58] but they are among the most sensitive. Real time investigative techniques like wiretapping may represent even more of an affront to privacy interests.[59] This is so because physical searches generally only uncover evidence of the target's past conduct (at least when, as often is the case in national security investigations, the search is conducted covertly when the target is not on the premises). Real time surveillance, by contrast, enables investigators to observe the target's conduct directly, as it occurs.[60]

Other investigative techniques—those that collect information that targets voluntarily handed over to third parties—represent lesser burdens on privacy interests. One example is the government's use of a pen register or trap and trace device to detect which numbers are dialed or received by a particular telephone; the user reveals that information to the phone company as a precondition of completing the call.[61] Because the target has compro-

57. *See* Silverman v. United States, 365 U.S. 505, 511 (1961) (reasoning that "[a]t the very core" of one's privacy interests "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion"); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) (stressing that "the search of the interior of homes" is "the prototypical and hence most commonly litigated area of protected privacy"); Payton v. New York, 445 U.S. 573, 589-90 (1980) ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home . . . ."); WILLIAM BLACKSTONE, 3 COMMENTARIES *288 (describing one's home as "his castle of defence and asylum").

58. *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978) (indicating that one's "capacity to claim the protection of the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place"); Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places.").

59. *See* Lopez v. United States, 373 U.S. 427, 471 (1963) (Brennan, J., dissenting) ("Electronic surveillance destroys all anonymity and all privacy; it makes government privy to everything that goes on."); Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) ("Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."), *overruled by Katz*, 389 U.S. 347, *and* Berger v. New York, 388 U.S. 41 (1967). *But see* United States v. Ehrlichman, 376 F. Supp. 29, 33 (D.D.C. 1974) (describing a wiretap as "a relatively nonintrusive search").

60. *See Kyllo*, 533 U.S. at 38 (explaining that a thermal imaging device "might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'").

61. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); *see also* Couch v. United States, 409 U.S. 322, 335 (1973) (finding no reasonable expectation of privacy in documents voluntarily given to accountant). Callers do not reveal to phone companies the content of their communications in the way they disclose the numbers dialed or received. Telecommunications carriers certainly have the capacity to intercept and record calls; modern pen/trap devices can be configured to collect content as well as trans-

mised his own privacy by sharing his affairs with a third party, any subsequent revelation of those affairs to investigators can be said to be a consequence of the target's initial decision to share information with an outsider. This is not to suggest, as the Supreme Court has held, that a target has *no* constitutionally cognizable privacy interest in data disclosed to others,[62] only that the interest in information turned over to large business entities is somewhat weaker than in information purposefully kept confidential or shared only among intimate acquaintances.

Not only will a target's privacy interests wax and wane depending on the investigative technique used, privacy interests may be uniformly less compelling in national security cases to the extent the targets are foreign nationals who claim few ties to this country other than mere physical presence. The Supreme Court has shown less concern for the privacy interests of aliens who are present in the United States only for a short time, or for transient purposes, than for those of American citizens or aliens who establish thick networks of reciprocal ties within their communities (for example, those who enter on immigrant visas).[63] International terrorists in particular may lack the full ties to the United States that qualify them for robust privacy interests, inasmuch as they are more likely to be temporary visitors to this country than American citizens or long term resident aliens. All nineteen of the 9/11 hijackers entered the United States on short term, nonimmigrant visas, such as student or work visas. And unlike England, which in July 2005 saw citizens unleash a series of suicide bombings in its capital city, the United States has not yet witnessed large numbers of citizens

actional data. *See, e.g.*, 147 CONG. REC. S10,372 (daily ed. Oct. 9, 2001) (statement of Sen. Leahy). But while federal law gives phone companies a relatively free hand to gather users' transactional information, *see* 18 U.S.C. § 2511(2)(h) (2000), it generally forbids them from collecting content, *see id.* § 2511(1). Given that prohibition, callers reasonably may expect the content of their calls to remain private.

62. *Cf.* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1576-82 (2004) (arguing that persons should not be held to surrender their reasonable expectations of privacy when they share information with certain third parties); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528-29 (2006) (same).

63. *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 261-65 (1990) (holding that a Mexican national, who was incarcerated at a pretrial detention facility in California, could not invoke the Fourth Amendment's guarantee against unreasonable searches and seizures to challenge a warrantless search by federal agents of his residences in Mexico, in part because, as a nonresident alien, he was not within the "class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community"); *id.* at 271 (affirming that "aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country"); Johnson v. Eisentrager, 339 U.S. 763, 770 (1950) ("The alien, to whom the United States has been traditionally hospitable, has been accorded a generous and ascending scale of rights as he increases his identity with our society."). *But see* David Cole, *Enemy Aliens*, 54 STAN. L. REV. 953, 978 (2002) ("[R]elatively little turns on citizenship status. The right to vote and the right to run for federal elective office are restricted to citizens, but all of the other rights are written without such limitation."); Kal Raustiala, *The Geography of Justice*, 73 FORDHAM L. REV. 2501, 2523 (2005) ("It does not take numerous years of residence, or even intent to naturalize, to enjoy many constitutional rights. Aliens who have spent almost no time in the United States are treated, for most purposes, the same as those who have lived here for years." (footnote omitted)).

mounting terrorist operations in this country on behalf of international terrorist groups like al Qaeda.

Counterintuitively, there are several ways in which secrecy can advance a target's privacy interests. First, investigative secrecy helps ensure that persons whom the government initially believes are threats to the national security, but who later are discovered to be innocent, are not unfairly stigmatized and do not face physical violence at the hands of vigilantes.[64] The privacy interest here is not in keeping information from the government but from the general public. For instance, in connection with its investigation of the September 11 attacks, the FBI took into custody a San Antonio radiologist named Al-Badr Al-Hazmi, who was thought (wrongly, it turned out) to have ties to two of the 9/11 hijackers, brothers Nawaf and Salem Al-Hazmi. Dr. Al-Hazmi was cleared several weeks later, but not before the government's suspicions were splashed all over the news media. Upon his release, Dr. Al-Hazmi was so concerned about his family's safety he hired a security firm to protect his home each night.[65] In such cases, the target's privacy interests are aligned with the Executive's interests in secrecy.[66]

Second, investigative secrecy can prevent the chilling effect that often occurs when the government's surveillance activities are publicly known. If one believes that the government is monitoring one's activities, one will tend, at the margins, to act in ways that are thought to meet with governmental approval. (At least where one places a higher value on avoiding government sanctions, discounted by the probability that they will be imposed, than on acting autonomously.) Monitoring thus "threatens . . . to chill the expression of eccentric individuality."[67] But conduct can only be chilled if

64. *See* Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 923 (D.C. Cir. 2003) (indicating that terrorism "detainees have a substantial privacy interest in their names and detention information because release of this information would associate detainees with the September 11 attacks, thus injuring detainees' reputations and possibly endangering detainees' personal safety"); N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 218 (3d Cir. 2002) (emphasizing that targets "have a substantial privacy interest in having their possible connection to the ongoing investigation kept undisclosed," given the "stigma concern[s]"). A similar concern that the government not unfairly stigmatize private persons is present, albeit inconsistently, in the Supreme Court's due process jurisprudence. *See* Paul v. Davis, 424 U.S. 693, 697 (1976) (acknowledging that state police officers who distributed flyers describing plaintiff as an "active shoplifter" caused plaintiff to be "suspected of shoplifting" and thereby "impair[ed] his future employment opportunities," but holding that such stigma did not implicate any liberty interest under the Due Process Clause); Wisconsin v. Constantineau, 400 U.S. 433, 437 (1971) (holding that state officials could not, consistent with the Due Process Clause, designate plaintiff without a prior hearing as a person to whom alcoholic beverages may not be sold, in part because "[t]he label is a degrading one," and "[w]here a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential").

65. *See* Ellise Pierce, *Coming Home*, NEWSWEEK, Oct. 3, 2001, http://www.msnbc.msn.com/id/3067606/site/newsweek/from/RL.2/.

66. The notion that secrecy vindicates target privacy interests is more persuasive in the surveillance context than in others where it has been offered, such as to justify the government's reluctance to release the names of "special interest" aliens detained in the 9/11 investigation. *See, e.g.*, *N. Jersey Media Group*, 308 F.3d 198; Detroit Free Press v. Ashcroft, 303 F.3d 681 (6th Cir. 2002). In those settings, persons' privacy interests can be vindicated by giving them the choice whether to publicize information about them. It would not be practicable to give targets such a choice here. Doing so necessarily would alert them to the fact that they are under investigation.

67. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L.

the actor believes that investigators are watching; if an individual has no reason to think he is being surveilled, he likely will continue to act according to his unalloyed preferences.[68] By keeping a target unaware that the government is monitoring him, secrecy thus removes the incentive to act consistent with one's estimation of what the government approves.

3. Third Party Speech Interests

When the Executive Branch asks third parties to assist national security investigations—for example, by turning over information concerning the target or by furnishing technical assistance in conducting the surveillance—it typically seeks to bind those third parties to secrecy. Secrecy requirements profoundly affect the speech interests of third parties who wish to publicly discuss their experiences. A rule barring a third party from publicizing certain facts in her possession amounts to a prior restraint on speech. Such restrictions have been regarded as imposing particularly harsh burdens on speech interests at least since the days of Blackstone, and American law historically has deplored them.[69] In fact, nondisclosure obligations may be even more burdensome than the standard issue prior restraint. The archetypical prior restraint is a licensing scheme under which speech may not occur unless a government functionary gives advance approval.[70] Such schemes present the danger that the licensor will approve or deny applications based on his agreement with, or distaste for, the views to be expressed[71]; but at least there is a possibility that the licensor may approve the

---

REV. 1373, 1426 (2000); *see also* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1268 (2004) (emphasizing that "surveillance can lead to self-censorship and inhibition").

68. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 27 (2004) ("Even if our government *is* watching us, if we don't know about it, in some sense it cannot hurt us—so long as we are never prosecuted or otherwise harmed by the disclosure."); Solove, *supra* note 62, at 495 (emphasizing that "awareness of the possibility of surveillance can be just as inhibitory as actual surveillance").

69. *See* Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976) ("[P]rior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights."); N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) ("Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963)) (internal quotation marks omitted)); 4 BLACKSTONE, *supra* note 57, at *151 ("The liberty of the press . . . consists in laying no *previous* restraints upon publications . . . ."); *id*. at *152 ("To subject the press to the restrictive power of a licenser . . . is to subject all freedom of sentiment to the prejudices of one man, and make him the arbitrary and infallible judge of all controverted points in learning, religion, and government.").

70. *See* Lovell v. City of Griffin, 303 U.S. 444, 451 (1938) (characterizing a municipal ordinance under which no literature could be distributed without government permission as "strik[ing] at the very foundation of the freedom of the press by subjecting it to license and censorship," and emphasizing that "[t]he struggle for the freedom of the press was primarily directed against the power of the licensor").

71. *See* Forsyth County v. Nationalist Movement, 505 U.S. 123, 133 (1992) (stating that "[n]othing in the [licensing] law or its application prevents the official from encouraging some views and discouraging others through the arbitrary application of fees," and stressing that "such unbridled discretion" poses a grave threat to speech interests); City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 757 (1988) ("[A] licensing [scheme] placing unbridled discretion in the hands of a government official or agency constitutes a prior restraint and may result in censorship.").

would be speaker's request. Not even that cold comfort is available to a third party on the receiving end of a nondisclosure obligation. Such secrecy rules categorically rule out any speech.[72]

The precise strength of a third party's speech interests hinges on the origins of the information whose disclosure the government seeks to prevent. The most burdensome restriction is one that bars a third party from revealing information she acquired on her own, apart from any interactions she may have had with government investigators. Such restrictions strike at the heart of a third party's speech interests.[73] For this reason, the Supreme Court, in *Landmark Communications, Inc. v. Virginia*, struck down a state law that prohibited the disclosure of any proceedings before a commission investigating charges of judicial misconduct, including information that would be speakers acquired through means other than their involvement in the commission's proceedings.[74]

Somewhat gentler are restrictions that prevent the third party from publicizing facts she obtained only by participating in the government's investigation—for example, the fact that the FBI served a subpoena on her or asked her to install a wiretap.[75] The third party did not possess the informa-

72. *See* Doe v. Gonzales, 386 F. Supp. 2d 66, 74 (D. Conn. 2005) ("The suppression of speech [authorized by an NSL secrecy rule] is broader than any licensing scheme. It constitutes a categorical prohibition on the use of any fora for speech, on all topics covered by [the statute], as contrasted with a licensing scheme, which limits only a particular forum."), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006); Doe v. Ashcroft, 334 F. Supp. 2d 471, 512 (S.D.N.Y. 2004) (reasoning that "a blanket permanent prohibition on future disclosures," as under an NSL secrecy rule, "is an even purer form of prior restraint than a licensing system in which the speaker may at least potentially obtain government approval and remain free to speak"), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

73. *See* Butterworth v. Smith, 494 U.S. 624, 636 (1990) (Scalia, J., concurring) ("I think there is considerable doubt whether a witness can be prohibited, even while the grand jury is sitting, from making public what he knew before he entered the grand jury room.").

74. 435 U.S. 829, 838 (1978) (stressing that the state's effort to bar witnesses from publicizing facts independently in their possession strikes "near the core of the First Amendment").

75. To say that restrictions on underlying facts are more burdensome than those on investigative facts is not to suggest that barring third parties from disclosing investigative facts is not onerous. Quite the contrary. The Executive essentially is dragooning third parties into its service, *cf.* Printz v. United States, 521 U.S. 898, 935 (1997) (holding that the Constitution bars the federal government from conscripting state officers), and then forbidding them from speaking about their impressment. Restrictions on publicizing investigative facts can be problematic indeed, especially when coupled with the public's independent interest in learning about its government's actions, and especially given the First Amendment's central purpose of facilitating speech about the government. If we focus on the *content* of the protected information (information concerning the government's activities vs. information concerning private conduct), we might well conclude that limits on speech about investigative facts are the least tolerable. By contrast, a focus on the information's *origins* (acquired at the government's discretion vs. acquired on one's own) would regard underlying facts restrictions as more onerous. The latter orientation may well be the appropriate one because in related contexts, courts have emphasized the government's decision to share information when deciding whether the recipients may be bound to secrecy. Former CIA officials can be made to submit book manuscripts to the agency for review for classified information, in part because the former officials acquired that data at the government's discretion. *See, e.g.*, United States v. Marchetti, 466 F.2d 1309, 1311 (4th Cir. 1972). Such a licensing scheme would be anathema if applied to persons who acquired the same information independently—e.g., the New York Times in the *Pentagon Papers* case. Of course, a third party (who has no choice but to assist the government's investigation) is not in precisely the same position as a prospective CIA employee (who, because she has the option of declining employment, can be deemed to have consented to the agency's policy of screening manuscripts).

tion before she was contacted by the government and possesses it now only because the government in its discretion has chosen to reveal it to her. In some sense, the government can be said to have a reversionary interest in the information that entitles it to control its further distribution.[76] This is why the Supreme Court, in *Seattle Times Co. v. Rhinehart*, upheld a court order barring civil litigants (including the defendant newspaper, which did not initiate the litigation) from publicizing information they obtained solely through discovery proceedings overseen by the court.[77]

4. Interests of the Public

The public has an interest of the highest order in ensuring that the Executive Branch does not abuse its powers to investigate and counteract threats to the national security. The potential for such abuses is especially great in national security investigations, and not just because the legal standards for gathering information tend to be more relaxed than in the criminal context. Persons who are believed to pose threats to the national security often are motivated by particular creeds, political or otherwise. The risk therefore exists that investigators will target them for surveillance on the basis of their beliefs, including persons who are not security threats but whose views are thought to resemble those of individuals who are.[78] Yet secrecy, by shielding the government's actions from public view, prevents the public from serving as this essential check on Executive Branch overreaching.[79] One reason the notorious abuses of the 1960s and 1970s were allowed to persist for so long was that they took place out of the public's eye.[80]

Not only does secrecy prevent the public from correcting past abuses, it also removes an incentive for Executive Branch officials to avoid future misdeeds. Government officials are less likely to misbehave if they know

76. *See Butterworth*, 494 U.S. at 636 (Scalia, J., concurring) (explaining that a grand jury witness's knowledge about grand jury proceedings "is knowledge he acquires not 'on his own' but only by virtue of being made a witness," and observing that such information "is in a way information of the State's own creation").

77. 467 U.S. 20, 32 (1984) ("As in all civil litigation, petitioners gained the information they wish to disseminate only by virtue of the trial court's discovery processes. . . . Thus, continued court control over the discovered information does not raise the same specter of government censorship that such control might suggest in other situations."); *id.* at 37 (emphasizing that the court's protective order did "not restrict the dissemination of the information if gained from other sources").

78. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 314 (1972).

79. *See* Grossjean v. Am. Press Co., 297 U.S. 233, 250 (1936) (stressing that "informed public opinion is the most potent of all restraints upon misgovernment"); Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 937-38 (D.C. Cir. 2003) (Tatel, J., dissenting) (describing "the public's interest in knowing whether the government, in responding to the attacks, is violating the constitutional rights of the hundreds of persons whom it has detained in connection with its terrorism investigation"); Detroit Free Press v. Ashcroft, 303 F.3d 681, 703-04 (6th Cir. 2002) (observing that "public access acts as a check on the actions of the Executive by assuring us that proceedings are conducted fairly and properly").

80. *See infra* notes 109-113 and accompanying text.

their actions are a matter of public record.[81] Just as a private citizen's conduct can be chilled by the suspicion that investigators are monitoring him, so can a government official's conduct be chilled by the recognition that his actions soon will be exposed to public scrutiny. Secrecy eliminates this incentive. Executive officials who are secure in the knowledge that they are operating out of the public eye will have one fewer reason—the threat of public embarrassment or, worse, individual civil or criminal liability—to exercise their powers with due attention to civil rights and liberties.

Secrecy both prevents the correction of wrongs and impedes the realization of positive goods. Government secrecy encourages suboptimal legal rules by denying citizens the opportunity to play a meaningful role in formulating the United States' national security policies. Information is essential to policymaking.[82] Yet citizens cannot engage on the issues of the day if their government keeps them in the dark. One cannot determine whether the techniques the Executive uses to investigate national security threats are proving effective unless one is familiar with the nature and scope of the government's investigative activities. Nor can one determine the appropriate balance between the needs of national security investigators and the requirements of civil liberties. Because sound policy is more likely to result when a multiplicity of voices have a say in its formulation,[83] secrecy can result in lower quality rules. And quite apart from its deleterious effects on the formulation of particular policies, secrecy undermines the ability of citizens to engage in democratic deliberation and participate in republican self-government.[84]

Yet the public's interests are not invariably advanced by disclosure. There are occasions when secrecy furthers the interests of the general public by preventing the release of sensitive information that could compromise the national security and imperil lives. Suppose a newspaper reports the location of a company of American soldiers in Afghanistan. Having read the

---

81. The insight that public awareness inevitably will alter officials' behavior often is cited by the Executive to justify the deliberative process privilege. *See* United States v. Nixon, 418 U.S. 683, 705 (1974) ("Human experience teaches that those who expect public dissemination of their remarks may well temper candor with a concern for appearances and for their own interests to the detriment of the decisionmaking process."); *see also* Neal Kumar Katyal, *The Public and Private Lives of Presidents*, 8 WM. & MARY BILL RTS. J. 677, 688 (2000) (explaining that the deliberative process privilege "ensures that the advice the President receives is candid and frank").

82. *See Ctr. for Nat'l Sec. Studies*, 331 F.3d at 938 (Tatel, J., dissenting) (emphasizing that "an informed citizenry is 'vital to the functioning of a democratic society'" (quoting NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978))); Stanley Futterman, *What is the Real Problem with the Classification System?*, *in* NONE OF YOUR BUSINESS, *supra* note 21, at 93, 94 ("There is no democracy without a concerned public, and there can be no concern about that which is not known. If a system of secrecy is working at high efficiency, the public will not even know that it does not know.").

83. *See, e.g.*, Fuchs, *supra* note 16, at 139 ("Openness can improve bureaucratic decisionmaking by allowing criticism of poor or inadequate analysis. It can also temper extremist viewpoints by exposing them to public scrutiny."). *See generally* CASS R. SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH (1993).

84. *See Detroit Free Press*, 303 F.3d at 704 (observing that public disclosure "helps ensure that 'the individual citizen can effectively participate in and contribute to our republican system of self-government'" (quoting Globe Newspaper Co. v. Superior Court, 456 U.S. 596, 604 (1982))).

press account, a group of al Qaeda and Taliban remnants ambush the unit and slaughter them. Members of the general public—to say nothing of the soldiers' family and friends—will find little comfort in knowing they had access to secrets that could inform foreign policy deliberations. The harms that typically result from releases of sensitive information may be less dramatic and more temporally remote. But in circumstances where such disclosures do in fact come at the cost of lost lives, the public's interest lies with secrecy, not openness.[85]

5. Congressional Oversight Interests

Discussions of secrecy often proceed in Manichean fashion, with the interests of the government pitted against those of private entities. But "the government" is no more of an undifferentiated whole than "the public" is. Congress certainly shares the Executive Branch's operational interests in effective national security operations, and secrecy certainly helps to advance them. But the national legislature also has a separate set of interests that necessarily conflict with those of the Executive—namely, in meaningful congressional oversight of the Executive Branch. Those interests cannot be vindicated if Congress lacks information about the nature and scope of the Executive's investigative activities.[86]

First, secrecy frustrates Congress's interest in ensuring that Executive agents faithfully execute the law and refrain from abusing their investigative powers. In other words, Congress can act as a surrogate for the targets and third parties whose privacy and speech interests may be imperiled by Executive overreaching. Second, secrecy denies Congress the information it needs to assess the effectiveness of the Executive's investigative techniques. Congress cannot intelligently debate legislation that would grant new powers to investigators, or that would restrict old ones, unless it knows how useful the existing investigative tools in the Executive's arsenal have proven.

Familiar public choice principles instruct that, as is true any time Congress makes policy that affects industry or public interest groups, there is the possibility of capture. But it seems probable in this context that Congress will be moved in the direction of more aggressive oversight, not less.

---

85. *See* Scott Shane, *A History of Publishing, and Not Publishing, Secrets*, N.Y. TIMES, July 2, 2006, § 4, at 4 (recounting the view of the late Katharine Graham, former publisher of the *Washington Post*, that a 1983 disclosure that American intelligence officers were intercepting communications between Syrian terrorists and their Iranian sponsors—and the subsequent cessation of that traffic—may have contributed to the bombing of Marine barracks in Beirut and the death of 241 Americans); *cf.* ALEXANDER M. BICKEL, THE MORALITY OF CONSENT 81 (1975) ("The game similarly calls on the press to consider the responsibilities that its position implies. *Not everything is fit to print*." (emphasis added)).

86. *See* Morton H. Halperin & Jeremy J. Stone, *Secrecy and Covert Intelligence Collection and Operations*, *in* NONE OF YOUR BUSINESS, *supra* note 21, at 105, 117 ("The executive branch thrives on secrecy because secrecy frees it from Congressional, judicial, and public oversight. But the Congress suffers from secrecy because its power is based on the ability to expose, to rally public opinion, to maintain a dialogue between constituents and elected officials and with the press.").

The industries that often are asked to assist the government in national security investigations—e.g., banks and telecommunications providers—may not have any direct interest in shielding their customers from surveillance. But they do care about maintaining customer goodwill, which could lead them to vindicate derivatively their customers' privacy interests. They also have interests in minimizing the compliance costs that result from government demands, as well as protecting trade secrets from being compromised. For instance, in early 2006, Google resisted a Justice Department subpoena seeking information about search terms entered by users; DOJ wanted the information in connection with its defense of the Child Online Protection Act, which bans certain types of pornography.[87] The same incentives may well be at work in the national security context. To the extent industry players calculate that the costs of pressuring Congress to discourage Executive Branch overreaching will be less than the costs of complying with investigators' requests, they will chart the former course.

It is possible to vindicate Congress's oversight interests in a way that accommodates the Executive's operational need for secrecy. Oversight can be conducted behind closed doors in the form of classified hearings by designated congressional committees. Congressional policymakers thus are able to receive the information they need to assess the effectiveness of investigations and to ensure the proper respect is shown to civil liberties, while at the same time preventing damaging public disclosures of sensitive information. (This is not a perfect solution, of course, as legislative secrecy prevents members of the public from effectively overseeing Congress itself.) In such circumstances, Congress may be said to be acting as the trustee of a blind trust, of which members of the public are the beneficiaries.

The following table depicts the ways in which investigative secrecy alternately can vindicate or frustrate the interests of various stakeholders:

	Interests vindicated by secrecy	Interests frustrated by secrecy
Executive Branch	(1) Protects sources and methods (2) Prevents diplomatic embarrassment (3) Avoids disruption to investigations	(1) Fosters interagency rivalries (2) Encourages conspiracy theories
Investigative Targets	(1) Protects the innocent from stigma and violence (2) Prevents chilling effect	(1) Prevents target from challenging surveillance in court (2) Prevents target from altering conduct
Third parties	n/a	(1) Bars third parties from speaking
Public	(1) Prevents disclosures that precipitate enemy attacks	(1) Eliminates check on Executive abuses (2) Inhibits democratic deliberations
Congress	n/a	(1) Eliminates check on Executive abuses (2) Denies information needed to legislate

87. *See* Katie Hafner, *U.S. Limits Demands on Google*, N.Y. TIMES, Mar. 15, 2006, at C1.

B. Toward a Taxonomy of Secrecy Rules

The diversity of these conflicting interests is only one reason why the analysis of secrecy in national security investigations is so complex. Any secrecy regime must choose from a wide range of policy options—e.g., what sort of information should be kept from disclosure? How long should secrecy endure? This subpart develops a taxonomy of secrecy by identifying some of the significant issues that must be addressed if one were to craft a secrecy regime on a blank slate, and by tracing the menu of policy choices that lie along each axis. These axes measure (1) the harms to be prevented; (2) the information to be protected; (3) the showing required before secrecy is imposed; (4) the breadth of a secrecy requirement; and (5) the duration of secrecy.

The first axis concerns the harms secrecy is designed to avert. Certain threats are present in all national security investigations, regardless of what technique the Executive Branch uses to collect information. There is the risk that disclosure of the surveillance will compromise intelligence sources and methods, thereby enhancing the ability of hostile powers to mount attacks against American interests and undermining the United States' ability to use force against her enemies. There is also the risk that revealing the intelligence gathering will alert targets that the government is on their trail, thereby disrupting an ongoing investigation. These harms essentially are coterminous with the Executive Branch operational interests recounted in Part I.A.1.

In addition, certain unique dangers arise when the government uses what Orin Kerr has called "prospective" surveillance techniques (which collect intelligence in real time, as it is being created), as differentiated from "retrospective" methods (which collect information that was created previously and now is being stored in some format).[88] A classic example of retrospective surveillance is the execution of a search warrant at a residence seeking tangible evidence that a crime has been committed. In the modern world, prospective surveillance often takes the form of wiretaps and email interception,[89] but the technique has been around for centuries in the form of undercover agents and confidential informants.

The additional risk with prospective surveillance is that disclosure of the monitoring will prevent the creation of the information sought in the first place. If a target knows that the government is eavesdropping on his communications, he either will refrain from undertaking those communica-

88. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 616-18 (2003) (distinguishing between prospective and retrospective surveillance); *see also* Mulligan, *supra* note 62, at 1566 (same).

89. *See* Mulligan, *supra* note 62, at 1558 (discussing "traditional voice communications over a wire, which, because of its ephemeral nature, can only be accessed by eavesdropping in real time or through the cooperation of a party to the communication"); *see also* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1381 (2004) (discussing internet surveillance); Kerr, *supra* note 88, at 616-18.

tions at all or will engage in them only through methods he is certain the government is not observing.[90] Perhaps the most celebrated example of these harms comes from the *9/11 Commission Report*. Shortly after the United States in August 1998 launched cruise missile strikes against terrorist bases in Afghanistan, a newspaper revealed that American investigators were aware that al Qaeda leader Osama bin Laden used a satellite telephone to communicate with his associates; bin Laden abruptly stopped using the phone and investigators lost the ability to eavesdrop on his conversations.[91] Any secrecy regime must decide how to account for the unique harms that are threatened when the Executive Branch engages in prospective surveillance.

The second axis concerns the nature of the information the secrecy regime seeks to keep confidential. A third party who is asked to assist a national security investigation will have any number of types of information in hand.[92] Imagine that an Assistant United States Attorney serves a grand jury subpoena duces tecum on a wireless telephone provider seeking information about a particular customer's cell phone usage. The company will have the underlying facts in which the government is interested—e.g., the rough physical location of the subscriber's phone at any given moment,[93] the numbers dialed and received by the phone, the method by which the subscriber's bills are paid, and the account's billing address. The company also will have certain information about the nature of the investigation. It will know that an investigation is underway and that the government has decided to use the particular investigative technique of grand jury subpoenas. It will

90. *See* Katz v. United States, 389 U.S. 347, 355 n.16 (1967) (indicating that, "if [the target] had been told in advance that federal officers intended to record his conversations, the point of making such recordings would obviously have been lost; the evidence in question could not have been obtained"); United States v. Belfield, 692 F.2d 141, 144 n.5 (D.C. Cir. 1982) ("The use of ordinary search warrants would not have been practicable for electronic surveillance, since such warrants must be served before the search is conducted."); Swire, *supra* note 13, at 1359 ("The need for secrecy flows specifically from the recognition that the ongoing usefulness of the wiretap will disappear if its existence becomes known.").

91. *See* 9/11 COMMISSION REPORT, *supra* note 54, at 127 ("Worst of all, al Qaeda's senior leadership had stopped using a particular means of communication almost immediately after a leak to the *Washington Times*. This made it much more difficult for the National Security Agency to intercept his conversations." (footnote omitted)). Some have suggested that the account of bin Laden's satellite phone going dark is an urban legend. The 1998 press accounts that are said to have tipped-off bin Laden did not mention that Americans were listening in on his satellite phone conversations, only that the al Qaeda leader was known to use such a device. And that information appears to have been already in the public domain; media organs had reported bin Laden's satellite phone use as far back as 1996. *See* Glenn Kessler, *File the Bin Laden Phone Leak Under "Urban Myths,"* WASH. POST, Dec. 22, 2005, at A2. Of course, bin Laden may have missed the earlier press accounts and may have inferred from the fact that investigators knew about his satellite phone that they were tapping it.

92. *See, e.g.*, Kamasinski v. Judicial Review Council, 44 F.3d 106, 110 (2d Cir. 1994) (identifying three classes of information to which a secrecy rule conceivably could apply: (1) "the substance of an individual's . . . testimony"; (2) "the witness's disclosure of the *fact* that testimony was given"; and (3) "information that an individual learns by interacting with the [government], such as information gained by hearing the testimony of other witnesses"). The second and third classes are both instances of "investigative facts."

93. *See* Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, N.Y. TIMES, Dec. 10, 2005, at A1.

be able to infer that someone using its subscriber's phone either is a target of the investigation or has been in contact with a target.

Any secrecy regime must decide which of these various categories of information should be subject to confidentiality requirements and which should not. At one end of the axis we would find restrictions on the third party publicizing what might be called "investigative facts," i.e., facts about the nature and status of the government's investigation. These would include the fact that government agents contacted the third party, that the third party was ordered to turn over certain information, that the order took the form of a grand jury subpoena, that the third party complied with the order, and so on. Investigative facts essentially are information about the Executive Branch's intelligence sources and methods. The third party's free speech interests are only minimally impacted by restrictions on disclosing investigative facts because the government chose to convey the information to her.[94]

At the far end of the axis is a prohibition on the third party disclosing facts she possesses quite apart from her participation in the investigation. These "underlying facts" are precisely what the government is interested in acquiring—in our hypothetical, the information about the target's use of the cell phone, method of payment, and so on. The third party's free speech interests are at their apogee here. Few burdens on a third party's free speech interests are as severe as a restriction on disclosing underlying facts she came to know through means other than her interactions with government investigators.

A third axis concerns the mechanism by which secrecy requirements are imposed. The most modest policy choice on this axis is a rule in which nondisclosure obligations are available only if the government can demonstrate (via certification or to a court), in addition to the showing needed to justify surveillance at all, a special need for secrecy. The analysis proceeds in two steps. The first question is whether the government should be permitted to conduct the surveillance. If the answer to that inquiry is yes, a second question is considered: whether the information gathering should be conducted in secrecy. The default position thus is openness and transparency, and secrecy is no more than an occasional exception. A typical special showing requirement is found in the Stored Communications Act, which entitles the government to access the contents of wire or electronic communications that are kept by a "remote computing service."[95] The default rule is that investigators must provide prior notice to the target,[96] but the government may delay if it convinces the court that immediate notification "may" produce a specified "adverse result."[97]

94. *See supra* notes 76-77 and accompanying text.
95. 18 U.S.C. § 2703(b)(1) (2000).
96. *See id.* § 2703(b)(1)(B).
97. *See id.* § 2705(a)(1)(A). The requisite "adverse results" include "endangering the life or physical safety of an individual" and precipitating "flight from prosecution." *Id.* § 2705(a)(2)(A)-(B).

At the mid-point of the third axis are rules under which the government presumptively is entitled to impose secrecy obligations on third parties, but those obligations could be suspended where a supervising entity deems them unwarranted. This species of secrecy rule collapses the two discrete questions—May the government surveil? May the government require secrecy?—into a single inquiry. Yet it retains an escape valve through which the critical second question can be addressed in isolation. When determining whether a proposed secrecy requirement is justified, the decisionmaker would be in a position to consider not only the strength of the Executive's operational interests but also how those interests interact with (and whether they are trumped by) the interests of other stakeholders.[98] Federal Rule of Criminal Procedure 6(e) is a good example. It generally bars certain persons associated with the grand jury process from "disclos[ing] a matter occurring before the grand jury," but it also affords the supervising court discretion to authorize disclosure of protected information in certain circumstances.[99]

The ground at the far end of the axis is held by automatic secrecy rules, the most draconian policy choice available. To impose a nondisclosure obligation, the government need not make any particular showing above what it must demonstrate to engage in surveillance in the first instance. Simply by demonstrating its legal entitlement to conduct surveillance, the government thereby would be permitted to bind third parties to secrecy. This sort of secrecy rule merges the two inquiries, and no mechanism exists to evaluate in isolation the propriety of secrecy. FISA's business records subchapter is an example of an automatic secrecy rule. That authority, which enables investigators to acquire "tangible things" from third parties, contains no mechanism by which the FISA court at the time of issuance could decline to require secrecy.[100]

The precision of a nondisclosure requirement is measured by a fourth axis. A secrecy rule could take the form of an indeterminate standard directing entities to maintain the confidentiality of the surveillance. For example, FISA's electronic surveillance authority imposes on third parties an obligation to act "in such a manner as will protect its secrecy"—i.e., the secrecy of the surveillance—but leaves the rule's precise scope somewhat opaque.[101] Alternatively, a secrecy obligation could take the form of a categorical prohibition on engaging in particular conduct. Thus the Federal Wiretap Act—the criminal law counterpart of FISA's electronic surveillance tool—broadly prohibits third parties from revealing the fact that surveillance is underway: "*No* . . . specified person shall disclose the existence of *any* in-

98. *Cf.* N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 217 (3d Cir. 2002) (stressing that, in analyzing whether public access to deportation proceedings involving alleged terrorism suspects plays a "significant positive role," "the calculus must perforce take account of the flip side—the extent to which openness impairs the public good" (internal quotation marks omitted)); *id*. at 224 (Scirica, J., dissenting) (agreeing with the majority on this point).

99. *See* FED. R. CRIM. P. 6(e)(2)(B).

100. *See* 50 U.S.C. § 1861(d) (2000).

101. *Id.* § 1805(c)(2)(B).

terception or surveillance . . . ."[102] The sweeping breadth of categorical rules can be mitigated by statutory carve-outs. Thus the NSL statutes permit third parties to reveal that investigators have sought records to legal counsel or to persons whose assistance is necessary to facilitate compliance with the demand.[103]

Secrecy rules taking the form of indeterminate standards are somewhat less burdensome than categorical prohibitions. Indeterminate standards do not clearly proscribe the entire universe of possible disclosures, only that subset that would compromise the overall confidentially of the surveillance. Arguably, such rules implicitly contemplate that certain disclosures are permissible—namely, those that stop short of undermining the investigation's overall secrecy. Thus a corporate agent who is served with an order directing the company to turn over information to investigators conceivably could divulge that request to her supervisors, as well as to the company personnel who have immediate possession of the information sought. More trivially, our corporate agent conceivably could reveal the government's request to her friends in a casual conversation. None of these disclosures would alert investigative targets or the general public that the government is engaged in monitoring, and thus they arguably would be consistent with an indeterminate "protect secrecy" directive. Categorical secrecy requirements draw no such fine distinctions. On their face, they purport to ban *all* disclosures to *all* entities for *any* reason. Our corporate agent would not be allowed to tell her friend about the investigators' demand for information, nor would she be permitted to alert the company employees responsible for processing such requests.

The fifth axis measures the duration of a secrecy requirement. The near side of the axis is occupied by secrecy rules that persist only temporarily. Temporary secrecy rules come in a variety of forms. They can feature date certain requirements, under which secrecy expires after a specified period of time. The Federal Wiretap Act is an example; it requires notice to targets no later than ninety days after the surveillance ends.[104] Temporary rules also can feature review mechanisms, which permit supervisors (whether the Executive or a court) to cancel secrecy when no longer justified. Thus the pen/trap statute imposes a nondisclosure obligation that ordinarily is permanent but may be lifted when "otherwise ordered by the court" overseeing the surveillance.[105] Or they can feature both date certain requirements and review mechanisms, like the Executive Order governing declassification of sensitive national security information.[106] The severity of any given temporary secrecy rule will depend on the precise form it takes. Hybrid rules—

102. 18 U.S.C. § 2511(2)(a)(ii) (emphases added).
103. *See* 12 U.S.C. § 3414(a)(5)(D)(iii) (2000); 15 U.S.C. § 1681u(d)(3) (2000); *id.* § 1681v(c)(3); 18 U.S.C. § 2709(c)(3); 50 U.S.C. § 436(b)(3).
104. *See* 18 U.S.C. § 2518(8)(d).
105. *Id.* § 3123(d)(1).
106. *See* Exec. Order No. 13,292 §§ 1.5(b), 3.1, 68 Fed. Reg. 15,315, 15,317, 15,319 (Mar. 28, 2003).

those containing both date certain provisions and review mechanisms—are the least burdensome. Rules consisting of one or the other are more so.

At the far end of the durational axis is the most onerous policy choice: a perpetual secrecy requirement that does not contemplate its eventual elimination. Thus FISA's electronic surveillance authority generally obliges third parties to assist investigators in secrecy,[107] but nothing in the statute fixes the duration of that obligation or gives decisionmakers the discretion to cancel it. Perpetual secrecy requirements generally are more burdensome than their temporary counterparts, in that there is no possibility of reprieve. But there is also a sense in which perpetual secrecy rules are more modest than some temporary alternatives. Given a broad statutory command of indefinite secrecy and a corresponding absence of any Executive discretion to tailor nondisclosure obligations to particular situations, there is no possibility of government caprice. A third party's speech interests are implicated forever, but she at least can be assured that she has not been singled out for disfavorable treatment on the basis of her political or other beliefs.

The following table depicts the five axes, with the range of policy options (or harms) arrayed from left to right in increasing order of severity:

	–	Policy choices	+
(1) Harms to be prevented	Disrupt an ongoing investigation	Compromise sources & methods; diplomatic friction	Prevent information sought from being created at all
(2) Type of information protected	Investigative facts		Underlying facts
(3) Mechanism for imposing secrecy	Special showing requirement	Presumptive secrecy requirement	Automatic secrecy requirement
(4) Breadth of secrecy rule	Indeterminate standard		Categorical prohibition
(5) Duration of secrecy	Temporary secrecy: Date certain? Review mechanism?		Perpetual secrecy

II. THE CURRENT SECRECY REGIME

Until quite recently in American history, the decision whether to investigate in secrecy turned solely on the perceived force of the Executive Branch's operational interests. The interests of other stakeholders simply didn't enter the equation. This Part begins by telling the story of how, in the 1960s and 1970s, the secrecy calculus was expanded to account for the countervailing interests of targets, third parties, the public, and Congress. It then surveys the policy choices reflected in the major tools used in national security investigations within the United States, explaining which interests various features of these laws seek to vindicate. In particular, this Part ex-

107. *See* 50 U.S.C. § 1805(c)(2)(B).

amines the investigative authorities and secrecy requirements in each of FISA's four subchapters, which govern (1) electronic surveillance, (2) physical searches, (3) pen registers and trap and trace devices, and (4) orders to produce business records and other tangible things. It also discusses the various National Security Letter statutes, which enable investigators to obtain documentary information in intelligence operations.

A. A Brief History of FISA

The history of FISA is a well tilled field, and I do not intend to re-plow it here.[108] Asserting an inherent power to defend the nation against hostile powers, every president from Franklin Delano Roosevelt to Jimmy Carter had authorized warrantless wiretaps in national security operations.[109] With the decision to surveil entrusted to the sole discretion of Executive Branch officials and with no judicial oversight, it was almost inevitable that abuses would occur. And so they did. Scores of dissident groups, civil rights activists, members of Congress, and others found themselves on the receiving end of warrantless monitoring.[110] The most egregious examples are well known but worth revisiting. In 1963, Attorney General Robert F. Kennedy authorized the FBI to surveil civil rights leader Dr. Martin Luther King, Jr., who was suspected of having ties to members of the American Communist Party.[111] The surveillance yielded embarrassing audiotapes of Dr. King in *flagrante delicto*, and FBI officials threatened to release them unless he committed suicide.[112] Sexual blackmail was a recurring theme. When inspecting the late J. Edgar Hoover's files in the 1970s, Deputy Attorney General Laurence Silberman discovered that LBJ aide Bill Moyers during the 1964 presidential campaign had ordered Hoover to snoop for evidence that Barry Goldwater staffers were homosexuals.[113] Surveillance of incumbents' political opponents often took place in election years. In 1972, operatives of the euphoniously acronymed Committee to Reelect the President—CREEP—broke into the Democratic National Committee's headquarters in the Watergate building to photograph documents and install wiretaps.

---

108. Readers who seek additional details of the statute's roots and development will find no shortage of excellent accounts to consult, including William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 10-74 (2000); Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 795-813 (1989); and Swire, *supra* note 13, at 1310-25. Matthew R. Hall, *Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence*, 41 WAKE FOREST L. REV. 61, 81-87 (2006), thoroughly compares FISA's investigative authorities to their criminal law counterparts.

109. *See* S. REP. NO. 95-604, at 7-8 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3908-09; Swire, *supra* note 13, at 1313-14.

110. *See* David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 HARV. C.R.-C.L. L. REV. 1, 19 (2003); Swire, *supra* note 13, at 1318-19.

111. *See* Robert A. Dawson, *Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1386 n.37 (1993); David J. Garrow, *The FBI and Martin Luther King*, THE ATLANTIC, July/Aug. 2002, at 80.

112. *See* Solove, *supra* note 67, at 1274.

113. *See* Laurence H. Silberman, *Hoover's Institution*, WALL ST. J., July 20, 2005, at A12.

Around the time these abuses were occurring and being uncovered, the Supreme Court was laying the jurisprudential foundation for judicial oversight of the Executive Branch's use of electronic surveillance techniques. In its 1928 ruling in *Olmstead v. United States*,[114] a five to four Court held that the Fourth Amendment permitted investigators to eavesdrop via wiretap on a criminal suspect's telephonic conversations without first obtaining judicial approval.[115] In a celebrated dissent, Justice Brandeis protested that the majority's account undervalued "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[116] It took nearly forty years, but Justice Brandeis finally got his way. In *Katz v. United States*,[117] the Supreme Court repudiated *Olmstead* and held that, because a wiretap is a "search" within the meaning of the Fourth Amendment, police must obtain a warrant before listening in on the conversations a suspect conducted in a telephone booth.[118] *Katz* conspicuously declined to extend its warrant requirement to surveillance undertaken in the name of national security.[119] But the pieces were in place for a fundamental reshaping of the law governing intelligence gathering.

The coup de grace came in 1972. That was the year the Supreme Court handed down its ruling in *United States v. United States District Court*,[120] popularly known as the *Keith* decision, after the federal district judge who initially heard the case. In *Keith*, the government brought criminal charges against several persons accused of domestic terrorism, including the bombing of a CIA office in Ann Arbor, Michigan.[121] During pretrial proceedings, it was revealed that the government had undertaken a number of warrantless national security wiretaps.[122] The Supreme Court concluded that, in "domestic surveillance" investigations, the Fourth Amendment required the government to obtain a "prior warrant" before conducting wiretaps; the Court remained silent on the standards for surveillance of *foreign* threats.[123] After *Keith*, it was inevitable that Congress would impose statutory restrictions on the President's heretofore unilateral power to authorize national

114. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

115. *See id.* at 464 ("There was no searching. There was no seizure. . . . There was no entry of the houses or offices of the defendants.").

116. *Id.* at 478 (Brandeis, J., dissenting).

117. 389 U.S. 347 (1967).

118. *Id.* at 358.

119. *See id.* at 358 n.23; *see also id.* at 359 (Douglas, J., concurring) (denying that the Executive Branch constitutionally may "resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters"); *id.* at 364 (White, J., concurring) (arguing that "[w]e should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable").

120. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972).

121. *Id.* at 299.

122. *See id.* at 299-300.

123. *Id.* at 321; *see id.* at 308 (declining to pass "judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country").

security surveillance. FISA is the result, enacted in 1978 with broad bipartisan support and the enthusiastic backing of the Carter Administration.[124]

B. Electronic Surveillance

As originally enacted, FISA regulated only electronic surveillance, not the myriad other techniques by which the Executive gathers intelligence. The statute's electronic surveillance authority[125] is the national security counterpart of the Federal Wiretap Act.[126] It generally governs the interception of various types of voice and other communications that originate in, take place wholly within, or terminate in the United States.[127] With a few exceptions, the government may not engage in these sorts of surveillance without submitting an application to and receiving approval from the Foreign Intelligence Surveillance Court, commonly known as the "FISC" or "FISA court."[128] The FISA court may not approve an application unless the government demonstrates, among other things, probable cause to believe that the target of the surveillance is a "foreign power" or an "agent of a foreign power."[129] "Probable cause" sounds familiar enough, but the FISA standard is somewhat different from the familiar criminal procedure rule.[130] In many, but not all, FISA investigations, the Executive Branch has to sat-

124. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1862 (2000)). It often is asserted that FISA represents Congress's acceptance of the *Keith* Court's invitation to "consider protective standards" for national security investigations, "which differ from those already prescribed for specified crimes in Title III." *Keith*, 407 U.S. at 322. *See* Banks & Bowman, *supra* note 108, at 76; Swire, *supra* note 13, at 1321; Alison A. Bradley, Comment, *Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT*, 77 TUL. L. REV. 465, 473 (2002). Not exactly. FISA governs surveillance of foreign threats to the national security, while *Keith*—and its invitation—concerned surveillance of domestic threats. *See* Cinquegrana, *supra* note 108, at 803 ("No congressional action has ever been taken regarding the use of electronic surveillance in the domestic security area.").

125. 50 U.S.C. §§ 1801-1811 (2000).

126. 18 U.S.C. §§ 2510-2522 (2000).

127. *See* 50 U.S.C. § 1801(f); *see also* Banks & Bowman, *supra* note 108, at 76-77 (discussing the categories of electronic surveillance regulated by FISA); Cinquegrana, *supra* note 108, at 811-12 (same). FISA does not regulate interception of communications that both originate and terminate outside the United States. The National Security Agency is believed to be responsible for conducting that sort of surveillance under different legal authorities. *See, e.g.*, Aid, *supra* note 30, at 61; Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247 (2005).

128. *See* 50 U.S.C. § 1803(a). FISA also establishes the seldom used Foreign Intelligence Surveillance Court of Review, to which the government may appeal if the FISA court denies a surveillance application. *Id.* § 1803(b).

129. *See id.* § 1805(a)(3)(A).

130. *See* S. REP. NO. 95-701, at 11 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3979 ("A judicial warrant is normally granted upon probable cause that a crime has been or is about to be committed. By contrast, in some cases the bill allows issuance of a court order upon probable cause that a person's activities 'may involve' a criminal violation."). *See generally* Beck v. Ohio, 379 U.S. 89, 91 (1964) (holding that, in ordinary criminal investigations, officers may conduct a search only if "the facts and circumstances within their knowledge and of which they had reasonably trustworthy information were sufficient to warrant a prudent man in believing that the petitioner had committed or was committing an offense").

isfy something very much like the probable cause standard that prevails in garden variety criminal cases.[131]

As far as secrecy is concerned, FISA's electronic surveillance authority imposes nondisclosure requirements on third parties whose assistance the government enlists. It directs "a specified communication or other common carrier, landlord, custodian, or other specified person . . . [to] furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy."[132] This secrecy rule aims at averting the standard set of harms—the danger that publication of the surveillance will disrupt an ongoing investigation or compromise intelligence sources and methods. But because electronic surveillance is a species of prospective intelligence gathering in which information is collected in real time, the nondisclosure requirement protects against an additional danger: the risk that a target's awareness of the surveillance will cause him to modify his behavior in a way that prevents the information sought from being created at all.

The wiretap nondisclosure requirement shares something else with virtually every other investigative secrecy rule: it only bars the publication of investigative facts. Third parties are directed to protect "its" secrecy, the pronoun referring back to "the electronic surveillance."[133] The secrecy requirement does not appear to prevent third parties from revealing any underlying information in their possession—viz., the contents of the intercepted communications. FISA's wiretap subchapter does not require the government to make any special showing to the FISA court to justify the imposition of a nondisclosure obligation. Simply by virtue of demonstrating its entitlement to conduct surveillance, the government thereby establishes its right to secrecy. The electronic surveillance secrecy rule is fairly narrow in scope. Rather than categorically barring third parties from revealing the fact that an investigation is underway, it features an indeterminate standard generally requiring third parties to maintain the secrecy of the monitoring.[134]

---

131. Specifically, if the target is not a United States person—i.e., if he is neither an American citizen nor an alien who is a lawful permanent resident, *see* 50 U.S.C. § 1801(i)—the government may surveil him simply by showing probable cause to believe that he works for a foreign power (for example, as an embassy employee). *See id.* § 1801(b)(1). If the target is a United States person suspected of "clandestine intelligence gathering activities," the Executive must show probable cause to believe that his activities "involve or *may* involve" a violation of federal criminal law. *Id.* § 1801(b)(2)(A) (emphasis added). If the target is a United States person suspected of "sabotage" or "international terrorism," the government will need to establish probable cause to believe that his conduct "involve[s]" a criminal violation. *Id.* § 1801(b)(2)(C), (c), (d). FISA's detractors often pan the statute's probable cause standard as a low hurdle the Executive easily can clear. *See, e.g.*, Solove, *supra* note 67, at 1290; Gregory E. Birkenstock, Note, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 844 (1992). In some cases they are right. But the reality is much more complicated.

132. 50 U.S.C. § 1805(c)(2)(B).

133. *Id.*

134. Ironically, FISA's wiretap secrecy rule is narrower than the categorical prohibition contained in Title III. *See* 18 U.S.C. § 2511(2)(a)(ii)(B) (2000) ("*No* . . . specified person shall disclose the existence of *any* interception or surveillance or the device used to accomplish the interception or surveillance . . . except as may otherwise be required by legal process . . . ." (emphases added)); *see also id.* § 2518(4)

FISA thus may permit disclosures insofar as they do not compromise the surveillance's overall confidentiality—e.g., to one's family members or colleagues. The electronic surveillance secrecy rule appears to be permanent: nothing in the statute sets a date on which secrecy will terminate, nor does it create a mechanism for canceling secrecy when no longer justified.

C. Physical Searches

Because FISA's initial incarnation only established a framework for electronic surveillance, physical searches generally continued to proceed under the Executive's inherent national security powers. It was not until 1994 that Congress added a physical search authority because of doubts about the constitutionality of such warrantless searches.[135] FISA's physical search subchapter is roughly equivalent to Federal Rule of Criminal Procedure 41, which grants courts the power to issue search warrants in ordinary criminal investigations. As with electronic surveillance, investigators may apply to the FISA court for an order approving a physical search. Such an order generally is required before the government may conduct a search, and the court may not approve a search unless probable cause exists to believe that the target of the search is a foreign power or agent.[136]

This physical search secrecy requirement differs in a number of key respects from its criminal law counterpart. The federal statute governing "sneak and peek" search warrants allows investigators to delay providing notice to the target where a court determines that immediate notification would have one of several specified adverse results.[137] The statute thus prevents the target from learning about the search by enabling the government to temporarily withhold information it otherwise would be required to give. But it does not impose secrecy obligations on third parties who help effectuate the search (e.g., a landlady who unlocks the door to the target's apartment). FISA's physical search secrecy rule is considerably broader. Not only does it allow the Executive to withhold information from a target, it

(providing that a court order authorizing electronic surveillance shall direct a third party to assist the government in a manner that will "accomplish the interception unobtrusively"). Title III thus appears to contain two distinct secrecy requirements. The first represents a categorical bar on revealing the surveillance; the second, like its FISA counterpart, takes the form of an indeterminate "maintain secrecy" obligation.

135. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443-53 (1994) (codified as amended at 50 U.S.C. §§ 1821-1829). For the history of the physical search subchapter, see Banks & Bowman, *supra* note 108, at 77; Swire, *supra* note 13, at 1328-29; and Bradley, *supra* note 124, at 481. *See generally* Daniel J. Malooly, Note, *Physical Searches Under FISA: A Constitutional Analysis*, 35 AM. CRIM. L. REV. 411 (1998).

136. *See* 50 U.S.C. § 1824(a)(3).

137. *See* 18 U.S.C. § 3103a(b)(1); *see also id.* § 2705 (defining "adverse result"). *See generally* Dalia v. United States, 441 U.S. 238, 247-48 (1979) (deeming "frivolous" the argument that the Fourth Amendment invariably requires law enforcement to provide contemporaneous notification that a search warrant has been executed, and reasoning "that 'officers need not announce their purpose before conducting an otherwise [duly] authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence'" (quoting Katz v. United States, 389 U.S. 347, 355 n.16 (1967))).

also enables the government to bind third parties to secrecy: "[U]pon the request of the applicant, a specified landlord, custodian, or other specified person [shall] furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy . . . ."[138]

This nondisclosure requirement is designed to prevent the usual set of harms, such as compromising intelligence sources and methods, disrupting an ongoing investigation, and diplomatic embarrassment. Because physical searches are a form of retrospective surveillance, in which the government collects information that was created at some point in the past, they do not present the special risks that target awareness will prevent the information from being created in the first place. Like FISA's electronic surveillance authority, the physical search secrecy rule directs third parties to help facilitate "the physical search in such a manner as will protect its secrecy"; the pronoun "its" refers back to "the physical search."[139] It thus is limited to disclosure of the fact that the government conducted a search. The rule does not further bar third parties from revealing any underlying information they may happen to possess independently.

FISA's physical search secrecy rule is broader than its criminal law counterpart in another respect. FISA imposes nondisclosure obligations on third parties automatically; the statute nowhere requires the government to make a special showing of need to bind third parties to secrecy. By contrast, in the criminal law world, the default rule is that notice is provided to the target at the same time a search is conducted. It is only when law enforcement officers are able to convince a court that there is "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" that they will be able to ensure secrecy.[140] But FISA's physical search nondisclosure requirement is somewhat narrower than other national security secrecy rules in at least one way. Like the electronic surveillance rule, it takes the form of an indeterminate standard requiring third parties to maintain the overall confidentiality of the search. The statute thus seems to permit any disclosures that do not compromise the search's overall secrecy.

The duration of this nondisclosure requirement is temporary. FISA's physical search subchapter does not establish a definite lifespan for secrecy, but it does contain a mechanism by which the Attorney General, in his discretion, may eliminate some secrecy rules.[141] This is another sense in which FISA is more restrictive than the sneak and peek law. That latter statute

138. 50 U.S.C. § 1824(c)(2)(B).
139. *Id.*
140. 18 U.S.C. § 3103a(b)(1).
141. *See* 50 U.S.C. § 1825(b) ("Where a physical search . . . involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search . . . and shall identify any property of such person seized, altered, or reproduced during such search.").

provides that secrecy shall expire on a date certain, albeit one subject to extensions. In particular, secrecy expires after thirty days ("or on a later date certain" if the court concludes lengthier secrecy is justified).[142]

D. Pen Registers/Trap and Trace Devices

After the 1994 addition of FISA's physical search authority, other amendments followed in due course. In 1998, Congress authorized the FISA court to approve applications to use pen registers and trap and trace devices in national security investigations.[143] This new subchapter is the counterpart of the federal pen/trap statute,[144] which is used in ordinary criminal cases. Pen/traps collect addressing and routing information about communications—for example, which numbers are dialed by a particular telephone or the email addresses from which a particular email account receives messages. They may not be used to collect the content of communications.[145]

While the Fourth Amendment does not require investigators to obtain prior court approval before using pen/traps,[146] Congress has adopted procedures above that constitutional floor. FISA authorizes the Executive Branch to apply to the FISA court for an order approving the installation of a pen/trap. Not surprisingly, given the constitutional baseline, the standard for obtaining a pen/trap order is less exacting than the requirements for electronic surveillance or physical searches. The Executive Branch need not prove probable cause; it only has to demonstrate (or perhaps merely assert) relevance to an ongoing investigation. Specifically, the Executive Branch must submit "a certification . . . that the information likely to be obtained is . . . relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[147]

The pen/trap subchapter is unusual in that it contains two discrete secrecy rules. The first is an indeterminate standard obliging third parties to maintain the confidentiality of the investigation. "[T]he provider of a wire or electronic communication service, landlord, custodian, or other person

142. 18 U.S.C. § 3103a(b)(3).

143. *See* Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2405-10 (1998) (codified as amended at 50 U.S.C. §§ 1841-1846 (2000 & Supp. III 2003)).

144. 18 U.S.C. §§ 3121-3127 (2000 & Supp. III 2003).

145. *See id.* § 3127(3)-(4) (clarifying that pen/trap information "shall not include the contents of any communication").

146. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979); *supra* notes 60-61 and accompanying text.

147. 50 U.S.C. § 1842(c)(2) (Supp. III 2003). It's hard to say with precision exactly what the standard is. The statute does not clearly answer whether the FISA court is limited to determining if the government has submitted the requisite certification, or whether it may go further and assess if there is a factual basis for the certification. Some clues may be gleaned from the analogous authority in the criminal law setting. The pertinent statute restricts courts to ensuring that the government filed the necessary certification. *See* 18 U.S.C. § 3123(a)(1) (Supp. III 2003) (directing a court to approve the use of a pen/trap "if the court finds that the attorney for the Government has certified . . . that the information likely to be obtained . . . is relevant to an ongoing criminal investigation"). It would be perverse if FISA's pen/trap tool were read to embody a more rigorous standard than its criminal law counterpart, since FISA is meant to give investigators more, not less, flexibility than they enjoy in the law enforcement world.

shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy."[148] The general terms of this first secrecy rule are complemented by the second, which provides more sweepingly that "such provider, landlord, custodian, or other person—(I) shall not disclose the existence . . . of the pen register or trap and trace device to any person unless or until ordered by the court."[149]

As a form of prospective surveillance, pen/traps present the special risk that disclosure of the monitoring will prevent the creation of the information the government seeks. If targets know that government agents are recording the telephone numbers they dial or the addresses to which they send emails, they will not engage in those activities. Like their counterparts elsewhere in FISA, the pen/trap secrecy rules seek to preserve the confidentiality of investigative facts (information that would reveal that an investigation is underway), not any underlying information in the third party's hands. Thus the first secrecy rule directs third parties to preserve "its secrecy," referring back to "the installation and operation of the pen register or trap and trace device."[150] The second rule is even more explicitly restricted to investigative facts, barring third parties from "disclos[ing] the existence of the investigation or of the pen register or trap and trace device."[151] Again like the other FISA authorities, the government in seeking a pen/trap need not make a special showing to impose a nondisclosure requirement on a third party. Simply by providing the FISA court with the necessary certifications of relevance, the government thereby is able to bind third parties to secrecy.

FISA's pen/trap secrecy rule differs from the statute's other nondisclosure requirements in a significant respect. Both the electronic surveillance and physical search subchapters are limited to indeterminate standards, which arguably permit third parties to make any disclosures that do not compromise the investigation's overall confidentiality. By contrast, the pen/trap authority's second secrecy rule categorically bars third parties from

148. 50 U.S.C. § 1842(d)(2)(B)(i).

149. *Id.* § 1842(d)(2)(B)(ii). Why did Congress give the pen/trap subchapter two secrecy rules? The legislative history for the 1998 FISA amendments is sparse. *See* Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37, 51 (2005) ("There is almost no legislative history for these two new provisions. They emerged in the Senate version of the Intelligence Authorization Act for Fiscal Year 1999, but they are not otherwise mentioned in the conference report or floor debate."). But some clues may be drawn from the circumstances in which the statute was enacted. The first secrecy rule is virtually identical to its electronic surveillance and physical search counterparts, with only minor linguistic changes to account for the differences in technologies. It is likely that the 1998 drafters simply modeled this secrecy rule on its predecessors. The second rule, in turn, appears to be modeled on the secrecy requirement contained in the business records authority (also enacted as part of the 1998 FISA amendments). That secrecy requirement, in turn, looks to have been based on the nondisclosure obligations in the preexisting NSL statutes. Congress thus was adopting a belt and suspenders approach. It recycled FISA's indeterminate standard secrecy rule, then added a categorical secrecy rule of the type it had before it in the NSL statutes and the business records authority.

150. 50 U.S.C. § 1842(d)(2)(B)(i).

151. *Id.* § 1842(d)(2)(B)(ii)(I).

disclosing investigative facts "to *any* person."[152] It contains no exceptions. On its face, then, the pen/trap subchapter purports to bar a third party from making even innocuous disclosures that preserve the overall confidentiality of the monitoring. The pen/trap secrecy rule is temporary. It does not fix a date on which secrecy naturally expires, but it does include a mechanism by which a nondisclosure obligation can be lifted. Secrecy remains in force "unless or until ordered by the court,"[153] though the statute nowhere spells out any factors to guide the exercise of that discretion.

E. Business Records

FISA's business records authority[154]—originally enacted in 1998,[155] rewritten in 2001 by Section 215 of the USA PATRIOT Act,[156] and revised further in 2006[157]—is the national security counterpart of Federal Rules of Criminal Procedure 6 and 17, which authorize grand jury subpoenas in ordinary criminal investigations. In particular, "Section 215" (as it is known in the trade) permits the government to submit to the FISA court an application for an order "requiring the production of any tangible things (including books, records, papers, documents, and other items)."[158] Investigators may obtain a Section 215 order if they submit "a statement of facts showing" (not merely "specifying" or "certifying") "that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[159]

Where Section 215 departs most dramatically from its grand jury counterpart is its secrecy requirement. It provides: "No person shall disclose to any other person . . . that the Federal Bureau of Investigation has sought or

152. *Id.* (emphasis added).
153. *Id.*
154. 50 U.S.C. §§ 1861-1862.
155. Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411-12 (1998) (codified as amended at 50 U.S.C. §§ 1861-1862).
156. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 287-88 (prior to 2006 amendments).
157. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192, 196-200 (2006) (to be codified at 50 U.S.C. § 1861(d)); USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 3, 120 Stat. 278, 278-79 (to be codified at 50 U.S.C. § 1861(f)(2)(A)(i)).
158. 50 U.S.C. § 1861(a)(1) (Supp. III 2003), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(a)(1).
159. *Id.* § 1861(b)(2)(A), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(b). Before the 2006 amendments, FISA's business records authority only required the Executive to "specify" that the materials were "sought for" a national security investigation. *Id.* § 1861(b)(2), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(b). Commentators disputed whether this "specification" requirement was akin to an actual relevance standard, *see, e.g.*, Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1194 (2004); Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 694-95 (2004); Woods, *supra* note 149, at 53, or whether the FISA court was limited to the ministerial task of determining whether the government had filed the requisite specification, *see, e.g.*, James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1482 & n.108 (2004). The 2006 addition of an actual relevance standard seems to settle the debate.

obtained tangible things under this section."[160] Several exceptions exist; third parties may reveal the order's existence to those whose assistance is needed for compliance, to legal counsel, and to others as permitted by the FBI Director.[161] Contrary to the claims of some commentators,[162] this secrecy rule is significantly broader than that of Federal Rule of Criminal Procedure 6(e) (which only binds grand jurors and government employees). But contrary to the views of others,[163] the secrecy requirement was neither created nor expanded by the USA PATRIOT Act. The 2001 secrecy rule—since amended—was substantively identical to the one contained in the original 1998 business records subchapter.[164]

Like all nondisclosure rules, Section 215 seeks to prevent ongoing investigations from being disrupted, the revelation of intelligence sources and methods, and diplomatic embarrassment. Section 215 authorizes a form of retrospective surveillance, so there is no risk of the additional harm that the target's knowledge would prevent creation of the intelligence sought at all. Also like other nondisclosure rules, the business records subchapter only bars publication of investigative facts; namely, the fact "that the Federal Bureau of Investigation has sought or obtained tangible things."[165] Recipients of a 215 order remain free to publicize any underlying information lawfully in their possession.[166]

---

160. 50 U.S.C. § 1861(d)(1) (Supp. III 2003), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(e).

161. *See id*. § 1861(d)(1)(A)-(C), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(e).

162. *See, e.g.*, James B. Perrine, *The USA PATRIOT Act: Big Brother or Business as Usual?*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 163, 188 (2005) (comparing Section 215 to grand jury proceedings, which are "cloaked in secrecy").

163. *See, e.g.*, Fuchs, *supra* note 16, at 134 (characterizing "the so-called gag order provisions of Section 215" as a "new law[]"); Michael O'Donnell, *Reading for Terrorism: Section 215 of the USA PATRIOT Act and the Constitutional Right to Information Privacy*, 31 J. LEGIS. 45, 46 (2004) (describing Section 215's "gag order" as a "significant change[]"); Swire, *supra* note 13, at 1308 (lamenting that Section 215 "ma[de] it a criminal act to report" that the government sought to obtain business records).

164. *Compare* 50 U.S.C. § 1862(d)(2) (2000) ("No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility, physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of Investigation has sought or obtained records pursuant to an order under this section."), *with* 50 U.S.C. § 1861(d) (Supp. III 2003) ("No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section."). Section 215 actually liberalized the old secrecy rule somewhat. Before, third parties were permitted to disclose the government's request only to those "officers, agents, or employees" necessary to facilitate compliance. 50 U.S.C. § 1862(d)(2) (2000), *amended by* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 287-88. After the PATRIOT Act, they could reveal the order to any "persons" needed for compliance, including, for example, independent contractors, such as an outside administrator of a company's computer network.

165. 50 U.S.C. § 1861(d).

166. In this respect, Section 215 actually is narrower than its criminal analogue. Rule 6(e) sweepingly prohibits certain individuals, including court employees, grand jurors, and lawyers for the government (but not witnesses called before the grand jury, *see* Butterworth v. Smith, 494 U.S. 624, 635 (1990)), from disclosing "a matter occurring before the grand jury." FED. R. CRIM. P. 6(e)(2)(B). This prevents them from revealing not just investigative facts—e.g., the fact that a grand jury has been empanelled, the names of the witnesses who have been called to testify—but also any underlying information (such as

No special showing of need is required of the government before the FISA court may order secrecy; a nondisclosure obligation is imposed automatically. Section 215 takes the form of a categorical prohibition on revealing the protected information: Subject to several exceptions, "[*n*]*o person* shall disclose to *any other person*."[167] Like FISA's physical search and pen/trap subchapters, the business records authority features a temporary secrecy rule. It lacks a date certain requirement but does have a review mechanism, and its procedures are significantly more detailed than those of its statutory neighbors. No sooner than one year after receiving a business records order, a third party may file with the FISA court a petition to set aside or modify the secrecy requirement.[168] The court may grant the petition only if it finds "there is no reason to believe" that disclosure "may" result in one of several specified harms, including disrupting an investigation or damaging diplomatic relations.[169] Certain high ranking Executive Branch officials, such as the Attorney General or FBI Director, then are entitled to certify that disclosure "may" produce a requisite harm, in which case secrecy may be modified only if the court finds the certification "was made in bad faith."[170]

F. National Security Letter Statutes

Section 215 is not the only tool the Executive Branch may use to obtain documentary information in national security investigations. In addition, there is a quintet of subpoena like authorities crafted by Congress over the course of several decades, and revised in 2006,[171] collectively known as the "National Security Letter," or "NSL," statutes.[172] NSL statutes generally allow the government (typically the FBI) in terrorism and espionage investigations to request that certain third party custodians turn over various classes of documents, such as financial records and transactional records of electronic communications. Unlike FISA's more comprehensive business records authority, only a narrow class of entities and records are subject to collection by NSL. Also unlike FISA, no prior judicial approval is required before the Executive may request documents via NSL. An NSL thus is a variety of administrative subpoena.[173] This subpart describes the basic fea-

---

the content of a particular witness's testimony).

167. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(e), 120 Stat. 192, 197 (2006) (to be codified at 50 U.S.C. § 1861(d)(1)) (emphasis added).

168. USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 3, 120 Stat. 278, 278 (to be codified at 50 U.S.C. § 1861(f)(2)(A)(i)).

169. *Id.* § 3.

170. *Id.*

171. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, §§ 115-119; USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, §§ 4-5.

172. *See* 12 U.S.C. § 3414 (2000) (Right to Financial Privacy Act NSL); 15 U.S.C. § 1681u (2000) (Fair Credit Reporting Act NSL); 15 U.S.C. § 1681v (Supp. IV 2004) (Fair Credit Reporting Act NSL); 18 U.S.C. § 2709 (2000) (Electronic Communications Privacy Act NSL); 50 U.S.C. § 436 (2000) (government employee NSL).

173. *See* Swire, *supra* note 13, at 1332.

tures of the various NSL statutes separately, then considers their secrecy rules (which are substantively identical) together.

The first NSL statute—enacted in 1978 as part of the Right to Financial Privacy Act, or "RFPA"[174]—enables the FBI to obtain certain "financial records" from "financial institutions." The definition of "financial record" is pretty much what one would expect: "any record held by a financial institution pertaining to a customer's relationship with the financial institution."[175] The meaning of "financial institution" is somewhat less so. In addition to banks and credit unions, the term includes pawnbrokers, travel agencies, automobile dealers, the United States Postal Service, and casinos.[176] The RFPA embodies something like the simple relevance standard under which subpoenas typically are available: the FBI need only certify to the financial institution that "such records are sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities."[177]

The Fair Credit Reporting Act (FCRA) NSL, originally enacted in 1995,[178] enables the FBI to demand that consumer reporting agencies disclose "the names and addresses of all financial institutions . . . at which a consumer maintains or has maintained an account."[179] The FCRA NSL contains the same "sought for" standard; the FBI may obtain the information it seeks by certifying "that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities."[180]

The FCRA contains a second NSL authority, enacted in 2001 in a little noticed provision of the USA PATRIOT Act.[181] Using this tool, investigators can get a "consumer report of a consumer and all other information in a consumer's file."[182] This NSL differs from its sister FCRA provision, in-

174. *See* Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, § 1114, 92 Stat. 3641, 3707. Some confusion exists as to whether the RFPA was in fact the first NSL statute or whether that distinction belongs to the Electronic Communications Privacy Act (ECPA) NSL, enacted in 1986. *See, e.g.*, Dempsey & Flint, *supra* note 159, at 1483 n.117 ("The first National Security Letter authority was not enacted until 1986."); Shumate, *supra* note 15, at 6 (claiming that "the Electronic Communications Privacy Act ('ECPA') authorized the initial use of NSLs in 1986"). The original 1978 RFPA granted the FBI the authority to *request* documents from financial institutions, but the government could not *demand* them. It was not until 1986—some months after the enactment of ECPA, which authorized the FBI to demand certain transactional records pertaining to communications—that Congress revised the RFPA to include a comparable mandatory authority. *See* Woods, *supra* note 149, at 43-44. The RFPA was born first, but didn't sprout teeth until later.

175. 12 U.S.C. § 3401(2) (2000).

176. *See* 31 U.S.C. § 5312(a)(2)(A)–(D), (O), (Q), (T), (V), (X) (2000); *id.* § 5312(a)(2)(E) (Supp. III 2003). 12 U.S.C. § 3414(d) provides that the term "financial institution" has the same meaning as in 31 U.S.C. § 5312(a)(2) & (c)(1), instead of the ordinary RFPA definition that is found at 12 U.S.C. § 3401(1).

177. 12 U.S.C. § 3414(a)(5)(A) (Supp. IV 2004) (footnote omitted).

178. *See* Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, § 601(a), 109 Stat. 961, 975 (1995).

179. 15 U.S.C. § 1681u(a) (Supp. III 2003).

180. *Id.*

181. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 358(g)(1)(B), 115 Stat. 272, 327-28.

182. 15 U.S.C. § 1681v(a).

deed from all other NSLs, in three crucial respects. First, the availability standard is higher. Where other NSLs may be used upon a certification of *relevance*, the second FCRA authority requires a certification that the information sought "is *necessary* for the agency's conduct or such investigation."[183] Second, this is the only NSL whose availability is restricted to international terrorism operations;[184] other NSLs may be used in investigations both of international terrorism and of clandestine intelligence activities. Third, while most NSLs may be used only by the FBI, this one may be invoked more broadly by any "government agency authorized to conduct investigations of . . . international terrorism."[185]

The fourth NSL was enacted as part of the 1986 Electronic Communications Privacy Act, or "ECPA."[186] This tool enables the FBI to order telecommunications providers to turn over certain information about wire and electronic communications, such as routing and addressing information, but not the content of those communications.[187] The ECPA NSL imposes a relevance standard, this time directly instead of in the roundabout "sought for" way; the FBI must certify that the "records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[188] Two federal district courts recently invalidated an old version of the ECPA NSL; they both concluded that its nondisclosure requirement violates third parties' First Amendment speech rights,[189] and one further held that the statute authorizes "searches" that are "unreasonable" within the meaning of the Fourth Amendment.[190]

The final type of NSL, enacted in the same 1994 legislation that established FISA's physical search authority,[191] enables investigators to obtain certain information about government employees. This NSL permits investigators to obtain information from the same sorts of entities named in the RFPA and FCRA NSLs—e.g., a "financial agency, financial institution, or . . . consumer reporting agency."[192] And it also permits investigators to acquire similar types of information: "financial records . . . consumer reports . . . [and] records . . . pertaining to travel."[193] But there's a big catch. This tool is narrowly limited to the collection of data about government employees who hold security clearances. In particular, investigators may only ob-

183. *Id.* (emphasis added).
184. *See id.*
185. *Id.*
186. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867.
187. *See* 18 U.S.C. § 2709(a) (2000).
188. 18 U.S.C. § 2709(b)(1)-(2) (Supp. III 2003).
189. *See* Doe v. Gonzales, 386 F. Supp. 2d 66, 74 (D. Conn. 2005); Doe v. Ashcroft, 334 F. Supp. 2d 471, 506 (S.D.N.Y. 2004). The Second Circuit dismissed the former case as moot and vacated the latter. *See* Doe v. Gonzales, 449 F.3d 415, 421 (2d Cir. 2006).
190. *See Ashcroft*, 334 F. Supp. 2d at 506.
191. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443-53 (1994).
192. 50 U.S.C. § 436(a)(1) (2000).
193. *Id.*

tain the records if they pertain to a government official who, during a background check, consented to the government accessing his records.[194] And the standard is significantly higher. The information sought must be "*necessary*" to an authorized investigation,[195] and there must be "reasonable grounds to believe, based on credible information" that the person might be sending classified information to foreign powers or agents.[196]

The five NSLs' secrecy rules are substantively indistinguishable. The ECPA NSL is representative. It provides: "No wire or electronic communication service provider . . . shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."[197] Because NSLs generally are used to engage in retrospective, not prospective, surveillance, the statutes' secrecy rules are meant to prevent the standard menu of adverse consequences that could result from a target's awareness that he is under surveillance: revelation of intelligence sources and methods and interference with an ongoing investigation. But one of the authorities—the ECPA NSL—conceivably could be used to engage in prospective surveillance, too.[198] An ECPA NSL thus presents an additional risk when it is used to gather intelligence prospectively: the target's awareness of the surveillance will prevent the information investigators seek from being created at all.

Like other secrecy requirements, NSL nondisclosure obligations only prohibit the disclosure of investigative facts. They do not prevent a third party from publicizing any underlying information she possesses on her own, apart from her participation in the government's investigation. Take the first FCRA NSL—it bars disclosure "that the [FBI] has sought or obtained" information and "inclu[sion] in any consumer report any information that would indicate" the FBI's intelligence gathering activities.[199] Until recently, the NSL statutes imposed secrecy automatically. But in 2006, Congress amended them to include special showing requirements. Now, secrecy is not available unless the Executive certifies that disclosure "may" result in one of several specified harms, such as "danger to the national security" or "interference with a criminal, counterterrorism, or counterintelli-

194. *See id.* § 436(a)(2)(A). The targets' privacy interests thus are minimized, as they previously consented to the intelligence gathering. *Cf.* United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) (holding that a former CIA official could, consistent with the First Amendment, be made to submit a book manuscript to the agency for review, in part because he had signed a secrecy agreement when he was hired).

195. 50 U.S.C. § 436(a)(1) (emphasis added).

196. *Id.* § 436(a)(2)(B)(i).

197. 18 U.S.C. § 2709(c) (2000); *see also* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 116(e), 120 Stat. 192, 216 (2006) (to be codified at 12 U.S.C. § 3414(a)(5)(D)(i)); *id.* § 116(b), (c), & (f).

198. *See* 18 U.S.C. § 2709(a) (making available for government acquisition "electronic communication transactional records"—namely, routing, addressing, and other information indicating that communications are taking place and who is communicating).

199. 15 U.S.C.A. § 1681u(d)(1) (Supp. 2006). The second clause appears redundant. Appending to a consumer report a notation that the FBI sought or obtained information would seem to constitute a "disclos[ure] to any person" within the meaning of the first clause. *See id.*

gence investigation."[200] All five NSLs feature categorical secrecy requirements. But the broad sweep of those rules is mitigated by several exceptions, which permit third parties to make compliance related disclosures and disclosures to legal counsel.[201]

The NSL statutes also are uniform as to their duration. Third parties' obligation to refrain from disclosing investigative facts does not expire on a date certain, but a review mechanism exists by which an otherwise indefinite secrecy requirement may be abolished when no longer appropriate. (This is new, too; before 2006, NSLs featured perpetual secrecy rules.) In particular, an NSL recipient may petition a local federal district court to modify or set aside a nondisclosure obligation.[202] The legal standard varies with the passage of time. If the petition is filed within a year, the court may not modify a secrecy rule unless it concludes "there is no reason to believe" that disclosure "may" result in one of several specified harms (the same harms the Executive must invoke to justify secrecy in the first place).[203] The government then has the option of submitting another certification—this time from a high ranking official—that disclosure "may" produce a requisite harm; if it does, the court may modify the secrecy requirement only if it finds the certification "was made in bad faith."[204] (These procedures are identical to those under FISA's business records authority.)[205] After a year, the presumption shifts slightly against secrecy. If the third party files her petition more than a year after receiving the NSL, the government has ninety days to either terminate the secrecy requirement or recertify that disclosure would result in a specified harm.[206] In the event of recertification, the court may not modify the secrecy rule unless "there is no reason to believe" that disclosure "may" produce one of the requisite harms.[207] If the recertification was made by one of several high ranking executive officials, secrecy may only be modified if the court finds it "was made in bad faith."[208]

The following table illustrates the operation of the existing secrecy regime:

200. USA PATRIOT Improvement and Reauthorization Act of 2005, § 116(a).
201. *See id.* Prior to the 2006 amendments, two NSL statutes included these exceptions (the first FCRA and government records NSLs), but three did not (the ECPA, RFPA, and second FCRA NSLs).
202. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, § 115.
203. *Id.*
204. *Id.*
205. *See* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-778, § 3, 120 Stat. 278, 279 (to be codified at 50 U.S.C. § 1861(f)(2)(C)).
206. USA PATRIOT Improvement and Reauthorizing Act of 2005, § 115.
207. *See id.*
208. *See id.*

	Electronic surveillance	Physical searches	Pen/traps	Business records	NSLs
Harms to be prevented	Standard harms; prevent creation of data sought	Standard harms	Standard harms; prevent creation of data sought	Standard harms	Standard harms; prevent creation of data sought (ECPA NSL)
Protected information	Investigative facts	Investigative facts	Investigative facts	Investigative facts	Investigative facts
Mechanism for imposing secrecy	Automatic	Automatic	Automatic	Automatic	Special showing requirement
Breadth of secrecy rule	Indeterminate standard	Indeterminate standard	Categorical, no exceptions	Categorical, some exceptions	Categorical, some exceptions
Duration of secrecy	Perpetual	Review mechanism	Review mechanism	Review mechanism	Review mechanism

III. A CRITIQUE OF THE EXISTING SECRECY REGIME

The fit between the operation of the current secrecy system as described in Part II and the array of interests and possible policy choices recounted in Part I is far from precise. In some cases, the existing regime assigns too much weight to the Executive Branch's operational interests; in others it overprotects the interests of other stakeholders. This Part identifies four such imbalances in the current system and recommends reforms to ensure that particular nondisclosure requirements more satisfactorily balance the competing values they implicate.

Specifically, the present system of investigative secrecy is flawed in that it fails to prevent third parties from disclosing any underlying information in which investigators are interested; the rules are limited to restrictions on revealing that the government is conducting an investigation.[209] Yet sometimes the disclosure of "underlying facts" can be as harmful as the release of "investigative facts." In this respect, the existing regime undervalues the Executive's operational interests while overprotecting the speech interests of third parties. Another way the current system undervalues the

209. *See* sources cited *supra* note 197.

government's operational interests is by pairing relatively weak secrecy requirements with investigative techniques by which intelligence is gathered in real time (such as electronic surveillance), and which therefore need particularly robust nondisclosure rules.[210] At the same time, investigative methods that have a somewhat lesser need for secrecy (such as NSLs) feature relatively strong nondisclosure rules.[211] The Executive Branch is far from the only victim. Current law under-protects the privacy and speech interests of targets and third parties, and overvalues the government's operational interests, insofar as it permits secrecy to be imposed automatically. Under many laws, the Executive Branch need not make any special showings before secrecy is imposed; simply by demonstrating its entitlement to surveil, it thereby demonstrates its entitlement to surveil in secrecy. Finally, existing secrecy rules generally feature nondisclosure obligations that are perpetual either in fact or by presumption, ignoring that the Executive's interests generally diminish over time while those of other stakeholders only grow stronger.

A. Extending Secrecy Rules to Underlying Facts

Third parties whose assistance the government seeks in national security investigations will possess a wide array of information acquired from a wide array of sources.[212] Any system of secrecy must choose which types it wishes to keep confidential: *investigative facts* (information about the nature and status of the government's investigation, learned by interacting with government agents), *underlying facts* (the substantive information in which the government is interested, acquired by the third party on his own), or some combination thereof. The current secrecy regime has cast its lot with the former. Almost uniformly, its components prohibit only the revelation of investigative facts a third party obtains by participating in the government's investigation.[213]

In general, this targeted prohibition is appropriate. Third parties don't seem to have much of an interest in publicizing underlying facts, as indi-

210. *See, e.g.*, USA PATRIOT Improvement and Reauthorization Act of 2005, § 116(a).

211. *See, e.g.*, *id.* § 116(e).

212. *See supra* note 92 and accompanying text.

213. *See, e.g.*, 50 U.S.C. § 1805(c)(2)(B) (FISA electronic surveillance rule requiring third parties to protect "its" secrecy, i.e., the secrecy of the electronic surveillance); *id.* § 1824(c)(2)(B) (FISA physical search rule requiring third parties to protect "its" secrecy, i.e., the secrecy of the physical search); *id.* § 1842(d)(2)(B)(ii) (FISA pen/trap rule barring third parties from "disclos[ing] the existence of the . . . pen register or trap and trace device to any person"); USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(e) (FISA business records rule barring any "person" from disclosing "that the Federal Bureau of Investigation has sought or obtained tangible things . . . under this section"); *id.* § 116(a) (to be codified at 18 U.S.C. § 2709(c)(1)) (ECPA NSL barring any "wire or electronic communications service provider" from disclosing "that the Federal Bureau of Investigation has sought or obtained access to information or records under this section"). Federal Rule of Criminal Procedure 6(e)(2)(B) appears to be the only component of the secrecy system whose strictures reach underlying facts, too; it sweepingly bars covered entities from disclosing any "matter occurring before the grand jury." FED. R. CRIM. P. 6(e)(2)(B).

cated by their apparent failure to exercise their right to do so under current law. Confining nondisclosure requirements to investigative facts also reflects the congressional judgments that such information (which is to say, data about the government's intelligence sources and methods) is particularly sensitive and worthy of protection, and that more sweeping restrictions pose even greater risks to speech interests.[214] But special cases may arise where a third party does want to publicize underlying information, and disclosure of those data may prove equally damaging. More fundamentally still, it is not always possible to distinguish meaningfully between an investigative fact and an underlying one. Current law does not adequately address these realities, and the secrecy regime needs a mechanism to protect underlying facts from disclosure in extraordinary cases.

The leading case is the Supreme Court's Delphic decision in *Butterworth v. Smith*.[215] There, the Court unanimously struck down as a violation of the First Amendment's free speech guarantee a Florida law that purported to bar grand jury witnesses from publicizing the content of their testimony after the grand jury's term ended.[216] According to the Court, the state's asserted interests in secrecy—encouraging witnesses to come forward and testify truthfully, preventing suspects from fleeing or intimidating witnesses, etc.[217]—did not "warrant a permanent ban on the disclosure by a witness of his own testimony once a grand jury has been discharged."[218] The Court was far from clear in its rationale. Was Florida's law infirm because it permanently barred witnesses from revealing the specified information, regardless of its content? Or was it unconstitutional because, regardless of its duration, the law restricted the disclosure of underlying facts? Proponents of each view will find in *Butterworth* plenty of fodder for their positions. At one point, the Court stresses that Florida's "ban extends not merely to the life of the grand jury but into the indefinite future."[219] It also emphasizes that the government's interests in secrecy diminish "[w]hen an investigation ends."[220] But elsewhere the *Butterworth* Court suggests that the distinction between investigative and underlying facts is what is driving its conclusion: "Here, by contrast, we deal only with respondent's right to divulge information of which he was in possession before he testified before the grand jury, and not information which he may have obtained as a result of his participation in the proceedings of the grand jury."[221]

---

214. *See supra* notes 76-77.

215. 494 U.S. 624 (1990).

216. *Id.* at 636. The law also may have prohibited them from revealing the fact that they testified—an investigative fact—but that aspect of the rule wasn't before the Court. *See id*. at 629 n.2.

217. *See id*. at 630.

218. *Id*. at 632; *see also id*. at 626 (holding "that insofar as the Florida law prohibits a grand jury witness from disclosing his own testimony after the term of the grand jury has ended, it violates the First Amendment to the United States Constitution").

219. *Id*. at 635.

220. *Id*. at 632; *see also id.* at 632 n.3.

221. *Id*. at 632 (citing Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984) (upholding against a First Amendment challenge a court order barring civil litigants from publicizing information they obtained

Justice Scalia's concurrence contains no such ambiguity. For him, Florida's secrecy rule offended the First Amendment not because of its indefinite duration but because it barred witnesses from publicizing information they obtained other than through the grand jury proceedings.[222] "I think there is considerable doubt whether a witness can be prohibited, even while the grand jury is sitting, from making public what he knew before he entered the grand jury room."[223] But the state has a freer hand to restrict disclosures of information that third parties obtain through the state's investigative processes. This is "knowledge [a third party] acquires not 'on his own' but only by virtue of being made a witness," and the state may have "quite good reasons" for keeping it "confidential even after the term of the grand jury has expired."[224] For Justice Scalia, restrictions on underlying facts are probably never constitutional, but lengthy prohibitions on publicizing investigative facts may well be.

Lower tribunals have shown no less confusion than the *Butterworth* Court in determining what it is about secrecy rules that turns the constitutional litmus paper. Courts wishing to invalidate an investigative fact nondisclosure requirement generally have tended to emphasize the durational aspect of *Butterworth*. Courts inclined to uphold such restrictions have focused on the Scalia distinction.

A good example of the former is *Doe v. Gonzales*,[225] in which the District of Connecticut struck down an old version of the ECPA NSL's secrecy requirement. 18 U.S.C. § 2709 only prevents third parties from revealing investigative facts, but at the time, it did so perpetually. For the court, the key feature was the NSL's permanent duration, not the information to which it applies.[226] "The provision of § 2709(c) that prohibits [a third party] from *ever* disclosing its identity" offends the First Amendment, the court reasoned, because the Executive Branch's interests in nondisclosure "cannot continue indefinitely. At some point, even if in the distant future," the government's need for secrecy diminishes.[227] The court went out of its way to disparage the alternative reading of *Butterworth*: "the Supreme Court did not reach the issue of whether disclosure of the mere fact that a grand jury was ongoing" (an investigative fact) "could be subject to a gag order."[228]

---

only through the discovery process), and Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829 (1978) (invalidating as a violation of the First Amendment a Virginia law barring public disclosure of information communicated to a commission investigating allegations of judicial misconduct, including information that would be speakers acquired on their own)); *see also id.* at 635 ("The effect is dramatic: before he is called to testify in front of the grand jury, respondent is possessed of information on matters of admitted public concern about which he was free to speak at will. After giving his testimony, respondent believes he is no longer free to communicate this information . . . .").

222. *See id.* at 636 (Scalia, J., concurring).

223. *Id*.

224. *Id*.

225. 386 F. Supp. 2d 66 (D. Conn. 2005), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006).

226. *See id.* at 79-80.

227. *Id.* at 79.

228. *Id.* at 80. The sister case of *Doe v. Gonzales*, *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzalez, 449 F.3d 415 (2d Cir. 2006), likewise emphasized the dur-

By contrast, in *Kamasinski v. Judicial Review Council*,[229] the Second Circuit upheld a Connecticut law that banned a complainant before a commission investigating alleged misconduct by state judges from disclosing the fact that he filed a complaint, as well as any information he acquired by interacting with the commission—i.e., investigative facts.[230] Distinguishing "between information that the individual obtains independently, and the *fact* that testimony has been given,"[231] and citing Justice Scalia's *Butterworth* concurrence, the Second Circuit reasoned that the former category of information is subject to greater regulation than the latter.[232] The *Kamasinski* court did observe that the secrecy rule was in force only until the state commission completed its preliminary investigation,[233] but that fact does not appear to have influenced the outcome of the case.

The existing secrecy regime, and Justice Scalia's *Butterworth* distinction that serves as its jurisprudential foundation, represents a classic case of over- and under-inclusivity. The rules simultaneously prevent third parties from publicizing investigative facts even when doing so would not harm the government's operational interests, while making no effort to restrict disclosure of even the most sensitive and damaging underlying facts.

The overinclusivity problem is easily conceived. Information about intelligence sources and methods certainly is among the most delicate data in the government's possession, and there are good reasons to keep it secret. But circumstances could arise when disclosure of those investigative facts would work only minimal, or even no, harms to the Executive Branch's operational interests. Suppose the government voluntarily reveals to the public that it is conducting a manhunt for a group of six suspected al Qaeda members in upstate New York. In addition to disclosing the existence of the investigation, the government also reveals some of the techniques used to track the cell's members: voluntary interviews with local witnesses, physical searches of an apartment complex where the cell members are believed

---

ational aspects of *Butterworth* in striking down the ECPA NSL's secrecy rule. *See Ashcroft*, 334 F. Supp. 2d at 512 (faulting ECPA's "blanket permanent prohibition on future disclosures"); *id.* at 514 (stressing that "[t]he statute *permanently* prohibits not only the recipient but its officers, employees or agents, from disclosing the NSL's existence"); *id.* at 519 (rejecting the relevance of Justice Scalia's *Butterworth* distinction because "the NSL statutes . . . impose a *permanent* bar on disclosure in every case, making no distinction among competing relative public policy values over time, and containing no provision for lifting that bar when the circumstances that justify it may no longer warrant categorical secrecy"); *see also In re* Grand Jury Proceedings, 417 F.3d 18, 27 (1st Cir. 2005) (reasoning that, in *Butterworth*, "the grand jury proceeding had long been completed and it was the permanency of the ban that most troubled the Supreme Court").

229. 44 F.3d 106 (2d Cir. 1994).

230. *See id.* at 111.

231. *Id.* at 110.

232. *See id.* at 110-11; *see also* Hoffmann-Pugh v. Keenan, 338 F.3d 1136, 1139-43 (10th Cir. 2003) (upholding a Colorado grand jury secrecy rule that prohibited a witness—a housekeeper of John and Patsy Ramsey, whose daughter, JonBenet, had been murdered—from revealing information she obtained only by testifying before a grand jury, and interpreting *Butterworth* as distinguishing "between information the witness possessed prior to becoming a witness and information the witness gained through her actual participation in the grand jury process").

233. 44 F.3d at 108 (indicating that "[t]he confidentiality provisions were in effect . . . only during the period before the [commission] made a probable cause determination").

to have resided, monitoring of email addresses believed to be registered to some of the suspects, etc. What interest could the Executive Branch possibly have then in continuing to enforce nondisclosure obligations against the targets' landlady or email provider? The sensitive facts about the investigation's existence and nature have already been disclosed—at the government's hand, no less—and no additional harms would be worked by permitting those same data to enter the public domain from other sources.[234] Another aspect of the overinclusivity problem is that investigative facts that at one time were sensitive may become less so with the passage of time, and the need to keep them confidential may evaporate.[235]

The under-inclusivity problem has received less attention, but it is every bit as real. First, the current system permits disclosures of underlying facts from which an informed observer could piece together investigative facts. In any number of cases, the divulging of underlying facts will yield valuable clues about the nature and direction of the government's investigation. Observers, especially sophisticated foreign powers and agents trained in the art of counterespionage, will be able to discern from these individual mosaic tiles the very investigative facts the secrecy regime aims to protect.

Imagine, counterfactually, that the FBI covertly installed a bug in the apartment of Mohammed Atta, the leader of the 9/11 hijackers. Imagine further that investigators did so by obtaining a FISA court order directing Atta's landlady to admit them to the apartment. The landlady's suspicions are aroused, and after the agents leave and Atta returns, she begins listening at the door of the apartment. Now suppose the landlady, while not giving any indication that the FBI ordered her to open the apartment (investigative facts), tells the local newspaper what she has overheard in the apartment (underlying facts). Atta quickly would conclude that his conversations are being monitored, probably so by the government. As a result, he likely would accelerate his plot, go into hiding, destroy evidence, and so forth. In other words, the disclosure of underlying facts can enable targets to infer the surrounding investigative facts. And that act of inference can cause the same harms to the Executive Branch's operational interests that would result from a direct publication of the investigative facts themselves.[236]

---

234. *See, e.g.*, Cooper v. Dillon, 403 F.3d 1208, 1217-18 (11th Cir. 2005) (reasoning that the "argument that important interests are served by maintaining the confidentiality of internal [police] investigations is undercut by the fact that the information in question was divulged by the state itself"); Doe v. Gonzales, 386 F. Supp. 2d 66, 81 (D. Conn. 2005) (indicating that "in this case, the existence of an investigation is already public: the defendants agreed to the docketing of the Redacted Complaint, which reveals that an investigation (of unknown topic) exists and that a NSL was issued in Connecticut to an organization with library records"), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006); *In re* Am. Historical Ass'n, 49 F. Supp. 2d 274, 293 (S.D.N.Y. 1999) (approving release of grand jury transcripts relating to Alger Hiss in part because "the witnesses' involvement with the investigation is public knowledge, as is the substance of portions of some of their grand jury testimony").

235. *See infra* Part III.D.

236. The magnitude of the resulting harms does not depend in any way on the substance of the disclosed underlying information. Even where the underlying facts are innocuous, e.g., a conversation between Atta and his guests about their favorite soccer team, the inferred investigative facts still will cause targets to take steps to evade detection. *See* United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir.

Second, the current secrecy regime allows publication of underlying facts whose release would harm Executive operational interests to the same extent as investigative facts. Even where the disclosure of underlying facts does not compromise the investigative facts whose confidentiality the government wishes to preserve, there may be circumstances where publicizing underlying facts is at least as damaging to the Executive Branch's operational interests. This is especially likely to be the case when some investigative facts already are circulating in the public domain. Suppose, again counterfactually, that the FBI is conducting a nationwide manhunt for Atta. The resident of the apartment next to Atta's sees the FBI most wanted bulletin on the evening news, immediately recognizes Atta, and calls the FBI to report her suspicions. A team of FBI agents obtains a FISA court order and executes a physical search of the apartment at a time when Atta is known to be away, seeking evidence that would confirm his identity. Any disclosure by the neighbor that the FBI conducted the search, an investigative fact, would produce the standard menu of adverse consequences: flight, destruction of evidence, etc. But the same harms would result from disclosure of underlying facts. If the neighbor reported to a local journalist that a wanted terrorist is living in her building, that would equally disrupt the investigation by alerting Atta that his cover is blown.

The present secrecy system is plagued by serious over and underinclusivity problems, but a still more fundamental difficulty exists. It is not always possible to differentiate between an investigative fact and an underlying fact. This is so because a third party's understanding of the data she acquired on her own inevitably will be influenced by her awareness that the government is mounting an investigation. When a third party reinterprets information she possesses on her own in light of that new data supplied by the government, is that properly regarded as an instance of an investigative fact, disclosure of which may be restricted, or an underlying fact, as to which no secrecy requirements presently apply? Consider the following hypothetical.

A hotelier in Norfolk, Virginia, plays host to a group of six men bearing Yemeni passports. Norfolk is the home port of the USS *Cole*, which was attacked by suicide bombers in the port of Aden, Yemen, on October 12, 2001. The hotelier knows that the visitors pay for their rooms in cash. She also knows that they make several telephone calls to an international number, again paid for in cash. One morning the apparent leader of the group asks the hotelier for directions to the Norfolk Naval Station, where the *Cole* at the time is docked for maintenance and resupply. The hotelier recalls the *Cole*'s history and the events in Yemen, she is aware that her hotel sees few international guests, and she knows that most customers pay their bills with

1989) ("[M]uch of the government's security interest in the conversation lies not so much in the contents of the conversations, as in the time, place, and nature of the government's ability to intercept the conversations at all.").

credit cards. But she does not suspect that the six Yemenis may be up to no good.

Now suppose the FBI approaches the hotelier and serves an order to hand over documents and other tangible things pertaining to the Yemenis: copies of the information the hotel recorded from their passports, records of their telephone calls, footage of them from the hotel's security cameras, hair samples from their used bed linens, and so on. The FBI thereby has alerted the hotelier to the fact, either expressly or by enabling her to draw the inference, that a national security investigation is underway.[237] Something clicks in her mind. She now comes to suspect that her Yemeni visitors have been sent to Norfolk to finish the job begun years ago in Aden and destroy the USS *Cole*. And it is her awareness of the government's investigative activities that causes her to form this conclusion. Because—and only because—of the FBI's actions, the hotelier has reinterpreted the underlying facts in her possession. If the government had not conveyed to her certain investigative facts, she would have regarded the underlying facts she held as signifying something altogether different, or perhaps as not signifying anything at all.

How would the existing secrecy regime treat the information the hotelier wants to convey to the public? They are not purely investigative facts because she was in possession of the various bits and pieces of information—the guests' Yemeni nationality, their interest in the whereabouts of the *Cole*, etc.—before she was approached by the government. But neither are they purely underlying facts because the hotelier would not have attached significance to them but for the fact that the FBI revealed to her certain information about its activities. The facts thus simultaneously were acquired apart from the hotelier's participation in the government's investigation and are information of the government's own creation.

The current system of investigative secrecy is inadequate because it does not provide clear rules for situations in which the information a third party wishes to reveal cannot easily be classified as investigative or underlying information, nor does it account for the severe harms that can result

237. Some instruments served on third parties expressly state that the information sought is wanted in connection with a national security investigation. According to an internal FBI memorandum, the second paragraph of each NSL must contain "the statutorily required certification language." Memorandum from General Counsel to All Field Offices 5 (Nov. 28, 2001), *available at* http://www.epic.org/privacy/terrorism/usapatriot/foia/fbi_nsl_memo.pdf. There are slight differences among the five NSL statutes' "certification language," but they all represent variations on this basic theme: the request is pursuant to "an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b)(1) (Supp. III 2003). Other authorities seek to prevent third parties from learning that the investigation has to do with national security, and thus reinterpreting otherwise innocuous underlying facts in light of that information. For example, FISA's business records authority provides that any court order directing a third party to turn over information to investigators "shall not disclose that such order is issued for purposes of [a national security] investigation." USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(d), 120 Stat. 192, 197 (2006) (to be codified at 50 U.S.C. § 1861(c)(2)(E)); *see also* 15 U.S.C. § 1681u(c) (Supp. III 2003) (authorizing court order to compel compliance with Fair Credit Reporting Act NSL, and specifying that "[t]he terms of an order issued under this subsection shall not disclose that the order is issued for purposes of a counterintelligence investigation").

when third parties disclose underlying information. To be sure, third parties may not seek to publicize underlying facts except in extraordinary cases—e.g., a landlady who wants to sound the hue and cry about what she believes to be an imminent terrorist attack. But to accommodate those rare situations, the secrecy rules should be adjusted to allow the imposition of nondisclosure requirements as to underlying information third parties obtained other than by participating in the government's investigation. This recommendation rests on the durational interpretation of *Butterworth*, under which indefinite nondisclosure requirements—regardless of whether they apply to investigative or underlying facts—are never permissible, but certain restrictions on divulging underling facts may be appropriate.

Any argument for imposing restrictions on the disclosure of underlying facts must come to grips with two realities: there is very little precedent for doing so (indeed, there is a great deal of precedent against such restrictions),[238] and measures of this sort implicate third party speech interests of the greatest magnitude. One struggles to conceive of a heavier burden on speech interests than an outright ban on third parties divulging underlying facts acquired on their own. Before the FBI asks our hypothetical landlady to help facilitate a search of Mohammed Atta's apartment, she remains entirely free to alert others that a wanted terror suspect is a tenant in her building. But the moment the FBI executes the search warrant, the landlady loses that right. Still, at least one federal appellate court recently signaled that underlying facts restrictions may be permissible in national security investigations. In *In re Grand Jury Proceedings*,[239] the First Circuit eliminated a restriction imposed by a lower court that barred a grand jury witness from revealing the substance of his testimony before the grand jury. But the appellate court was quick to emphasize that such bans do not invariably offend the First Amendment: "We do not say that a witness could never be precluded from discussing independent recollections; situations involving national security are too obvious a concern to encourage general pronouncements."[240] And Federal Rule of Criminal Procedure 6(e) is something of a precedent for secrecy as to underlying facts, albeit a rather weak one. That Rule bars the entities to which it applies from "disclos[ing] a matter occurring before the grand jury,"[241] which encompasses not only the fact that a given witness testified but also the substance of that testimony. The key

238. *See, e.g.*, Butterworth v. Smith, 494 U.S. 624 (1990); Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829 (1978); *In re* Grand Jury Proceedings, 417 F.3d 18, 28 (1st Cir. 2005) (modifying a court order that barred a grand jury witness from publicizing both the fact and the substance of his testimony; henceforth the order would not restrict disclosure of the witness's "independent recollections" apart from the grand jury process); Doe v. State of Fla. Judicial Qualifications Comm'n, 748 F. Supp. 1520, 1529 (S.D. Fla. 1990) (striking down a Florida law prohibiting a complainant from disclosing that he filed a complaint with a commission investigating alleged judicial misconduct, and characterizing the fact of filing as an underlying fact because "this information is known to the Plaintiff outside of any participation in a judicial proceeding").

239. 417 F.3d at 28.

240. *Id.*

241. FED. R. CRIM. P. 6(e)(2)(B).

words in the last sentence are "the entities to which it applies." For Rule 6(e)'s strictures only reach a small class of government agents or employees—"a grand juror," "an interpreter," "a court reporter," etc.[242]—who never would possess the protected information but for their governmental status and their participation in the grand jury process. It therefore would be a mistake to place too much reliance on Rule 6(e) as a basis for barring private citizens from revealing underlying facts.

These are difficult obstacles. But in light of the possibility that disclosures of underlying facts could prove every bit as damaging to the Executive's operational interests as the release of investigative facts, a statutory mechanism should exist to regulate the former. What would those rules look like? At least five safeguards would need to be put in place to guarantee that the Executive Branch's operational interests in fact justify proposed restrictions on disclosing underlying facts, and to ensure that the resulting strain on third party speech interests is no more severe and endures no longer than necessary.

First, underlying fact restrictions should only be available if the government obtains *ex ante* approval from a court. (More on the standard below.) The Executive Branch should not have the authority to impose the requirements unilaterally. Such a power would too closely resemble that of the unchecked government licensor condemned by Blackstone and centuries of American jurisprudence. And it would present too great a potential for abuse, whether because the Executive might actively target dissidents for secrecy or because bureaucratic laziness and a preoccupation with efficiency might prompt the government to adopt a default rule that underlying facts must never be disclosed. Instead, a neutral and detached magistrate should be interposed between Executive and third party to test and verify the government's representations that publication of underlying facts would harm the national security.

FISA's four investigative authorities easily could be adapted to accommodate this principle. The statute already contemplates pre-surveillance judicial review, and it would only take a sentence or two of new language to retrofit those mechanisms to enable the FISA court, in assessing whether to approve surveillance at all, to weigh whether a proposed underlying facts restriction is warranted. The NSL statutes would require a bit more work. Because NSLs are a species of administrative subpoena, issued without any *ex ante* court involvement, a judicial review process would have to be grafted onto the existing statutes. The Executive Branch thus would continue to be able to issue NSLs and bar third parties from revealing that the FBI sought information from them (an investigative fact) without prior court approval, but if the government wanted to go further and limit disclosures of underlying facts, it would need advance permission from a court, perhaps the FISA court. This bifurcated process would be somewhat cum-

242. FED. R. CRIM. P. 6(e)(2)(B)(i)-(iii).

bersome, but there is precedent for it. Third parties who receive NSLs don't always comply with them immediately, in which case the government may file with a federal district court a motion to compel.[243] In the process envisioned here, by contrast, the government's submission to the reviewing court would occur before, not after, it issued its demand for information.

Second, not only must there be judicial review before an underlying facts secrecy rule is imposed, a mechanism must exist by which a third party may challenge any such restriction in court on an *ex post* basis. During the initial ex parte proceedings at which the Executive Branch makes its case for secrecy, the supervising court will only be exposed to the government's perspective. *Ex post* proceedings will enable the third party to offer evidence as to the magnitude of the restriction's burden, and thus allow the court more precisely to assess whether the government's claimed needs justify interfering with her speech interests. FISA's business records subchapter and the NSLs already have such a review mechanism, but those of the physical search and pen/trap subchapters are skeletal at best, and the electronic surveillance subchapter lacks any mechanism at all. Part III.D argues that, as a general matter, meaningful review procedures should be added to each of these statutory authorities; they are even more essential as to restrictions on disclosing underlying facts.

Third, underlying facts secrecy should be permitted only if the supervising court concludes that its imposition satisfies strict scrutiny.[244] The Executive Branch thus would be required to demonstrate that its operational interest in protecting its particular intelligence sources and methods or in preventing disruption to a specific ongoing investigation—not just its undifferentiated interest in national security—amounts to "a compelling Government interest."[245] Courts generally agree that maintaining the integrity of national security operations can count as a compelling interest.[246] But the

243. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 115(3), 120 Stat. 192, 212-13 (2006) (to be codified at 18 U.S.C. § 3511(c)).

244. The standard by which courts assess investigative facts secrecy rules is far from clear. Sometimes, that the government created the restricted information is said to justify subjecting the challenged rule to intermediate, rather than strict, scrutiny. *See, e.g.*, Seattle Times Co. v. Rhinehart, 467 U.S. 20, 32 (1984) (in determining "whether a litigant's freedom comprehends the right to disseminate information that he has obtained pursuant to a court order[,] . . . it is necessary to consider whether . . . '[secrecy] . . . [furthers] an important or substantial governmental interest unrelated to the suppression of expression' and whether 'the limitation of First Amendment freedoms [is] no greater than is necessary'" (quoting Procunier v. Martinez, 416 U.S. 396, 413 (1974))). In other cases, the fact that the government created the information informs the strict scrutiny analysis, leading courts to apply a more forgiving version of that test. *See, e.g.*, Kamasinski v. Judicial Review Council, 44 F.3d 106, 109, 111 (2d Cir. 1994) (indicating that, because the secrecy rule was content based, "strict scrutiny is the correct standard," and upholding the rule on the basis of the conclusory statement that "Connecticut's interests in preserving the integrity of its judiciary" were sufficiently great). Still other courts apply the strict scrutiny test at undiluted strength. *See, e.g.*, Doe v. Gonzales, 386 F. Supp. 2d 66, 82 (D. Conn. 2005), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006); Doe v. Ashcroft, 334 F. Supp. 2d 471, 525-26 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

245. United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 813 (2000).

246. *See* Dep't of Navy v. Egan, 484 U.S. 518, 527 (1988) (citing the Executive's "'compelling interest' in withholding national security information from unauthorized persons in the course of executive business"); Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam) (indicating that "[t]he

Executive also would need to establish that restricting disclosure of underlying facts is a "narrowly tailored" way of accomplishing those objectives—i.e., that there is no "less restrictive alternative" that "would serve the Government's purpose."[247] This is where the action is likely to be. Such an extraordinary measure as restricting third party disclosures of facts independently in their possession should be reserved for cases of extraordinary need—e.g., where the publication of underlying facts would reveal to a hostile foreign power what sources and methods the government is using, where disclosure of underlying facts would cause targets to go into hiding or otherwise disrupt the investigation, or where the underlying facts and investigative facts are so intertwined that they are analytically indistinguishable.

Fourth, in addition to the review mechanism, any court approved bar on divulging underlying facts must expire after a time certain. This limitation reflects the magnitude of the burden on third party speech interests, as well as the reality that those burdens' severity only grows with the passage of time. Court approved extensions should be available, but only if the Executive Branch can demonstrate to the court's satisfaction that the continued operation of the secrecy rule, taking account of any changed social circumstances, still satisfies strict scrutiny. It is not to be expected that the Executive Branch would need such rules to persist for lengthy periods of time. The operational interests that are threatened by publication of underlying facts tend to be related to preventing disruption of an ongoing investigation—preventing the landlady from tipping off Mohammed Atta just long enough for the FBI to take him into custody. Less frequently will the Executive's interests in preserving intelligence sources and methods be implicated by the disclosure of underlying facts.

Fifth, it goes without saying that congressional oversight is even more essential when the Executive's conduct by stipulation implicates speech interests of the highest order. The public, which by design is kept in the dark about the surveillance details, is not in a position to check abuses and assess effectiveness, so Congress must stand in its shoes. Congress would do well to insist that the relevant oversight committees receive regular reports, as well as in person testimony from the responsible Executive officials, on the circumstances in which third parties have been barred from publicizing underlying facts. The twice yearly reports called for by FISA may not be sufficient; Congress might wish to receive monthly updates.

Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service"); *see also Gonzales*, 386 F. Supp. 2d at 78 (declining to "question that national security can be a compelling state interest, or that non-disclosure of a[n] NSL recipient's identity could, in some circumstances, serve that interest"). *But see* Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004) ("We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens.").

247. *Playboy*, 529 U.S. at 813.

B. Strengthening Secrecy Rules for Prospective Surveillance

In an ideal regime, the need for secrecy and the breadth of a given secrecy requirement would be correlative. As one increases, so would the other; as one diminishes, so would the other. This is another way of saying that an ideal system of secrecy would insist on a tight nexus between the first axis (measuring the harms to be averted by secrecy) and the fourth axis (measuring the precision of a secrecy rule) discussed in Part I.B above. As such, we would want to see strong nondisclosure requirements associated with the investigative methods as to which secrecy is paramount, while somewhat weaker restrictions would suffice for the techniques for which secrecy is comparatively less important.

In particular, we would want vigorous secrecy rules to be paired with the investigative tools that authorize prospective surveillance—i.e., methods by which the government is able to collect information in real time, at the moment it is created, such as wiretapping and other forms of electronic surveillance. This is so because the use of prospective surveillance methods presents unique dangers that do not arise when the government engages in retrospective surveillance—i.e., when it gathers intelligence that was created in the past and now is stored in some format. That additional danger threatened by prospective surveillance is that, if the target becomes aware that investigators are monitoring him, he will not create the information the government seeks to acquire in the first place. If Osama bin Laden learns that investigators are listening in on his satellite telephone conversations, he will stop having them.

By contrast, an ideal secrecy regime could feature somewhat weaker rules for retrospective surveillance methods, such as physical searches. Secrecy certainly is important, even necessary, to the effective use of these techniques; a target's awareness that agents are on his trail will cause him to take any number of actions that would frustrate the government's investigation. But the target cannot act to prevent the creation of information that, by stipulation, was generated at some point in the past. If Mohammed Atta learns the FBI has searched his apartment for incriminating computer files, he may go into hiding and take steps to destroy other evidence of his complicity. But he cannot prevent the government from acquiring the computer files. Secrecy is needed to prevent these adverse consequences from befalling an investigation, but the harms from a breach of confidentiality are not quite as drastic.

The current secrecy regime strays far from the ideal; in several ways it is 180 degrees out of phase. Take FISA's electronic surveillance subchapter. That authority, which permits a form of prospective surveillance, nevertheless features a relatively weak secrecy rule: "[A] specified communication or other common carrier, landlord, custodian, or other specified person . . . [shall] furnish the applicant forthwith all information, facilities, or technical

assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy . . . ."[248] It thus places third parties under a general duty to maintain "its secrecy," which is to say the secrecy of the surveillance. The statute reflects an indeterminate standard, as opposed to a categorical prohibition, and contains no specification of what sorts of conduct violate the "protect secrecy" imperative. One can imagine any number of disclosures that are consistent with the general duty to maintain the secrecy of the surveillance—namely, disclosures that do not result in investigative targets or the general public becoming aware of the surveillance. A third party who receives process for her employer of an FBI request for information might tell a friend about the government's demand. She might tell other company personnel who are in immediate possession of the data the government seeks. None of these revelations would threaten the secrecy of the surveillance; the target of the investigation and the public at large still would remain in the dark about the government's investigative activities. Each such disclosure therefore arguably is compatible with the overall "protect secrecy" duty.

By contrast, a number of retrospective intelligence gathering authorities feature sweeping secrecy rules, notwithstanding their comparatively lesser need for secrecy. Such requirements take the form of categorical prohibitions on any disclosures of protected data, no matter how low the likelihood that they will undermine the government's operational interests. (Some such rules have exceptions, permitting disclosures to legal counsel or to persons who are needed to facilitate compliance.) One example is FISA's business records subchapter, which provides that "[n]o person shall disclose to any other person . . . that the Federal Bureau of Investigation has sought or obtained tangible things under this section."[249] On their face, categorical prohibitions prohibit *all* disclosures of *all* protected information to *all* persons for *all* reasons (subject to any exceptions). There is no need to determine on a case by case basis whether a particular revelation has the effect of compromising the overall confidentiality of the surveillance, for categorical prohibitions do not leave to chance the identification of which disclosures are so harmful as to be prohibited. *All* disclosures that are not expressly excepted are prohibited.[250]

---

248. 50 U.S.C. § 1805(c)(2)(B) (Supp. III 2003).

249. *Id.* § 1861(d). The five NSL statutes feature virtually identical rules. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 116(e), 120 Stat. 192, 216 (2006) (to be codified at 12 U.S.C. § 3414(a)(5)(D)), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 4(d)(2), 120 Stat. 278, 281 (2006) (to be codified at 12 U.S.C. § 3414(a)(5)(D)(iv)); USA PATRIOT Improvement and Reauthorization Act of 2005, § 116(b), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, § 4(c)(1); USA PATRIOT Improvement and Reauthorizing Act of 2005, § 116(c), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, § 4(c)(2); USA PATRIOT Improvement and Reauthorizing Act of 2005, § 116(a), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, § 4(b); USA PATRIOT Improvement and Reauthorizing Act of 2005, § 116(f), *amended by* USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, § 4(e).

250. The existing secrecy regime isn't all wrong. FISA's pen/trap and physical search subchapters have secrecy rules that are carefully calibrated to the operational harms those investigative methods

In important respects, then, the current secrecy regime is backwards. Prospective surveillance techniques need strong secrecy rules taking the form of categorical prohibitions, but FISA's electronic surveillance subchapter features a relatively weak nondisclosure requirement.[251] Retrospective surveillance techniques would be content with somewhat weaker secrecy rules taking the form of indeterminate standards, but FISA's business records subchapter and the NSL statutes feature strong nondisclosure requirements. Congress therefore should recalibrate the existing secrecy rules to more precisely track the particular need for secrecy presented by each investigative technique. Specifically, the weaker rule in FISA's electronic surveillance subchapter should be replaced with a stronger categorical prohibition on all disclosures of protected information. Such a change could be accomplished with very little effort. Congressional drafters could simply copy the secrecy requirement reflected in FISA's pen/trap subchapter.

Congress also may wish to consider retrofitting the retrospective surveillance authorities with somewhat weaker secrecy requirements to reflect that disclosures of protected information under these tools are likely to be marginally less damaging. But there are good reasons to retain the existing categorical prohibition secrecy rules. Like any other indeterminate standards, generalized "protect secrecy" directives—whether paired with prospective or retrospective investigative techniques—are problematic to the extent they necessitate case by case determinations, on a retrospective basis, of the precise meaning of that standard. Given their ambiguity, one cannot know in advance precisely what sort of conduct the rules proscribe. Both the Executive Branch and other stakeholders have a shared interest in avoiding nondisclosure rules the scope and meaning of which are opaque. Such legal

---

threaten to produce. A pen/trap is a form of prospective surveillance, and the statute therefore properly contains a sweeping categorical prohibition secrecy rule. *See* 50 U.S.C.A. § 1842(d)(2)(B)(ii) (Supp. 2006). The physical search subchapter is the mirror image. It authorizes a form of retrospective surveillance and thus rightly imposes a weaker obligation under which a third party must maintain overall secrecy but apparently may make such disclosures as are consistent with that overarching duty. *See id.* § 1824(c)(2)(B). These features likely owe more to chronology than to deliberate policy choices. The physical search authority was added in 1994, when the most relevant model for Congress was the weak secrecy rule in the adjacent electronic surveillance subchapter; Congress probably just copied that predecessor over into the physical search authority. The pen/trap subchapter was added in 1998, in the same legislation through which Congress enacted the business records subchapter with its robust secrecy rule (which itself was cribbed from the NSL statutes).

251. The relative weakness of FISA's electronic surveillance secrecy requirement is doubly perverse. Not only does it proscribe fewer disclosures than the rules associated with some retrospective intelligence gathering techniques, it is even weaker than its criminal law counterpart. The Federal Wiretap Act, which authorizes electronic surveillance in ordinary criminal investigations, features a categorical secrecy requirement: "*No* . . . specified person shall disclose the existence of *any* interception or surveillance . . . ." 18 U.S.C. § 2511(2)(a)(ii) (Supp. III 2003) (emphasis added). This disparity is absurd given that the Executive Branch's interests in secrecy are even weightier in intelligence operations than in standard criminal investigations. In addition, countervailing interests on the other side of the ledger—target privacy interests—may be weaker in national security operations than in standard criminal cases. This is so because targets of international terrorism investigations tend to be nonimmigrant foreign nationals who boast few ties to this country, whereas garden variety crime appears to be evenly distributed across the population without regard to citizenship or immigrant status. *See supra* note 63 and accompanying text.

uncertainty harms both entities by inviting litigation over a secrecy rule's reach, which in turn requires them to devote scarce resources to court battles and thereby increases both entities' transactions costs. Resources that the government otherwise would deploy incapacitating national security threats, and that private entities otherwise would devote to producing socially useful outputs, instead will be directed to inefficient legal wrangling. Of course, secrecy requirements in the form of indeterminate standards do have the advantage of flexibility for situations that cannot be anticipated in advance.[252]

In addition to this common harm, indeterminate secrecy standards would damage respective interests that are unique to the government and third parties. A third party could face sanctions if she makes disclosures that she believes are not covered by a secrecy requirement, but that a reviewing court later determines fall within the law's reach. Such a third party has no agenda to defy nondisclosure requirements; she would just as soon comply with an obligation as flout it. But she could make an honest mistake about what the law requires of her and thereby expose herself to punishment. That scenario would trigger strong due process and free speech concerns[253] and raise the specter of selective Executive enforcement.[254] The opposite harm is possible, too. An indeterminate secrecy requirement can also chill a third party from making disclosures that she otherwise would make, and that the law does not in fact proscribe. A third party confronted with an ambiguous "protect secrecy" imperative may well conclude that the safest course is not just to refrain from disclosing the investigative facts that are the focus of the nondisclosure requirement but also any underlying facts that she independently possesses and that the secrecy rule does not reach. Indeterminacy thus encourages risk averse third parties to refrain from engaging in speech they otherwise would undertake.[255]

The government's reasons to disfavor ambiguous secrecy requirements are no less weighty. An indeterminate standard may cause a well meaning third party to make damaging disclosures she would not make if the law's

252. *See generally* Cass R. Sunstein, *Problems with Rules*, 83 CAL. L. REV. 953 (1995); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976).

253. *See* City of Chicago v. Morales, 527 U.S. 41, 56 (1999) (indicating that a criminal law is subject to invalidation on vagueness grounds if it "fail[s] to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits"); Giaccio v. Pennsylvania, 382 U.S. 399, 402-03 (1966) (emphasizing "that a law fails to meet the requirements of the Due Process Clause if it is so vague and standardless that it leaves the public uncertain as to the conduct it prohibits").

254. *See* Kolender v. Lawson, 461 U.S. 352, 359 (1983) (faulting vague statutes on the ground that they "necessarily 'entrust[] lawmaking to the moment to moment judgment of the policeman on his beat'" (quoting Smith v. Goguen, 415 U.S. 566, 575 (1974))).

255. *See* NAACP v. Button, 371 U.S. 415, 433 (1963) (indicating that free speech rights are "delicate and vulnerable, as well as supremely precious in our society[, and t]he threat of sanctions may deter their exercise almost as potently as the actual application of sanctions"); *see also* Shankman, *supra* note 15, at 252-54, 260 (arguing that the ECPA NSL's secrecy requirement is vague, and reasoning that such a rule "puts NSL recipients in the difficult predicament of watching their every word, indefinitely, for fear of violating the permanent nondisclosure provision").

content were clear. Even where a third party is operating in good faith and doing her level best to comply with a nondisclosure obligation, she could make a mistake that introduces sensitive information into the public domain. Indeterminate secrecy requirements may also complicate the government's efforts to hold accountable third parties who reveal sensitive data with less innocent motivations. Under the rule of lenity—a common law rule of statutory construction that also is animated by the Constitution's Due Process Clauses—there is a presumption against concluding that a person's conduct offends legal requirements that are truly ambiguous.[256] Given the ambiguity that surrounds many applications of indeterminate standard secrecy requirements, a court that adjudicates whether a given disclosure was unlawful may well decide to stay its hand. The Executive Branch thus would find its ability to prevent publication of delicate national security information compromised. (From the government's perspective, there may be some upside to indeterminacy; it dissuades third parties from testing the boundaries of permissible disclosures.) Third parties and the Executive Branch alike thus have complementary reasons to look with skepticism on any efforts to add weaker secrecy requirements to the statutes authorizing retrospective surveillance.

C. Requiring Special Showings for Secrecy Rules

Secret surveillance raises two analytically distinct questions. Should the Executive Branch be permitted to demand access to information in the hands of third parties? Should the Executive Branch be permitted to bind those third parties to secrecy? An affirmative answer to the first tells us nothing about the proper resolution of the second. One can conclude that the FBI should be able to ask a phone company for information about a suspected terrorist's calls without committing oneself to the view that the company should be barred from revealing that fact to its shareholders or the general public.

Underlying the distinction between these two questions is the reality that, from the standpoint of a third party, a nondisclosure requirement represents a greater affront to liberty interests than the underlying obligation to hand over information to investigators. Government demands for data only minimally impact the third party's privacy interests because it is the investigative target, not the custodian, who typically will be the subject of that information. A third party who produces the data thereby tends to reveal that she has interacted with the target, and she may have a privacy interest in avoiding that sort of confirmation.[257] But such interests are fairly weak,

256. *See* Dunn v. United States, 442 U.S. 100, 112 (1979) ("[N]o individual [should] be forced to speculate, at peril of indictment, whether his conduct is prohibited.").

257. A similar principle is at work in the cases holding that a person may invoke the Fifth Amendment privilege against self-incrimination in response to a subpoena duces tecum, where the production of the documents is akin to testimony that they exist, that they are in the person's possession, and that they are authentic. *See* Fisher v. United States, 425 U.S. 391, 410 (1976).

and weaker still when the third party is a large commercial entity that maintains identical business relationships with countless other consumers. Third party privacy interests are likely to be especially weak when the custodian is a common carrier, such as a local phone company. Virtually nothing can be inferred about a common carrier from the fact that it did business with the target, given that it has a legal obligation to do business with all comers.

The same cannot be said of the burdens third parties face from secrecy requirements. By restricting individuals' ability to engage in expression, nondisclosure obligations implicate speech interests of the highest order. We thus have a classic case of the government holding the power to direct or prohibit certain underlying conduct and also asserting the power to regulate speech about that conduct. The fact that the former restrictions represent relatively light burdens does not mean that the latter should be countenanced. A state may well have the power to proscribe the consumption of alcoholic beverages, but it does not follow that the state may take the additional step of banning commercial advertisements for alcoholic beverages. As the Supreme Court has emphasized, "we think it quite clear that banning speech may sometimes prove far more intrusive than banning conduct."[258] Likewise, a conclusion that national security investigators ought to be able to obtain information about targets from third parties by itself tells us nothing about whether the third parties should be bound to secrecy.

In designing a secrecy regime from the ground up, one therefore would want bifurcated proceedings that isolate the two basic questions—May the government surveil? May the government require secrecy?—from one another and permit them to be addressed in isolation. Secrecy should be bought retail, not wholesale; we should impose it by identifying the specific instances where it is necessary, not by designating an entire class of cases as subject to secrecy. To put it mildly, the current secrecy regime imperfectly realizes this ideal. Many of the authorities used to collect intelligence in national security investigations contain automatic secrecy requirements, in particular all four FISA subchapters. These rules conflate the question whether surveillance is justified with the question whether secrecy is justified. Automatic secrecy rules stand in sharp contrast to the special showing requirements that characterize both NSLs and many tools from the world of ordinary criminal investigations. For instance, under the sneak and peek statute, the default rule is that the investigators must provide contemporaneous notification of the search; they may undertake surreptitious searches only if they are able to convince the warrant issuing court that one of several adverse results may materialize.[259]

---

258. 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 511 (1996); *see also id.* (rejecting "the assumption that words are necessarily less vital to freedom than actions, or that logic somehow proves that the power to prohibit an activity is necessarily 'greater' than the power to suppress speech about it").

259. *See* 18 U.S.C. 3103a (Supp. III 2003), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 114, 120 Stat. 192, 210-11 (2006).

No reason is readily apparent why FISA authorizes automatic secrecy while the NSLs feature stricter special showing requirements. The relative strength of targets' privacy interests cannot account for the difference. NSLs represent less of an affront to privacy than certain FISA techniques since they allow investigators to collect information that targets voluntarily handed over to third parties. If anything, it is the NSLs that should feature relatively burdensome automatic secrecy requirements. Nor can the weight of the Executive's operational interests justify automatic secrecy rules for all four FISA authorities. Electronic surveillance and pen/traps both entail prospective intelligence gathering and thus present the special danger that a breach of secrecy will prevent the information sought from being created at all. But the physical search and business records tools authorize the same sort of retrospective surveillance as the NSL statutes. Nor can the special treatment the current regime affords to NSLs be justified by the fact that, unlike FISA, no judicial review is required before they are issued. FISA does mandate more *ex ante* process than the NSL statutes, but the litigation before the FISA court does not concern the specific issue of secrecy. The fact that the FISA court tests the Executive's representations as to, say, the target's status as an agent of a foreign power, does not ensure that the unique concerns implicated by secrecy will be addressed adequately—or at all.

Congress should include similar requirements in FISA. There are two models that would translate this ideal into practice: special showing rules, under which secrecy is only available when the government separately demonstrates the need for it, and presumptive rules, under which secrecy is presumptively imposed but may be suspended in circumstances where it is deemed inappropriate. These represent the near- and mid-points, respectively, on the third axis above.[260] The former are preferable for several reasons. First, special showing requirements are consistent with our first principles. In the American system of government, openness is the rule to which secrecy is the exception. The presumption should always be against secrecy, and the government should have to demonstrate its entitlement to operate out of the public eye. Second, not only is there a strong preference against secrecy, there is an equally forceful preference against restrictions on expression. The decision to bind third parties to secrecy, and thus restrict their ability to engage in speech, should be made deliberately and should never be the default position. Such limitations should be imposed only when the government is able to establish a compelling need for them.

Third, reticulated schemes of presumptions and shifting burdens have an uneasy relationship with the ex parte proceedings in which surveillance and secrecy are approved. The *McDonnell Douglas/Burdine*[261] burden shifting approach is appropriate in the employment discrimination context be-

260. *See supra* notes 95-99 and accompanying text.

261. *See* Tex. Dep't of Cmty. Affairs v. Burdine, 450 U.S. 248, 252-56 (1981); McDonnell Douglas Corp. v. Green, 411 U.S. 792, 802 (1973).

cause it pits two adverse parties against one another. After the plaintiff establishes a prima facie case of discrimination, the burden shifts to the defendant employer to offer a nondiscriminatory explanation for its conduct, and then the plaintiff is given the additional opportunity to show that the employer's explanation is pretext. But the FISA court proceedings in which surveillance initially is authorized are ex parte, and no adverse party would be present to cast doubt on the government's prima facie case for secrecy. In short, shifting burdens requires adversary litigation, a practice that is alien to surveillance proceedings.

Special showing requirements are preferable to presumptive and automatic rules for a fourth reason. Not only are they more protective of third party speech interests, they also offer enhanced protection for target privacy interests. Of necessity, targets are excluded from the proceedings in which surveillance is authorized, and given the lengthy terms of secrecy common to national security investigations, they may not learn the government was monitoring them for years (or ever). A special showing requirement is a way of putting the Executive Branch through its paces and thus represents a modicum of process to be afforded to the investigative targets about whom the government seeks information. Investigative targets may be thought of as third party beneficiaries of such arrangements.

Perhaps counterintuitively, special showing requirements may well advance the Executive Branch's interests, as well. This is so because they represent a form of narrow tailoring that increases the likelihood that any nondisclosure requirement will survive subsequent judicial review. One of the two district courts that invalidated the pre-2006 ECPA NSL on First Amendment grounds faulted its then automatic rule as "a blunt agent of secrecy applying in perpetuity to all persons affected in every case" and denied that such a rule could count "as narrowly-tailored."[262] The court further suggested that nondisclosure obligations with a tighter nexus to the harms to be prevented would be permissible.[263] Faced with the prospect of wholesale judicial invalidation of automatic secrecy rules, the government may prefer as an alternative special showing rules that more closely calibrate speech restrictions to the threatened harms.

Applying these principles to FISA, the Executive should not be permitted to bind third parties to secrecy unless it is able to demonstrate to the FISA court's satisfaction that public disclosure of the protected information would be harmful—i.e., that disclosure would compromise intelligence

262. Doe v. Ashcroft, 334 F. Supp. 2d 471, 516 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006); *see* Shankman, *supra* note 15, at 259 (arguing that the ECPA NSL's automatic "disclosure ban is not narrowly tailored to serve the government's interests").

263. *See Ashcroft*, 334 F. Supp. 2d at 516 (indicating that "the Government makes convincing points in showing that it would be consistent with the First Amendment to impose . . . limited secrecy in many cases involving a § 2709 NSL"); *cf.* Doe v. Gonzales, 386 F. Supp. 2d 66, 76-77 (D. Conn. 2005) (explaining that "the court cannot conclude on the record in this case that, *in these circumstances*, the government has a compelling interest in barring the disclosure of Doe's identity" because "[n]othing specific about this investigation has been put before the court that supports the conclusion that revealing Does' [sic] identity will harm it"), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006).

sources and methods, disrupt an ongoing investigation, produce diplomatic embarrassment, and so on. Congress may wish to accomplish this change by importing into FISA a mechanism akin to the one in the sneak and peek statute,[264] while expanding the list of secrecy triggering "adverse results" to include harms that are unique to national security investigations.[265] The process afforded by special showing proceedings before the FISA court would be more robust than the certification requirements common to NSLs. This is fitting, given the relative strength of the target privacy interests implicated by the use of various investigative techniques. The wiretapping and physical searches permitted by FISA are especially intrusive, and one would want more process to correspond to the resulting weightier privacy interests. By contrast, the documentary surveillance contemplated by the NSL statutes poses less of a threat to privacy interests—because the target already has shared the data voluntarily with a third party custodian—so less rigorous process should suffice.

The NSL statutes need adjusting, too. NSLs feature special showing requirements in the form of government certifications. But some NSL based secrecy rules should require *ex ante* judicial approval, not just unilateral Executive certifications. In Part III.A, this Article recommends expanding the scope of secrecy requirements to bar disclosure of underlying facts, at least in extraordinary circumstances. It further argues that the government should continue to be able to issue an NSL, along with its investigative fact nondisclosure rule, unilaterally; but if the Executive Branch wanted to go further and impose secrecy as to any underlying facts, it would need to justify such a move before a court. In such circumstances, the standard NSL secrecy certification would be inadequate, and Congress should insist that the Executive make a special showing to the supervising court.

Finally, what are the respective roles of the Executive Branch and of the federal courts in applying special showing requirements? Is the Executive entitled to any judicial deference on the question of whether the harms that secrecy seeks to avert are likely to come to pass? It depends. Federal courts too often treat the question of deference as an all or nothing proposition, invoking "national security" as a talisman that obviates the need to engage in any meaningful judicial review of Executive actions.[266] But the reality is

264. *See* 18 U.S.C. § 3103a.

265. Congress may wish to consider exempting FISA's electronic surveillance and pen/trap subchapters from special showing requirements, either by retaining the existing automatic secrecy rules or substituting presumptive secrecy rules. Secrecy is especially important to prospective intelligence gathering methods; if the surveillance is compromised, targets will act to prevent the data sought from being created at all. In other words, the magnitude of the threatened harm is so significant, and its likelihood of materializing is so great, that in these narrow circumstances the law justifiably might make secrecy the default position.

266. *See* Dep't of Navy v. Egan, 484 U.S. 518, 530 (1988) (emphasizing that "courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs"); Haig v. Agee, 453 U.S. 280, 292 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention."); United States v. Truong, 629 F.2d 908, 913-14 (4th Cir. 1980) ("[T]he courts are unschooled in diplomacy and military affairs, a mastery of which would be essential to passing upon an executive branch request that a foreign intelligence

much more nuanced than that. Whether courts should defer to the government's claim that secrecy is needed to prevent certain threats turns on just what threats are implicated by a given national security investigation.

Some of the harms to be prevented in national security operations are identical to the ones that ordinary criminal authorities seek to forestall. Hence FISA's physical search secrecy rule and the federal sneak and peek statute both aim at preventing the disruption to an ongoing investigation that inevitably results when targets learn that their residences have been searched. In applying the sneak and peek law, courts are called upon on a regular basis to assess whether, for example, disclosure will "endanger[] the life or physical safety of an individual," precipitate "flight from prosecution," or result in "destruction of or tampering with evidence."[267] If judges are able to predict whether a gangster is likely to destroy evidence, there is no compelling reason to deny them the identical power to predict whether a terrorist is likely to do the same. In short, courts should be reluctant to show deference to Executive predictions that certain harms will occur when those harms are common to the criminal context as well as the national security arena.

Other types of threats lie farther away from the heartland of judicial expertise, and it is these harms as to which courts should show some deference to the Executive Branch. Courts simply lack the institutional competence to know whether the disclosure of a particular nugget of information will compromise the government's intelligence sources and methods, or will result in diplomatic embarrassment.[268] The Executive Branch is better positioned, both because of its expertise and because of other contextual information to which it alone has access, to determine what probative value a given sensitive datum will have for an enemy observer.[269] A court considering whether to impose a secrecy requirement will not have access to that informational background and thus will not be able to fully understand the contextual significance of the datum in question.[270]

---

wiretap be authorized.").

267. 18 U.S.C. § 2705(a)(2) (defining "adverse result"); *see id*. § 3103a(b) (authorizing courts to delay notification of a search if there is "reasonable cause" to believe that immediate notice "may have an adverse result (as defined in section 2705)").

268. *See* CIA v. Sims, 471 U.S. 159, 176 (1985) (explaining that "a court's decision whether an intelligence source will be harmed if his identity is revealed will often require complex political, historical, and psychological judgments," and indicating that "[t]here is no reason for a potential intelligence source, whose welfare and safety may be at stake, to have great confidence in the ability of judges to make those judgments correctly").

269. *Id.* at 180 (emphasizing that "it is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence gathering process"); Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 928 (D.C. Cir. 2003) (reasoning that "the government's top counterterrorism officials are well-suited to make this predictive judgment" as to whether disclosure of information will harm the national security).

270. *See Ctr. for Nat'l Sec. Studies*, 331 F.3d at 928 (reasoning that "the judiciary is in an extremely poor position to second-guess the executive's judgment in this area of national security"); N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198, 219 (3d Cir. 2002) (citing "judges' relative lack of expertise regarding national security and their inability to see the mosaic").

Federal courts often blur the distinction between these two classes of threats and defer not just to Executive Branch predictions about the harms that will result from publication of sources and methods, but also to claims about the harms that will result from the disruption of an ongoing investigation. The Sixth Circuit in *Detroit Free Press v. Ashcroft*,[271] recited the litany of harms the government claimed would result if FOIA was interpreted to require it to reveal information about "special interest" aliens who were detained immediately after the 9/11 attacks and were subject to removal proceedings. To wit: disclosure "could subject [detainees] to intimidation or harm," enable terrorists to shift responsibility for a planned attack to a "substitute" cell, and encourage terrorists to "creat[e] false or misleading evidence."[272] Each of these is an instance of the standard adverse results that are common to both national security investigations and ordinary criminal investigations—intimidating witnesses, going into hiding, and interfering with evidence. Yet the Sixth Circuit nevertheless concluded that the Executive Branch's predictions of harm were entitled to deference (though it went on to hold that FOIA still obliged the government to release the information).[273]

In short, to the extent the Executive Branch seeks to justify secrecy on the ground that disclosure will disrupt an ongoing investigation—which courts regularly measure in the criminal context—judges should review those assertions with something resembling de novo review. But to the extent a case for secrecy turns on predictions about the likely effects of disclosure on intelligence sources and methods and on the nation's diplomatic relations—areas that are within the Executive's unique expertise—courts should be more hesitant to second guess a government representation that a nondisclosure obligation is needed.

D. Establishing Limited Duration Secrecy Rules

The interests implicated by secrecy requirements are not static; some interests tend to strengthen over time, whereas others tend to diminish. In particular, the burdens secrecy imposes on the interests of stakeholders such as third parties and targets generally grow weightier.[274] Such burdens tend to increase arithmetically as time passes, with an additional unit of harm added for each moment a secrecy rule is in effect. Each moment that a secrecy requirement is in place prevents third parties from speaking about their experiences, prevents targets from judicially challenging government surveillance, and denies the public the information it needs to check the

271. 303 F.3d 681 (6th Cir. 2002).

272. *Id.* at 705-06.

273. *See id.* at 707 ("Inasmuch as these [government] declarations establish that certain information revealed during removal proceedings could impede the ongoing anti-terrorism investigation, we defer to their judgment.").

274. *Cf.* Elrod v. Burns, 427 U.S. 347, 373 (1976) ("The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.").

Executive Branch and to engage in democratic deliberations.[275] Secrecy rules also can work exponential harms to stakeholders' interests, with a rate of increase that itself increases in response to changed social circumstances. A third party who assists government investigators later might discover that a terrorist attack is imminent, in which case she has a significantly greater speech interest in revealing that information to the public. The privacy interests of an individual whose phone calls the government inadvertently intercepts while surveilling a target will become even stronger when investigators come to believe that he is an active participant in the plot or is committing other crimes. And it is even more essential, when Congress is considering legislation to recalibrate the Executive's investigative powers, that legislators and the public alike have access to all the data they need to make informed policy calls.[276] In such cases, the burdens imposed by secrecy do not just accumulate one unit at a time but are multiplied by an X-factor.

By contrast, the Executive Branch's various operational interests in secrecy generally weaken as time passes. Some of these interests diminish relatively quickly—namely, the government's interests in preventing a pending investigation from being disrupted.[277] While an investigation is underway, secrecy is needed to prevent targets from fleeing, destroying evidence, intimidating witnesses, and the like. But the need to prevent those evils evaporates once the investigation has ended: The targets might be taken into custody; they might be killed by a military strike abroad; the Executive might determine that they are not in fact threats to the national security. National security operations may last longer than their criminal counterparts, but by definition, there is no need to prevent disruption to an ongoing investigation when that investigation is no longer going on.

The force of other Executive interests weakens more slowly. These are the government's interests in preserving the confidentiality of its intelligence sources and methods, and in avoiding the diplomatic embarrassment that can result if it were disclosed that the United States monitored (or received information from) officials of foreign governments. A particular investigation may have concluded, but disclosure of the sources and methods used in that operation could prevent government agents from employing the same techniques in other, related investigations. The use of FISA to intercept emails among al Qaeda operatives A, B, and C may result in A being taken into custody, but B and C may remain at large, and investigators might want to keep eavesdropping on their email traffic to detect clues that will assist in apprehending them. A third party internet service provider who prematurely discloses that it was assisting the FBI in collecting A, B, and C's emails will alert B and C that the government is on their trail and cause

275. *See supra* Parts I.A.2-4.
276. *See supra* Part I.A.5.
277. *See* Butterworth v. Smith, 494 U.S. 624, 632-33 & n.3 (1990) (indicating that the government's interests in secrecy diminish "[w]hen an investigation ends").

them to take steps to evade detection. The completed investigation of A no longer can be harmed, but the still pending investigations of B and C will have been compromised. In short, for as long as the government continues to use particular sources and methods to gather intelligence it will have an active interest in keeping those investigative techniques out of the public eye. A similar need is evident as to surveillance of foreign governments and their agents. Public knowledge that the United States has subjected foreign officials to monitoring can leave a lasting mark on this country's diplomatic efforts long after the surveillance has taken place.

For these reasons, lengthy terms of secrecy to protect intelligence sources and methods and to prevent diplomatic embarrassment have been the historical norm. It took fifty years for all of the grand jury transcripts associated with the government's investigation of Alger Hiss, a suspected Soviet agent, to be released.[278] And it was not until a full century after the Revolutionary War ended—by which time the United States and Britain were close allies—that it was revealed that the personal secretary to Benjamin Franklin, then serving as the American ambassador at Versailles, was a British spy.[279] Yet the traditional practices of the Executive Branch also reflect the reality that, once an investigation has wound down, some details about the manner in which it was conducted can be released without fear of compromising the government's operational interests. In early 2006, President George W. Bush offered details about a number of terrorist plots that national security officials are said to have foiled, including a 2002 plan by Khalid Shaikh Mohammed, mastermind of the 9/11 attacks, to hijack commercial aircraft and destroy the U.S. Bank Tower in Los Angeles.[280]

The government's operational interests thus may necessitate lengthy terms of secrecy, but they do not justify indefinite secrecy. Given that the Executive's interests wane over time and that the interests of other stakeholders only grow stronger, an ideal secrecy regime would eschew permanent nondisclosure obligations. Secrecy rules of only temporary duration are not just sound policy, they likely are required by the Constitution. Secrecy requirements that remain in place long after the harms that justified their initial imposition cannot be regarded as sufficiently tailored to pass constitutional muster.[281] To put matters somewhat differently, permanent secrecy rules are a textbook case of overinclusivity; they bar third parties from re-

278. *See In re* Am. Historical Ass'n, 49 F. Supp. 2d 274 (S.D.N.Y. 1999).

279. O'TOOLE, *supra* note 4, at 1-2.

280. *See* Elisabeth Bumiller & David Johnston, *Bush Gives New Details of 2002 Qaeda Plot to Attack Los Angeles*, N.Y. TIMES, Feb. 10, 2006, at A22.

281. This is why—or at least is one of the reasons why—the Supreme Court in *Butterworth v. Smith*, 494 U.S. 624 (1990), invalidated a Florida grand jury secrecy requirement; the rule *permanently* barred witnesses from revealing to the public the substance of their testimony. *See id*. at 635-36. Likewise, the twin district courts in the Second Circuit that struck down the ECPA NSL's old secrecy requirement did so principally on the ground that it remained in place indefinitely and thus was not precisely calibrated to the harms to be averted. *See* Doe v. Gonzales, 386 F. Supp. 2d 66, 79, 80 (D. Conn. 2005), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006); Doe v. Ashcroft, 334 F. Supp. 2d 471, 512, 514 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

vealing protected information even when such disclosures no longer would work any harm to the Executive Branch's operational interests.

Two ingredients could be used to fashion a temporary secrecy rule: date certain requirements (under which secrecy naturally expires at a statutorily specified point) and review mechanisms (which allow supervisors to cancel a secrecy requirement when it becomes no longer justified). Both features are needed to ensure that secrecy persists no longer than necessary. A date certain requirement creates a presumption that secrecy will terminate, and a review mechanism enables supervising entities to abolish secrecy before its natural lifespan ends, thereby ensuring that the secrecy system can respond to changed circumstances. A nondisclosure requirement containing a review mechanism but lacking a date certain provision presumes that secrecy will persist forever.[282] Such a rule removes the burden of proof from the government to justify the continued imposition of secrecy and places it squarely on the third party, who must demonstrate that secrecy is inappropriate. A rule lacking a date certain requirement thus blinks at the first principle that secrecy is an occasional exception to the general policy of openness, and should not be imposed (or maintained) as the default position. If responsibility for conducting the review is vested in the Executive Branch, not a court, such a rule presents the further risk that secrecy will be maintained as a result of government caprice. An unsupervised Executive may succumb to the temptation of extending secrecy arbitrarily, with the lengthiest terms reserved for disfavored individuals or groups, such as those who oppose the government's national security policies.[283] Equally unacceptable are secrecy rules that have date certain requirements but lack review mechanisms. Such rules lock all stakeholders into a predetermined term of secrecy, and there is no way to adjust a nondisclosure obligation to account for changed circumstances. Even if new developments result in secrecy no longer being appropriate, the stakeholders are without recourse until the date certain arrives.

Hybrid date certain and review mechanism secrecy requirements have the additional advantage of echoing the standards and procedures set out in the Executive Order that governs declassification of sensitive national security information. Executive Order 13,292 generally requires that, at the time of classification, a date certain be established on which the data will be declassified automatically.[284] The default rule is ten years, but it may be extended to twenty-five years where "the sensitivity of the information" warrants.[285] The initial term of classification also is subject to extension, appar-

282. *Cf.* Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 475 (2005) ("[T]he default presumption [under a secrecy rule that lacks a date certain requirement] is that notice will not occur.").

283. *See Gonzales*, 386 F. Supp. 2d at 75 (stressing that secrecy rules have "the practical effect of silencing those who have the most intimate knowledge of the statute's effect and a strong interest in advocating against the federal government's broad investigative powers," namely, "those who are actually subjected to the governmental authority by imposition of the non-disclosure provision").

284. Exec. Order No. 13,292, § 1.5(a), 68 Fed. Reg. 15,315, 15,317 (Mar. 25, 2003).

285. *Id.* § 1.5(b).

ently for additional terms of ten or twenty-five years[286]; but the presumption is that, absent additional action by the government, information will be declassified at the end of the original lifespan. Executive Order 13,292 also contains a review mechanism that allows individuals (apparently including private persons) to petition the government to declassify information on an accelerated basis, if it no longer is sufficiently sensitive to warrant classification.[287] It would be incongruous for details about the use of FISA and NSLs to be presumptively secret and disclosable only in special circumstances, while information that is potentially even more vital to the national security presumptively is subject to declassification after a specified period.

Judged by this standard, the existing system of secrecy is imperfect. Almost all secrecy rules feature temporary nondisclosure requirements in the form of review mechanisms.[288] Yet date certain requirements, with their presumption that secrecy will lapse, are nowhere to be found. Moreover, several investigative authorities' review mechanisms are exceedingly weak, as they either entrust the power to suspend secrecy to the sole discretion of the Executive Branch, contain no standards to guide supervisors' judgment when reviewing the continuing propriety of secrecy, or both. And one investigative tool provides for perpetual secrecy, with no possibility of reprieve. The secrecy regime may be flawed, but it is far less so than it used to be. Until quite recently, perpetual secrecy rules were the norm. In 2006, Congress abolished the NSL statutes' indefinite nondisclosure requirements and replaced them with the temporary rules that generally characterize the current system. The 2006 legislation was a step in the right direction, but Congress still has a ways to go before it reaches its destination.

The NSL statutes' temporary secrecy rules come closest to the ideal.[289] Their review mechanisms place responsibility for abolishing secrecy in the hands of courts,[290] thereby minimizing the risk of government arbitrariness. They also spell out in detail the standards to be applied and procedures to be followed when adjudicating whether secrecy should be maintained, including guaranteeing third parties the right to participate in the litigation.[291] This

286. *See id.* § 1.5(c) (authorizing an original classification authority to "extend the duration of classification," provided the "the standards and procedures for classifying information under this order are followed"). Because the order's "standards and procedures" establish a default initial classification period of ten years, with 25 years available in special circumstances, *see id*. § 1.5(b), it appears that extensions likewise are subject to the ten and twenty-five year rules.

287. *See id.* § 3.5(a), (c).

288. The rules that prevail in standard criminal investigations uniformly provide for temporary secrecy. *See* 18 U.S.C. § 2518(8)(d) (2000) (Wiretap Act date certain secrecy rule, requiring notice to target within 90 days); *id*. § 3103a(b)(3) (Supp. III 2003) ("sneak and peek" date certain secrecy rule, requiring notice to owner of searched property generally within 30 days); *id*. § 3123(d)(2) (Supp. III 2003) (pen/trap secrecy rule with review mechanism, barring disclosures "unless or until otherwise ordered by the court"); FED. R. CRIM. P. 6(e)(3) (grand jury subpoena secrecy rule with review mechanism, barring disclosures subject to certain exceptions including authorization by the supervising court).

289. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, § 115(2), Pub. L. No. 109-177, 120 Stat. 192, 211-12 (2006) (to be codified at 18 U.S.C. § 3511(b)).

290. *See id.*

291. *See id.*

helps ensure procedural regularity. Yet the NSL statutes contain no date certain provision and thus reflect an implicit presumption that secrecy should remain in place indefinitely. Congress should finish the work it started and outfit the NSL statues with date certain requirements that fix a definite date on which secrecy presumptively will lapse.

FISA's physical search and pen/trap subchapters suffer from an additional flaw.[292] Not only do they lack date certain requirements, their skeletal review mechanisms fail to provide effective relief to those burdened by secrecy. Both authorities leave the decision to abolish nondisclosure obligations to the unguided discretion of a supervisor—the Attorney General for physical searches, the FISA court for pen/traps. Nor do they afford third parties the right to participate in proceedings to determine the ongoing propriety of secrecy. The physical search subchapter is an especially narrow escape valve, allowing secrecy to be cancelled only if the property searched was (1) the home of (2) a "United States person" (i.e., an American citizen or permanent resident alien).[293] No mechanism exists to eliminate secrecy as to searches that pertain to individuals who are not United States persons. Nor can secrecy be cancelled as to searches of offices, automobiles, vacation homes, or other types of property owned by United States persons. More troubling still, the physical search subchapter threatens to produce government caprice. Although the FISA court is initially responsible for approving any searches (and thereby authorizing secrecy), it plays no role in the elimination of secrecy; the Attorney General alone may lift a secrecy requirement. By delegating to the Executive the power to determine which third parties will be relieved of their nondisclosure obligations, the rule runs the risk of officials exercising their discretion to retain secrecy as to disfavored individuals or groups. That in turn incentivizes the affected parties to curry favor with the government—for example, by not exercising their rights to challenge investigators' requests for information or by turning over more information than investigators have asked for. So in addition to equipping FISA's physical search and pen/trap subchapters with date certain provisions, Congress would do well to fortify their review mechanisms to more closely resemble those of the NSL statutes.

The secrecy rule in FISA's electronic surveillance subchapter is even worse.[294] It is perpetual; it neither fixes a date certain on which secrecy will lapse nor does it establish a review mechanism to cancel secrecy when it is no longer appropriate. Elsewhere in this Article I have suggested that the unique harms threatened by the use of prospective surveillance techniques may justify a quicker trigger for the imposition of secrecy.[295] But not even that argument justifies retaining secrecy long after the harms—of whatever

292. *See* 50 U.S.C. § 1825(b) (2000); 50 U.S.C.A. § 1842(d)(2)(B)(ii)(I) (Supp. 2006).
293. *See id.* § 1801(i).
294. *See id.* § 1805(c)(2)(B) (Supp. III 2003), *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, § 102(b)(1).
295. *See supra* note 265.

magnitude—that made it necessary have dissipated. The electronic surveillance authority should see its perpetual secrecy rule abolished and replaced with a temporary one.

Congress therefore should amend FISA and the NSL statutes to include, in addition to review mechanisms, the date certain requirements needed to ensure a closer fit between secrecy rules and the precise evils they seek to counter. How long should that initial term of secrecy generally persist? No *a priori* answer exists. A wide range of acceptable options is available: one year, the ten or twenty-five years specified by the classification Executive Order, or an indeterminate "reasonable period" chosen by the FISA court at the time it authorizes the surveillance. Ultimately, the fact that secrecy presumptively will terminate on a date certain is more important than precisely when it will terminate, especially given the presence of review mechanisms. About all that can be said is that the period should not be so long as to be the equivalent of the indefinite secrecy requirements that used to characterize the system. But the initial term should be longer in national security investigations than under garden variety criminal authorities, given the greater force of the Executive Branch's operational interests and the reality that national security operations often unfold over lengthier periods of time.

The harms that justified initial periods of secrecy will not always dissipate on schedule. By the time the date certain arrives, the government may not yet have apprehended the principal target because it wishes to learn more about his co-conspirators, or investigators may be using the same intelligence sources and methods in related operations. The secrecy regime therefore needs a mechanism by which, in appropriate circumstances, a nondisclosure obligation that is set to expire can be renewed for an additional fixed period of time. But if the need for such a mechanism is evident, so is the potential for abuse. Extension could be layered on top of extension *ad infinitum*, thereby defeating the very purpose of insisting on date certain rules in the first place. Strict safeguards would need to be in place to ensure that any extensions of date certain rules do not metamorphose into permanent ones, and to ensure that the duration of secrecy requirements remain precisely tailored to the threats they are designed to ward off.

First, it goes without saying that any extension of secrecy should not be indefinite but should itself be for a statutorily specified term. Congress would have to choose whether an extension would persist for the same period of time as the initial secrecy requirement or be of shorter duration; it would be hard pressed to justify an extension the length of which exceeds the initial period of secrecy. Second, for each extension, the Executive Branch should be required to make at least the same showing that was necessary to justify the initial nondisclosure requirement. That is, it should have to demonstrate that disclosure of the surveillance continues to pose a threat to the integrity of the investigation, to the confidentiality of intelligence

sources and methods, or to other aspects of national security.[296] Something like a de novo showing should be required; the fact that the Executive Branch's operational interests at some point in the past were deemed sufficient to justify secrecy would not be at all relevant to the question whether, at the time of the proposed extension, there is a continuing need for secrecy. Congress might even consider writing into the law a presumption against extensions of secrecy (or at least a presumption against multiple such extensions).

Finally, whether an extension of secrecy is justified in an individual case will depend critically on precisely which threatened harms the Executive Branch invokes to justify the nondisclosure requirement. Only in rare circumstances will the risk of disrupting an ongoing investigation justify repeated extension of secrecy rules; such harms tend to dissipate relatively quickly and do not long outlive the particular investigation with which they are associated. By contrast, the system should be more tolerant of multiple extensions of nondisclosure requirements when the government's purpose is to protect its intelligence sources and methods or to forestall diplomatic embarrassment. A daisy chain of such extensions conceivably could produce lengthy terms of secrecy that run many years and thus may resemble the indefinite nondisclosure requirements that this Article (and many courts) have condemned. But while any lengthy period of secrecy imposes significant burdens on speech, privacy, and public accountability interests, such burdens are lessened to the extent they are adopted on case by case bases through individualized determinations of necessity, and to the extent the system contemplates an eventual stopping point.[297]

CONCLUSION

George Washington was right, but so was Patrick Henry. It really is true of national security investigations that "upon secrecy, success depends."[298] But it is no less the case that "the most wicked and pernicious of schemes" can be accomplished "under the dark veil of secrecy."[299] One reason why it is so difficult to formulate optimal secrecy policies is that the process does not involve a simple two column ledger, with a debit on one side precisely corresponding to a credit on the other. Rather, it is a multidimensional matrix, and it features strong arguments on all fronts. Each stakeholder—whether the Executive Branch, investigative targets, third party witnesses,

296. The procedures for extending date certain secrecy rules thus would dovetail with the special showing requirements under which secrecy initially would be authorized. Secrecy neither could be imposed nor maintained as the default position, but could only be utilized upon the government's demonstration that it is needed.

297. *See* Doe v. Gonzales, 386 F. Supp. 2d 66, 79 (D. Conn. 2005) (emphasizing that, while the government's "interest cannot continue indefinitely," it may justify secrecy that lasts into "the distant future," and suggesting that secrecy justifiably may "continue[] until a subject's or someone else's death (if an individual) or dissolution (if an entity)"), *vacated as moot*, 449 F.3d 415 (2d Cir. 2006).

298. Letter to Col. Elias Dayton, *supra* note 1, at 479.

299. 3 ELLIOT'S DEBATES, *supra* note 2, at 170.

the general public, or members of Congress—may claim, with some justice, that their interests are so weighty that they ought to be decisive. Which interest should prevail in a particular setting is radically contextual, and the outcome will depend on the interactions among those myriad interests. This tension among rival claimants, and rival claims, has been with us for more than two centuries, and it cannot be resolved by invoking simplistically any one set of interests as a trump card. My hope is that the analysis and prescriptions contained in this Article will prove a modest contribution to that enduring conversation.

Toward that end, our system of investigative secrecy would benefit from reforms that would better prioritize the underlying values of secrecy in the positive requirements of secrecy law. For starters, Congress should consider creating a mechanism by which nondisclosure requirements may be applied, in special cases, to sensitive underlying data in the hands of third parties, not just to facts about the government's investigative activities. Congress also would do well to strengthen the inexplicably weak secrecy rules the current regime assigns to certain prospective intelligence gathering techniques, such as FISA's wiretap electronic surveillance authority. Next, the investigative secrecy system would benefit from abolishing the automatic nondisclosure rules that characterize the current regime and replacing them with special showing requirements under which the Executive Branch has to demonstrate the need for secrecy. Finally, Congress should consider abolishing the existing regime's perpetual secrecy requirements and substituting rules that lapse after a set period of time. Reforms such as these would be a modest step toward ensuring that the Executive Branch is able to mount maximally effective national security investigations while at the same time preventing the vital interests of other stakeholders from being trampled needlessly.