CONSTITUTIONAL REGULATION OF NATIONAL SECURITY INVESTIGATION: MINIMIZING THE USE OF UNRELATED EVIDENCE

*Matthew R. Hall**

TABLE OF CONTENTS

* Assistant Professor, University of Mississippi School of Law. Before joining the faculty at the University of Mississippi, the author worked at the Department of Justice in the Civil Division's Office of Immigration Litigation on a team of attorneys handling immigration matters related to national security and counterterrorism. The author received research support for this Article from the Center for Justice and Rule of Law at the University of Mississippi School of Law, which is funded by the Office of Justice Programs at the Department of Justice. The opinions expressed in this Article, however, are those of the author alone.

I. INTRODUCTION

Could courts regulate national security investigation if the Supreme Court found the full arc of intelligence surveillance statutes constitutional? Yes. The principle of minimization—the process of limiting the acquisition, retention, and dissemination of private information acquired during an investigation—could evolve to function as a limit on the use of information unrelated to national security. Even if the Foreign Intelligence Surveillance Act ("FISA"),[1] as amended by the USA PATRIOT Act ("Patriot Act"),[2] passes constitutional scrutiny, this new body of constitutional doctrine

1. Originally enacted as the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1863 (2000)).

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.). Only a portion of the Patriot Act's provisions, which span over three hundred pages, alter the structure of FISA. Several of those provisions are scheduled to expire as this Article goes to press, although Congress appears prepared to renew these sections with some amendment. *See* Laurie Kellman, *Congress Extends Patriot Act Five Weeks*, WASH. POST, Feb. 3, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/02/AR2006020201915.html. This Article does not attempt to address the debate over Patriot Act renewal or to analyze the ramifications of the multitude of proposed amendments. Nor does the Article assess domestic surveillance by the National Security Agency (a development that arose as this Article progressed through the law journal editorial process). For a few brief thoughts on the relationship between such surveillance and the proposals in this Article, see *infra* note 43.

would help alleviate some of the concerns that attend national security surveillance. Previous efforts at regulation problematically restricted the initiation of national security investigation. By functioning as a "use limit," preventing the Executive Branch from using evidence unrelated to national security, the minimization principle would allow necessary national security investigation but would regulate the process by preventing it from, either in appearance or reality, usurping normal criminal procedures. Indeed, no court should validate the current national security investigation system without conditioning that approval on the recognition of a use limit.

The premise that the courts will uphold the current universe of national security investigation statutes and procedures is emphatically not normative; this Article is not meant as an argument that the courts should uphold FISA. Nor does this Article reach for an endpoint at which national security investigation is either constitutionally validated or censured. Similarly, it does not propose a set of legislative or administrative reforms designed to soften the rough texture of national security investigation or ameliorate its shortcomings. The Article operates on the assumption that September 11, 2001, caused an evolutionary leap in the inherent structure of national security investigation—a leap that the courts will not attempt to reverse. Pragmatically, then, instead of arguing for courts to turn back the clock, focus should turn to regulating the scope and practice of national security investigation.

Given the assumption that courts do find FISA constitutional, much of the current scholarly debate loses its immediacy. Many of the cogent arguments about either the constitutional infirmity of FISA or the constitutional soundness of national security investigation take on the tenor of policy debates rather than vibrant legal arguments. Crucially, the concerns underlying those arguments, especially the arguments against the Patriot Act amendments to FISA, should serve as the vital propulsive force for the evolution of constitutional doctrine. Therefore, this Article addresses the essential apprehensions about national security investigation by formulating a proposal for constitutional regulation. This Article anticipates the next stage of the discussion—the one occurring the day after the Supreme Court upholds FISA—by providing a robust constitutional response to the evolution of national security investigation.

Before proceeding further, some semantic clarifications are in order. The term "national security investigation," as used in this Article, means the scrutiny of foreign threats to peace and stability within the United States through the use of electronic surveillance,

physical search, and a variety of other tools directed toward obtaining documentary and transactional records. Primarily, the structure of national security investigation flows from FISA, as amended by the Patriot Act. FISA grants the Executive extraordinary powers to comprehensively and surreptitiously investigate targets. For example, a single surveillance order would permit the FBI to "conduct, simultaneously, telephone, microphone, cell phone, e-mail and computer surveillance of the . . . target's home, workplace and vehicles;" while a single search order would authorize searches of "the target's residence, office, vehicles, computer, safe deposit box and U.S. mails."[3]

Given the remarkable power of national security investigation, the Article continues in Part II with an examination of the fundamental concerns and apprehensions about that process. It turns in Part III to the basics—the statutes and tools of national security investigation. In Part IV, the Article compares national security investigation and normal criminal law processes. The Article continues in Part V to address the evolution of national security jurisprudence in order to understand the constitutional framework under which courts have examined national security investigation. In Part VI, the Article makes use of that framework by proposing that the constitutional requirement of minimization should evolve to limit the use of evidence acquired through national security investigation but unrelated to a national security matter. This penultimate Part of the Article also examines the details and implications of such a proposal: how it would function as an exclusionary rule, where and how it fits into the surrounding jurisprudence, whether it should apply beyond a criminal case-in-chief, whether it should contain an exigency exception, whether the rule conflicts with the plain view doctrine, how it would interact with the fruit of the poisonous tree doctrine, whether the rule would improperly prevent common uses of information derived from national security investigation, and ways through which the Executive might circumvent the rule. Finally, in the Conclusion, the Article critiques the proposal.

II. FUNDAMENTAL CONCERNS

National security investigation has attracted a significant body of scholarship, with much of the recent work devoted to either condemning[4] or endorsing[5] the Patriot Act amendments to FISA.[6]

3. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 616-17 (FISA Ct. 2002), *rev'd on other grounds, In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

4. *See, e.g.*, James X. Dempsey, *Section 206: Roving Surveillance Authority*

This debate has taken on a classic polarized and polemic form: either the primary purpose test is constitutionally mandated[7] or the

Under FISA; Why Section 206 Should Be Modified, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT 18 (Stewart A. Baker & John Kavanagh eds., 2005) [hereinafter Dempsey, *Section 206*]; James X. Dempsey, *Sections 209, 212, and 220: Access to Wire and Electronic Communications; Why Sections 209, 212, and 220 Should Be Modified*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* at 32 [hereinafter Dempsey, *Sections 209, 212, and 220*]; Kate Martin, *Section 203: Authority to Share Criminal Investigative Information; Why Sections 203 and 905 Should Be Modified*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* at 4 [hereinafter Martin, *Sections 203 and 905*]; Suzanne Spaulding, *Intercepting Lone Wolf Terrorists; "If It Ain't Broke, Don't Fix It," in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* at 86; Peter P. Swire, *Sections 214 and 215: Pen Register and Trap and Trace Authority Under FISA and Access to Business Records Under FISA (Libraries Provision); Reply*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* at 54 [hereinafter Swire, *Section 214*]; *see also* William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1192 (2003); Jennifer M. Collins, *And the Walls Came Tumbling Down: Sharing Grand Jury Information With the Intelligence Community Under the USA PATRIOT Act*, 39 AM. CRIM. L. REV. 1261 (2002); James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1483-86 (2004); Jules Lobel, *The War on Terrorism and Civil Liberties*, 63 U. PITT. L. REV. 767, 785-90 (2002); Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1111-19 (2002); Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1330-39 (2004) [hereinafter Swire, *The System*]; Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179, 180 (2003); Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 974-84 (2002); David Hardin, Note, *The Fuss Over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 318-24 (2003); Sharon H. Rackow, Comment, *How the USA PATRIOT Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1674-80 (2002); Jeremy C. Smith, Comment, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412, 441-52 (2003); George P. Varghese, Comment, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 421-30 (2003). *See generally* Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of the USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37, 52 n.103 (2005) (collecting articles).

5. *See, e.g.*, Viet Dinh, *Section 203: Authority to Share Criminal Investigative Information; Reply, in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* note 4, at 10; Andrew C. McCarthy, *Section 218: Amending the FISA Standard; Why Section 218 Should Be Retained*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* note 4, at 66.

6. *See infra* notes 60, 69, 92, 103, 197 and accompanying text; *see also infra* Part V.D (describing the changes to FISA made by the Patriot Act, and the judicial reaction).

7. *See, e.g.*, Banks, *supra* note 4, at 1192; Swire, *The System*, *supra* note 4,

Constitution does not suicidally constrain national security investigation in an inefficient manner.[8] Admittedly, many commentators have proposals for reform.[9] The vast majority of critics envision the debate unfolding toward an endpoint—FISA as amended is struck down, upheld, or further amended. If the courts uphold FISA with its Patriot Act amendments, this debate does not become moot. Instead, it should fuel the development of robust constitutional doctrine capable of regulating national security investigation.

Fundamentally, concern about national security investigation flows from our historical experience of invasive law enforcement practices and abusive national security investigation of domestic threats. Sweeping national security investigation, particularly electronic surveillance, resembles a general warrant, the use of which moved the Founders to include the Fourth Amendment in the Bill of Rights.[10] More immediately, suspicion about national security investigation flows from the Executive's use of warrantless surveillance against a variety of civil rights, anti-war, and dissident organizations during the second half of the Twentieth Century.[11] Ironically, Congress enacted FISA in part to prevent the continuation of these abusive practices.[12]

Framed even more broadly, the basic concern lies in the nature of national security investigation itself: the government spying on

at 1339-68; Breglio, Note, *supra* note 4, at 196-97; Hardin, Note, *supra* note 4, at 342-44; Rackow, Comment, *supra* note 4, at 1680-83; Varghese, Comment, *supra* note 4, at 421-30.

8. *See, e.g.*, Dinh, *supra* note 5, at 13; McCarthy, *supra* note 5, at 70.

9. *See, e.g.*, Banks, *supra* note 4, at 1185-88; Risa Berkower, *Sliding Down a Slippery* Slope*? The Future Use of Administrative Subpoenas in Criminal Investigations*, 73 FORDHAM L. REV. 2251, 2286-87 (2005); Fernando A. Bohorquez, Jr., *Challenges to Challenging the Patriot Act*, 77 N.Y. ST. B.J. 24, 32-33 (2005); Collins, *supra* note 4, at 1279-86; Dempsey & Flint, *supra* note 4, at 1488-1502; Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 458-60 (2005); Swire, *The System*, *supra* note 4, 1350-68; Woods, *supra* note 4, at 68-71; Breglio, Note, *supra* note 4, at 203-15; Evans, Comment, *supra* note 4, at 985-89; Smith, Comment, *supra* note 4, at 452-53.

10. *See* Berger v. New York, 388 U.S. 41, 58-60 (1967) (describing unrestricted electronic surveillance as a general warrant—a roving commission to intrude, issued without reference to a particular offense or evidence); *see also* Dempsey, *Section 206*, *supra* note 4, at 19 (examining the dangers of roving surveillance); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1269-70 (2004) (comparing electronic surveillance practices to general warrants).

11. *See* Saito, *supra* note 4, at 1078-1104. This concern, perhaps, is not merely historical. *See* Michael Dobbs, *FBI Monitored Web Sites for 2004 Protests*, WASH. POST, July 18, 2005, at A3; Eric Lichtblau, *Large Volume of F.B.I. Files Alarms U.S. Activist Groups*, N.Y. TIMES, July 18, 2005, at A12.

12. *See* S. REP. NO. 95-604 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904.

its own people.[13] Indeed, the Supreme Court has recognized that an Executive equipped with the power to spy within its own borders will have a tendency to target those who most dramatically oppose that government, and a people who know that their government possesses the spy power will suffer the chilling effects most profoundly when they contemplate dissent.[14] Because First Amendment jurisprudence entails a purpose and effects test to evaluate the chilling of speech, and because only a rare challenge to national security investigation would yield evidence of an illicit purpose, the Fourth Amendment carries a particularly heavy load in preventing FISA, and other intelligence tools, from deterring dissent.[15] Even without the targeting of dissent, widespread government surveillance carries with it a risk of self-censorship stemming from the fear of government monitoring. While this same phenomenon can serve to prevent terrorism, it also stifles individualism and resembles totalitarian efforts at social control.[16] To address this problem, privacy needs protection not only doctrinally, but psychologically—the relevant jurisprudence needs to function in court, and it needs to reassure the public by ameliorating fear of surveillance.[17]

Although judicial supervision of national security investigation[18] provides sufficient process to dispel some suspicions of Executive abuse, reducing what Jeffrey Rosen has referred to as the "Nixon effect,"[19] judicial supervision does not eliminate the potential

13. *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 4 & n.16 (2000) (explaining that national security surveillance has its roots in spying rather than policing).

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

15. *See* Banks & Bowman, *supra* note 13, at 6; Saito, *supra* note 4, at 1057.

16. *See* Solove, *supra* note 10, at 1267-68. *But cf.* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 27-28 (2004) (stating that many people voluntarily remain ignorant of surveillance and suffer injury only if the Executive acts against them).

17. *See* Solove, *supra* note 10, at 1270.

18. *See infra* Part III.A (explaining the process of obtaining warrant-like orders from the FISA court).

19. *See* Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 ARIZ. L. REV. 607, 611 (2004) ("The modern version of the general search is President Nixon's effort to scan the tax returns of Vietnam protestors and threaten them with prosecution."); *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 810 (1994) ("Due process values may even call for judicial preclearance of certain types of government searches and seizures, if there are good reasons for suspecting strong and systematic over-zealousness on the part of certain segments of executive officialdom."); Freiwald, *supra* note 16, at 34 (describing misuses of surveillance information); Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 162 (2004) (describing procedural limits on surveillance as "structural hedges" preventing the abuse of power).

corrupting influence of extraordinary surveillance power. Indeed, the perilous temptations of electronic surveillance—its "power and effectiveness"—are inextricably wedded to its legitimate attractiveness.[20]

The danger of national security investigation lies not only in the pernicious possibility of outright abuse, but also in the slow corruption of our institutions—for example the elimination of grand jury secrecy[21] or the erosion of the judicial role through devices like national security letters.[22] Similarly, the prospect of "mission creep" poses a long-term institutional danger.[23] The concern springs from the ability of sophisticated investigative techniques to discern patterns of criminal conduct from large amounts of data—a process often called "data mining"[24] or "dataveillance."[25] If the FBI compiles troves of information during its intelligence operations,[26] the temptation to sift that data and unearth crime could lead the agency to shift these efforts from national security to regular crime control once it had the information and tools at its disposal—the agency's mission might shift, or creep, from one based on particularized investigation to omnipresent information gathering.[27] Indeed, a jurisprudential license for mission creep appears in the Supreme

20. *See* Freiwald, *supra* note 16, at 17 ("In general, electronic surveillance has permitted law enforcement agents to be where they could not otherwise be, to perceive what they could not otherwise perceive, to have nearly infinite endurance, and to retain information forever."); *id.* at 43-52; Kreimer, *supra* note 19, at 155-56.

21. *See* Collins, *supra* note 4, at 1264-65; *see also infra* Part III.C (describing the changes to grand jury secrecy in the Patriot Act).

22. *See infra* Part III.B (describing national security letters); *cf.* Berkower, *supra* note 9, at 2285 (expressing concern over the loss of judicial review in proposed FBI administrative subpoena authority).

23. *See* Berkower, *supra* note 9, at 2286.

24. *See id.*; Kreimer, *supra* note 19, at 164-65.

25. *See* Rosen, *supra* note 19, at 615.

26. *See* Kreimer, *supra* note 19, at 134-35 (describing the Justice Department's efforts to develop a national intelligence "data space").

27. *See* Berkower, *supra* note 9, at 2280-86; Dempsey & Flint, *supra* note 4, at 1492 ("The fear is that having developed an effective and justified analytic tool and gained access to commercial sources of information for counterterrorism purposes, an agency or other agencies will then seek to use the information for purposes extending beyond counterterrorism, purposes that on their own would not have supported access to the information, but that seem to offer benefits at a marginal cost once the information is available."); *see also* Martin, *Sections 203 and 905*, *supra* note 4, at 10 ("One of the most basic protections against government abuses has been the principle that a government agency should only collect information about individuals that it needs for a specific and articulated purpose, should use it only for the purposes for which it was collected, should not keep it any longer than necessary, and should not share it with other government agencies except for very good reasons.").

Court's formless "special needs" doctrine.[28]

Nearly universally, the critics of national security investigation argue that FISA allows the Executive to conduct more sweeping and lasting surveillance than under the criminal law, and on a different, if not lower, showing of cause.[29] Accordingly, the critics fear that the Executive will use national security investigation pretextually when the real goal is normal law enforcement.[30] Although this concern is certainly not new,[31] it has accelerated because of the Patriot Act amendments to FISA, the increased cooperation and sharing of information between intelligence and criminal investigators,[32] and the Executive's focus on terrorism, which more closely resembles ordinary crime than does traditional espionage.[33]

The secrecy of national security investigation constitutes the ultimate problem—it facilitates the abuse of power.[34] While Congress oversees the Executive's overall conduct of national security investigation, a specific inquiry remains secret from the target, unlike criminal law where the target normally receives contemporaneous or reasonably prompt notice.[35] Although the target learns of a national security investigation if the government

28. *See* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 598-99 (1995) (arguing that the special needs "concept threatens to envelop Fourth Amendment analysis, making the special needs test the rule, rather than the exception"); *see also infra* notes 251-253 and accompanying text (describing the possible use of the special needs doctrine to validate FISA).

29. *See infra* Parts IV.A-B (describing the differences between FISA and criminal law).

30. *See* Banks, *supra* note 4, at 1171 (stating that "prosecutors may seek to use FISA to end-run the traditional law enforcement warrant procedures" and thus "become less accountable to the Constitution and courts"); Solove, *supra* note 10, at 1291 (explaining the danger of an "end run" around the protections of Title III); *id.* at 1303 (describing judicial efforts to ensure that the Executive uses FISA only for bona fide, rather than pretextual, purposes); *see also* Parts V.A-D (noting the judicial response to the pretext concern).

31. The concern long predates the enactment of FISA in 1978. *See* Abel v. United States, 362 U.S. 217, 230 (1960).

32. *See infra* notes 69-82 and accompanying text; *see also* Part III.C (describing cooperative efforts and information sharing under the Patriot Act).

33. *See* Saito, *supra* note 4, at 1118-19; Solove, *supra* note 10, at 1291; Hardin, Note *supra* note 4, at 341-44 (characterizing FISA's "intricate framework" as achieving a "constitutional and political equilibrium" but sacrificing traditional probable cause); Rackow, Comment, *supra* note 4, at 1680-81.

34. *See* Berger v. New York, 388 U.S. 41, 60 (1967); Freiwald, *supra* note 16, at 19; Solove, *supra* note 10, at 1290; Christina E. Wells, *Information Control in Times of Crisis: The Tools of Repression*, 30 OHIO N.U. L. REV. 451, 493-94 (2004) (describing the link between the "culture of secrecy" and efforts at achieving political control).

35. *See infra* notes 140-142, 160-164 and accompanying text (comparing the FISA and criminal law notice procedures).

brings suit, even then the individual never sees the originating documentation as in a criminal case.[36] If the national security paradigm truly paralleled criminal law, the targets of FISA search and surveillance would receive notice and have the opportunity to challenge the investigation with full access to the originating documentation.[37] In the criminal law universe, the Executive must account directly with the target for its actions, but, when it comes to national security, secrecy allows the Executive to remain unanswerable.[38]

These critiques offer several salient lessons to help guide the formulation of constitutional doctrine capable of regulating FISA. First, any proposal should provide some reassurance that it can prevent abuse. Second, regulation of national security investigation should diminish the deleterious effects of surveillance on privacy and its chilling effects on dissent. A new doctrine ideally should work to retard mission creep. Limitations on national security investigation must deter the pretextual use of intelligence investigation. Finally, new rules should attempt to compensate for the unavoidable secrecy inherent in national security. With these fundamental apprehensions firmly in mind and with a sense of the goals of constitutional regulation of national security investigation, it now makes sense to examine the specific statutes and tools employed by the Executive.

III. THE STRUCTURE OF NATIONAL SECURITY INVESTIGATION

National security investigation, as this Article uses the term, refers to surveillance and searches conducted by the FBI[39] under the authority of FISA and a few other scattered statutes. This form of investigation focuses on foreign threats to national security—including foreign powers, foreign intelligence operations, and international terrorism—within the United States. Indeed, a lay person might well refer to national security investigation as counterintelligence and counterterrorism.[40]

36. *See infra* notes 83-88 and accompanying text (describing FISA's challenge process); *see also infra* note 322 (explaining that in no reported case has a target ever received the originating documentation).

37. *See* Banks, *supra* note 4, at 1161-62; *see also* Amar, *supra* note 19, at 803-04 (explaining that, even for electronic surveillance under the criminal law, the level of secrecy strains the constitutional limits on reasonableness).

38. *See* Freiwald, *supra* note 16, at 19.

39. *See* Exec. Order No. 12,333, § 1.14, 3 C.F.R. 210 (1981-82), *reprinted in* 50 U.S.C. § 401 (2000) (assigning the task of domestic counterintelligence to the FBI).

40. Some terminological confusion may arise because FISA covers foreign threats within the United States, while the non-FISA definition of "foreign intelligence" excludes counterintelligence. *See id.* § 3.4(d), 3 C.F.R. 215 (1981-

A. FISA

Investigation under the ambit of FISA takes several forms based on an order approved by the Foreign Intelligence Surveillance Court ("FISC"),[41] or in limited circumstances, the approval of the Attorney General. While conceivably the Executive may claim or possess independent and inherent constitutional authority for additional national security powers,[42] Congress has starkly framed that issue, at least as far as it concerns electronic surveillance, by cautioning that FISA and normal criminal warrants constitute the "exclusive means" of surveillance.[43] The statute grants its broad investigative powers only over foreign, rather than domestic, threats to national peace and order.

1. Electronic Surveillance and Physical Searches

The standard FISA investigation begins with a request to the FISC for a surveillance or search order. The Attorney General must approve[44] an application establishing probable cause that the target is a "foreign power or agent of a foreign power."[45] For surveillance, the Executive must also show probable cause that the target uses or will use the locale at which the surveillance will occur. For a physical search, the application must demonstrate that the target controls the relevant property or that the property is in transit to or

82), *reprinted in* 50 U.S.C. § 401 (2000) (defining "foreign intelligence").

41. 50 U.S.C. § 1803(a) (2000 & Supp. I 2001). The FISC conducts its business effectively in secret. *Id.* § 1803(c). The Executive appeals denials to a three-judge "court of review"—the Foreign Intelligence Court of Review ("FISCR"). *Id.* § 1803(b).

42. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 320-22 (1972) (rejecting the Executive's claim of authority to conduct warrantless surveillance of a non-foreign target but leaving open the status of surveillance directed at foreign targets).

43. *See* 18 U.S.C. § 2511(2)(f) (2000); *see also* Banks & Bowman, *supra* note 13, at 92 (explaining this exclusivity provision). Indeed, this Article does not purport to address the controversy over whether the Bush Administration possesses either statutory or inherent authority to conduct surveillance of communications between people in the United States and suspected terrorists abroad. *See* Adam Liptak, *In Limelight at Wiretap Hearing: 2 Laws, but Which Should Rule?*, N.Y. TIMES, Feb. 7, 2006, at A2. Presumably, a surveillance program with no statutory controls—such as the one undertaken by the Bush Administration—would demand similar, if not significantly more stringent, constitutional regulation than the tightly regulated process under FISA. Thus, if the Bush Administration's use of the National Security Agency to conduct domestic surveillance proves constitutional, the limitations on the use of unrelated evidence proposed in this Article, should apply with equal force to information gathered through those investigations. *See infra* Part VI.

44. 50 U.S.C. §§ 1805(a)(2), 1824(a)(2) (2000); *see also* Exec. Order No. 12,139, 3 C.F.R. 397-98 (1979-80) (empowering the Attorney General to approve applications for electronic surveillances and physical searches).

45. 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A).

from the target.[46]

Under FISA, the probable cause standard depends on the strength of the relationship between the target and the foreign threat.[47] The statute straightforwardly defines "foreign power" as foreign governments, foreign political organizations, and international terrorist groups.[48] The heavy lifting involved in distinguishing between domestic and foreign threats, however, takes place through the rubric of "agent of a foreign power." Critically, the requirements differ depending on whether the Executive targets a so-called "United States person," including United States citizens and permanent resident aliens,[49] or a non-United States person.

To establish that a non-United States person is an agent of a foreign power, the statute demands that the Executive submit probable cause that the target acts for a foreign power, is or may be involved in espionage for a foreign power, or is involved in international terrorism.[50] Notably, under the final possible classification, the Executive need not demonstrate a connection with a foreign power, although the foreign versus domestic distinction persists in the requirement of evidence of a connection to *international* terrorism. This aspect of the provision allows the Executive to target a non-United States person who acts as a "lone wolf" terrorist.[51] By distinction, to establish that a United States person is an agent of a foreign power, the statute mandates that the Executive provide probable cause that the target is *knowingly* involved in espionage, sabotage, or international terrorism for a foreign power.[52]

The net result of the repeated statutory trope of "foreign power" allows the Executive abundant permutations in the use of FISA in a traditional counterintelligence function focused on the spying operations of other governments. On the other hand, to employ FISA against an individual as a tool of counterterrorism, the

46. *Id.* §§ 1805(a)(3)(B), 1824(a)(3)(B).

47. *Compare* § 1801(b)(2) (2000) (requiring proof of a knowing mental state) *with* § 1801(b)(1) (requiring only proof of conduct) *and* § 1805(d) (dispensing with numerous application requirements and limits if the investigation targets a foreign power itself rather than an agent thereof) *and* §§ 1802(a), 1822(a) (allowing, based on the Attorney General's certification, without a FISC order, surveillance and searches of a foreign power itself).

48. *Id.* §§ 1801(a), 1821(1).

49. *Id.* §§ 1801(i), 1821(1).

50. *Id.* §§ 1801(b), 1821(1).

51. *See* Mary DeRosa, *Intercepting Lone Wolf Terrorists; Summary*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* note 4, at 81-82. Some commentators have criticized the "lone wolf" provision as a form of legislative mission creep, moving FISA incrementally away from its focus on foreign threats. *See* Spaulding, *supra* note 4, at 89-90.

52. §§ 1801(b)(2), 1821(1).

Executive must rest on a more slender reed and show a connection to international terrorism.[53] Because FISA covers terrorism itself and preparatory conduct, the sweep of the statute includes logistic support far removed from the violent acts themselves.[54]

The statute adds an important caveat to the probable cause analysis to prevent FISA investigations from trenching on constitutional liberties. Namely, the scheme prohibits the probable cause finding that a United States person is an agent of a foreign power from resting "solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States."[55] This provision finds strong reinforcement in the requirement that a United States person acts as an agent of a foreign power only if that person possesses a knowing mental state.

The statutory scheme also contains exceptions to the requirement that the Executive particularly identify either the target or the locus of the investigation. Under the electronic surveillance provisions, the statute allows the Executive to submit a description of the target and communication device if the target's identity is unknown,[56] and it allows the Executive to conduct "roving" surveillance if necessary.[57] Similarly, the physical search provisions allow the Executive to submit a description of the target if the identity is unknown.[58]

Two additional limits—not based on probable cause—serve to regulate access to surveillance and search authority. Foremost, the Executive must certify that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information.[59] Importantly, the Patriot Act lowered the threshold for conducting a FISA investigation by introducing the term "significant" to FISA; previously, the statutory language embodied the more rigorous

53. *Id.* §§ 1801(c), 1821(1).

54. *See* FBI OFFICE OF THE GENERAL COUNSEL, NATIONAL SECURITY LAW UNIT, WHAT DO I HAVE TO DO TO GET A FISA? 8 (2002), http://www.epic.org/privacy/terrorism/fisa/fisa-recipe.pdf [hereinafter FBI OGC] (stating that "'preparation' as used here takes its meaning from the context of the definition of 'international terrorism,' it could reasonably be interpreted to include, *e.g.*, providing the personnel, training, funding or other means for the commission of acts of terrorism, rather than participating in a particular bombing"); *cf.* 18 U.S.C. § 2339A (2000 & Supp. II 2002) (criminalizing providing material support to terrorists); 8 U.S.C. § 1182(a)(3)(B)(iv)(VI) (2000 & Supp. II 2002) (defining, for immigration purposes, the term "engage in terrorist activity" as meaning, among other things, providing material support to terrorists).

55. 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A).

56. *See id.* § 1805(c)(1)(A)-(B) (2000 & Supp. I 2001); *see also* Mary DeRosa, *Section 206: Roving Surveillance Authority Under FISA; Summary*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT, *supra* note 4, at 18.

57. § 1805(c)(2)(B); *see also* DeRosa, *supra* note 56, at 17.

58. § 1824(c)(1)(A).

59. *Id.* §§ 1804(a)(7)(B), 1823(a)(7)(B) (Supp. I 2001).

standard that foreign intelligence collection had to constitute "the purpose" of the investigation.[60] The statutory scheme further mandates that the Executive certify that it cannot obtain the foreign intelligence information it seeks through normal investigative techniques.[61] Moreover, these certifications must come from a high-level national security official.[62]

Taken together, these two provisions—which again play off of the foreign versus domestic distinction, and formally entail a national security intelligence versus criminal law enforcement dichotomy—serve to distinguish FISA investigation from normal criminal law enforcement. The FISC reviews these certifications under a deferential standard: if the target is a United States person the FISC reviews for clear error; otherwise, presumably, the FISC reviews only for facial compliance.[63] Finally, the FISC may also mandate that the Executive furnish additional information to assess any of the required determinations.[64]

Following the investigatory process itself, FISA provides downstream regulation of the Executive's use of the information it obtains.[65] Through statutory, administrative, and judicial "minimization procedures"[66] the FISA scheme limits the acquisition, retention, and dissemination of non-public information regarding United States persons.[67] Beyond a general requirement of minimization, the statute provides several details—procedures to prevent the disclosure of the identity of United States persons, an

60. USA PATRIOT Act § 218, 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2001).

61. § 1804(a)(7)(C) (requiring, additionally, the basis for the certification); § 1823(a)(7)(C) (same).

62. *Id.* §§ 1804(a)(7), 1823(a)(7).

63. 50 U.S.C. §§ 1805(a)(5), 1824(a)(5); *see also* H.R. REP. NO. 95-1283, at 80 (1978) (explaining that the "clearly erroneous standard of review is not, of course, comparable to a probable cause finding by the judge").

64. §§ 1805(d), 1824(c).

65. *Id.* §§ 1806, 1825 (2000 & Supp. II 2002).

66. *Id.* §§ 1801(h), 1821(4) (2000 & Supp. II 2002). Both § 1801(h) and § 1824(4) direct the Attorney General to promulgate more detailed procedures, which are classified. FBI OGC, *supra* note 54, at 16 (stating that "most minimization procedures are classified"). Moreover, each application for a FISC order contains a statement of proposed minimization procedures. *Id.* §§ 1804(a)(5), 1823(a)(5). Additionally, the FISC approves and supervises the minimization process. *Id.* §§ 1805(a)-(c); 1824(a)-(c).

67. §§ 1806(a), 1825. The standard minimization scheme allows the Executive to retain all information that could be foreign intelligence. *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 617-18 (FISA Ct. 2002), *overruled by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002). At acquisition, the Executive takes in all available information, conducting minimization later after processing (typically transcription and translation, followed by analysis). *Id.* If retained as foreign intelligence, the information then enters an indexed storage system for retrieval. *Id.* at 618.

exception to minimization allowing the retention and dissemination of information about criminal conduct unrelated to national security, and an exception to minimization of certain information obtained improperly but necessary to prevent death or bodily harm.[68]

While these requirements loosely serve to segregate FISA investigation from criminal investigation, other provisions of FISA, added by the Patriot Act, create notable tension by allowing consultation and information sharing between the intelligence investigators and criminal law enforcement.[69] For instance, FISA permits consultation with other law enforcement agencies to "coordinate efforts to investigate or protect against" sabotage, international terrorism, or espionage.[70] Although the statute merely authorizes consultation, the Attorney General's directives implementing FISA *mandate* consultation with the Criminal Division at Main Justice and relevant United States Attorneys' Offices.[71] This consultation "may include the exchange of advice and recommendations on all issues necessary" including the initiation, goals, strategies, methods, and operation of the investigation.[72]

A similar pattern pertains to information sharing. FISA allows the Executive to share information for lawful purposes and subject to minimization procedures.[73] The statute mandates only that if a government entity intends to use information derived from a FISA investigation in a trial or other proceeding (judicial or administrative), the government must give reasonable notice[74] to aggrieved persons.[75] The statutory scheme also includes one internal check—the Attorney General must approve in advance the use of FISA information in a criminal proceeding.[76]

Other than these notification and approval requirements, the

68. §§ 1801(h), 1821(4).

69. USA PATRIOT Act § 504, 50 U.S.C. § 1806 (Supp. I 2001).

70. §§ 1806(k), 1825(k). Both provisions expressly note that coordination does not preclude certification that a significant purpose of FISA surveillance is to obtain foreign intelligence information. *Id.* §§ 1806(k)(2), 1825(k)(2).

71. U.S. ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION 26-27 (2003), http://www.cdt.org/security/usapatriot/031031nsiguidelines.pdf [hereinafter AG GUIDELINES].

72. Memorandum from U.S. Att'y Gen. John Ashcroft to FBI Director, Asst. Att'y Gen., Criminal Division, Counsel for Intelligence Pol'y, U.S. Att'ys, at II.B (Mar. 6, 2002), http://www.fas.org/irp/agency/doj/fisa/ag030602.html (providing for the same level of consultation with United States Attorneys' Offices) [hereinafter AG Memo on Intelligence Sharing].

73. 50 U.S.C. §§ 1806(a), 1825(a).

74. *Id.* §§ 1806(c)-(d); 1825(d)-(e).

75. *See id.* §§ 1801(k), 1821(2) (2000) (defining "aggrieved person").

76. *Id.* §§ 1806(b), 1825(c).

statute provides no specifics on the scope of information sharing. The Attorney General, however, has issued detailed guidance on that process: "information should be shared as consistently and fully as possible"[77] to achieve the goal of protecting life or property, preventing crime, and obtaining information for the FBI to conduct further investigation.[78] More specifically, the FBI must share information with the Criminal Division, relevant United States Attorneys' Offices,[79] the Department of Homeland Security,[80] other federal authorities,[81] and state and local law enforcement.[82]

The statute constructs a unique framework for aggrieved persons[83] to challenge the FISA investigation. As a threshold matter, the challenge will occur only if the aggrieved person knows of the FISA investigation.[84] In general, FISA requires notice only when a government entity uses or discloses FISA information.[85] Upon notice, the aggrieved person may move to suppress the information.[86] If the Attorney General files an affidavit averring that "disclosure or an adversary hearing would harm the national security," the federal district court for the locale (regardless of the forum in which the principal dispute is occurring) will conduct an in camera and ex parte review.[87] The statute authorizes the court to make disclosures "under appropriate security procedures and protective orders" only as "is necessary to make an accurate determination of the legality of the" surveillance or physical search.[88]

2. Pen Register Investigations

FISA provides for investigation through the use of trap-and-trace devices and pen registers[89]—referred to together as "pen

77. AG GUIDELINES, *supra* note 71, at 24.

78. *Id.* at 25.

79. *Id.* at 25-26; *see also* AG Memo on Intelligence Sharing, *supra* note 72, § III (describing mandatory access of the United State Attorneys' Offices to information acquired by the FBI's international terrorism investigations).

80. AG GUIDELINES, *supra* note 71, at 27-29.

81. *Id.* at 29.

82. *Id.* at 29-30.

83. 50 U.S.C. §§ 1801(k), 1821(2) (2000).

84. *See id.* §§ 1806(c)-(f), 1825(b), (d), (f).

85. *See supra* note 74 and accompanying text; *see also* S. REP. NO. 95-701, at 11 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3980. *But cf.* § 1825(b) (providing for notice of a physical search if the Attorney General determines that national security no longer requires secrecy).

86. §§ 1806(e), 1825(f).

87. *Id.* §§ 1806(f), 1825(g).

88. *Id.* §§ 1806(f), 1825(g).

89. These technologies record incoming and outgoing phone numbers, but they also could record a number of other non-content attributes of electronic communications, such as routing and addressing information (like the history

registers investigation." The statute allows the Executive to obtain this form of surveillance authority with a FISC order[90] based on a certification that the surveillance likely will obtain foreign intelligence information not concerning a United States person or is "relevant" to an investigation to protect against international terrorism or espionage and that any "investigation of a United States person is not conducted solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution."[91] Before the Patriot Act, though, the statute more stringently required that the Executive show reason to believe that a foreign power or agent of a foreign power would use the target communication line in connection with espionage or international terrorism.[92] Notably, nothing in the statute mandates that the judicial officer considering the application weigh probable cause or the strength of the certification.[93] FISA applies the same rules governing dissemination, use, notice, and challenge for information derived from this form of surveillance as it does for electronic surveillance and physical search.[94]

3. Investigations Without a FISC Order

Several FISA provisions deviate from the standard model by allowing the Attorney General to conduct electronic surveillance or physical search without an order from the FISC. Generally, investigation under these provisions otherwise follows the normal FISA standards for probable cause or certification, and minimization. Investigation resting on the Attorney General's own authority, rather than independent judicial review, comes in two forms.

The first form of Attorney General-ordered investigation requires an "emergency situation" as a predicate.[95] The Attorney General must inform a FISC judge of the emergency order immediately and must submit promptly an application to the FISC

function on a Web browser). *See id.* § 1841(2) (2000) (adopting the definitions of these terms as given in 18 U.S.C. § 3127); Freiwald, *supra* note 16, at 61 (cautioning that "[t]he government has interpreted the pen register provisions to authorize devices that can record contents, so long as they are not configured to do so when they are used").

90. The Chief Justice may also appoint magistrate judges to exercise this authority on behalf of the FISC. § 1842(b)(2) (2000).

91. *Id.* § 1842(c)(2) (Supp. II 2002).

92. *See* USA PATRIOT Act § 214, 50 U.S.C. § 1842 (Supp. I 2001).

93. § 1842(d)(1) (2000) (providing for approval "if the judge finds that the application satisfies the requirements of this section").

94. *Id.* § 1845.

95. *Id.* §§ 1805(f), 1824(e), 1843 (2000 & Supp. II 2002).

for an order validating the emergency investigation.[96] Should the Executive not obtain validating approval from the FISC, the statutes generally prevent the Executive from using any information obtained.[97] The second form of Attorney General-ordered investigation derives its logic from the tight nexus with a foreign target. The Attorney General may conduct, without a FISC order, electronic surveillance of a foreign power and physical search of premises or property of a foreign power so long as that investigation does not pose a "substantial likelihood" of resulting in the investigation of a United States person.[98] Further, the Attorney General must certify these findings and submit them to the FISC immediately.[99]

4. Orders for Production of Tangible Things

Finally, FISA provides authority for the Executive to obtain a FISC order for the production of tangible things—including records, books, papers, documents, and other items—based on an application to the FISC[100] specifying that the Executive seeks them "for an investigation to obtain foreign intelligence information" that does not concern a United States person, "or to protect against international terrorism" or espionage.[101] The statute contains the common limit that the Executive cannot conduct an investigation of a United States person "solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution."[102] Prior to the enactment of the Patriot Act, however, the statute demanded that the Executive offer specific facts giving reason to believe that the subject of the investigation was a foreign power or agent of a foreign power.[103] Nothing in the statute mandates that the judicial officer considering the application weigh probable cause.[104] The order does

96. *Id.* § 1805(f) (providing a seventy-two-hour time limit); § 1824(e)(1)(A)(ii) (providing a seventy-two-hour time limit); § 1843(a) (providing a forty-eight-hour time limit).

97. The statutes, however, do contain an exception "if the information indicates a threat of death or serious bodily harm to any person." *Id.* §§ 1805(f), 1824(e)(4), 1843(c)(2). Further, for surveillance and search, if the Executive should not obtain validating approval, FISA provides for notice of the investigation to aggrieved United States persons, unless the Attorney General files and then renews an ex parte "showing of good cause." *Id.* §§ 1806(j), 1825(j).

98. *Id.* §§ 1802(a)(1)(B), 1822(a)(1)(A)(ii).

99. *Id.* §§ 1802(a)(3), 1822(a)(3).

100. *Id.* § 1861(b)(1)(B) (Supp. II 2002) (providing also for magistrate judges to receive such applications).

101. *Id.* § 1861(a)(1).

102. *Id.*

103. *See* USA PATRIOT Act § 215, 50 U.S.C. § 1861 (Supp. II 2002).

104. § 1861(c)(1).

not contain any reference to the purpose of the investigation, and its recipient, although shielded from liability, must not disclose, except to parties necessary for compliance, that the FBI "has sought or obtained tangible things" under FISA.[105] Of course these orders entail the gathering of information about a foreign intelligence target from third parties rather than surveilling that target directly through electronic or physical means.

B. National Security Letters

Similarly, the collection of several narrower categories of information about a target from third parties occurs under three statutes directed at transactional records. Specifically, the FBI is authorized to obtain "financial institution," "consumer reporting agency," and "electronic communication service provider" records through the use of a "national security letter"[106]—a document requiring no probable cause and no judicial approval. These three schemes all require that the recipient of the national security letter keep the request confidential.[107] The financial institution and communication service provider statutes allow the FBI to disseminate information to other federal agencies only if relevant to their authorized responsibilities;[108] while the consumer credit statute restricts the FBI to sharing the information with other federal agencies only for counterintelligence and counterterrorism purposes.[109] All the statutes mandate that the other agencies comply with FISA information sharing guidelines.[110]

Under the financial institution statutes, the FBI may obtain financial records.[111] The term "financial institutions" includes a host of businesses involved in commercial transactions, rather than just

105. *Id.* § 1861(c)(2)-(e).

106. "The term 'national security letter' does not appear in the statute, but the legislative history indicates that it was in common use by" the time the first of the authorizing statutes passed Congress. Woods, *supra* note 4, at 44 n.45. Congress and a number of experts have recently debated eliminating national security letters, and the tangibles provision, and enacting instead a process for FBI administrative subpoenas. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 493-94 (S.D.N.Y. 2004) (describing various legislative proposals); Michael J. Woods, *Patriot Act and Privacy: Both Need Congressional Safeguards*, WASH. TIMES, June 9, 2005, at A21 (arguing that administrative subpoenas would provide more judicial review); *see also* Berkower, *supra* note 9, at 2271-86 (analyzing the merits of the proposal to provide the FBI with administrative subpoena power).

107. 12 U.S.C. § 3414(a)(5)(D) (2000); 15 U.S.C. § 1681u(d) (2000); 18 U.S.C. § 2709(c) (2000).

108. 12 U.S.C. § 3414(a)(5)(B); 18 U.S.C. § 2709(d).

109. 15 U.S.C. § 1681u(f).

110. 12 U.S.C. § 3414(a)(5)(B); 15 U.S.C. § 1681u(f); 18 U.S.C. § 2709(d).

111. 12 U.S.C. § 3414(a)(5)(A).

banks.[112] Under the statutes governing consumer credit reporting agencies, the FBI may obtain the identity of not only all financial institutions where a customer has or had an account, but also records concerning that customer's present and past addresses and employers.[113] From electronic communication service providers, the FBI may obtain subscriber information and billing records.[114] In all cases, the FBI must submit a written certification from an official no lower than an FBI Special Agent in Charge of a field office or a Deputy Assistant Director, as designated by the FBI Director.[115] That official need only certify that the information requested is for the conduct of an investigation to protect against international terrorism or espionage, and not conducted solely based on activities protected by the First Amendment.[116] Before the Patriot Act, the relevant statutes mandated that the Executive show specific facts giving reason to believe that the target was a foreign power or an agent of a foreign power.[117]

C. Sharing of Criminal Investigation Information

Several statutory provisions aid foreign intelligence investigators, even if the underlying investigation falls beyond their control. For instance, the criminal electronic surveillance statute provides for sharing of national security information with foreign intelligence investigators.[118] Because of the Patriot Act, the grand jury rules contain an exception to grand jury secrecy requirements for the sharing of such information.[119] The disclosure of grand jury information occurs without the permission or supervision of the court, which would otherwise be the norm, and subject only to the requirement that the government report within a reasonable time to

112. 31 U.S.C. § 5312(a)(2) (including, within the definition of "financial institution," banks, thrifts, credit unions, investment brokers and dealers, insurance companies, travel agencies, telegraph and wire transfer companies, business engaged in vehicle sales, the Postal Service, casinos, and persons involved in real estate closings).

113. 15 U.S.C. § 1681u(a)-(b) (Supp. II 2002).

114. 18 U.S.C. § 2709(b) (Supp. II 2002).

115. 12 U.S.C. § 3414(a)(5)(A) (Supp. II 2002); 15 U.S.C. § 1681u(a)-(b) (Supp. II 2002); 18 U.S.C. § 2709(b) (Supp. II 2002).

116. 12 U.S.C. § 3414(a)(5)(A) (Supp. II 2002); 15 U.S.C. § 1681u(a)-(b) (Supp. II 2002); 18 U.S.C. § 2709(b) (Supp. II 2002).

117. *See* 12 U.S.C. § 3414(a)(5)(A) (2000) (amended 2001); 15 U.S.C. § 1681u (a)(2)(A)-(B), (b)(2) (2000) (amended 2001); 18 U.S.C. § 2709(b)(1)(B), (2)(B)(ii) (2000) (amended 2001).

118. 18 U.S.C. § 2517(7) (Supp. II 2002).

119. FED. R. CRIM. P. 6(e)(3)(D) (as amended by USA PATRIOT Act § 203). The precise ordering of Rule 6(e)(3) was changed by Supreme Court amendment after the Patriot Act was passed. *See* 535 U.S. 1186-87 (2002).

the court.[120] Moreover, post office regulations authorize mail covers for national security investigation purposes.[121] Finally, a general provision in the national security statutes authorizes criminal investigators to share information with the intelligence community.[122]

IV. NATIONAL SECURITY INVESTIGATION VS. CRIMINAL PROCEDURE

National security investigation takes on particular importance, not just because its targets pose particular concern, but because its methods and standards differ from normal criminal procedure.[123] Under FISA, the Executive can do things it simply cannot accomplish under the criminal law. In general, criminal law contains more stringent standards for initiating an investigation and greater restrictions on the length and scope of an investigation. In a few regards, though, FISA contains the more rigorous procedures.

A. Electronic Surveillance

Under criminal law, electronic surveillance of communications containing content is governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[124] Probable cause under Title III requires substantial evidence to believe that the target has, is, or is about to commit a listed predicate offense.[125] In contrast, for FISA, electronic surveillance requires probable cause that the target is a foreign power or agent of a foreign power.[126] Criminal law surveillance focuses directly on the nexus between the target and crime; whereas FISA demands a foreign link with the target, only more distally probing for criminal conduct.

For a counterterrorism investigation of a United States person, however, both FISA and the criminal law require similar evidence of a connection to crime. For example, in the case of a person suspected of providing logistical communications support to a foreign terrorist group, the Executive could criminally investigate with probable cause to believe that the target is violating 18 U.S.C.

120. FED. R. CRIM. P. 6(e)(3)(D)(ii). For a full explanation of the national security exception to grand jury secrecy, see generally Collins, *supra* note 4.

121. *See* 39 C.F.R. § 233.3(1) (2005).

122. 50 U.S.C. § 403-5d(1) (Supp. II 2002).

123. *See In re* Sealed Case, 310 F.3d 717, 737-42 (FISA Ct. Rev. 2002).

124. Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-22 (2000 & Supp. II 2002)) (referred to as either Title III or the Wiretap Act).

125. 18 U.S.C. § 2518(3)(a) (2000).

126. 50 U.S.C. § 1805(a)(3)(A) (2000).

§ 2339A, the material support to terrorists statute.[127] Under FISA, the parallel investigation would require probable cause to believe that the target knowingly engages in international terrorism or preparatory acts as a principal, accomplice, or conspirator.[128] In this example, although the mechanics of probable cause work differently in Title III and FISA, the quantum of proof might actually amount to the same kind and level of evidence, and certainly entails a parallel connection to criminal activity.[129]

In other contexts, the difference between Title III and FISA comes into bold relief. For a counterintelligence investigation of a United States person, the Executive needs to establish only that the target knowingly engages in espionage that *may involve* a violation of criminal statutes.[130] The level of probable cause under FISA diminishes even further when the Executive targets a non-United States person engaged in espionage or international terrorism—in these instances, the statute begins to move away from requiring proof of mental state and toward requiring proof only of conduct.[131] For surveillance of a foreign power, the Executive need offer evidence only to show that the target is a foreign entity—the statute demands no proof of conduct or purpose.[132]

The two schemes also differ in the probable cause approach to the precision of surveillance and the relationship of the target or the offense to the locale or device surveilled—the particularity requirements. Under Title III, the Executive needs probable cause that the surveillance will intercept particular communications regarding the offense and that the target possesses the device surveilled or uses it in connection with the offense.[133] Under FISA,

127. *See* 18 U.S.C. § 2516(q) (Supp. II 2002) (listing material support among the predicate offenses for surveillance); *see also supra* note 54 (noting the material support offense).

128. 50 U.S.C. § 1801(b)(2)(C), (E) (2000).

129. *See In re* Sealed Case, 310 F.3d 717, 738 (FISA Ct. Rev. 2002) ("[W]here a U.S. person is involved, an 'agent of a foreign power' is defined in terms of criminal activity.").

130. § 1801(b)(2)(A); *see also Sealed Case*, 310 F.3d at 738 ("Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases.").

131. Specifically, the Executive must establish that the target engages in the terrorism or preparatory conduct or may engage (as principal, accomplice, or conspirator) in espionage. § 1801(b)(1)(B).

132. *See id.* § 1801(a); *see also Sealed Case*, 310 F.3d at 738 n.21 (noting that "[t]he term 'foreign power' . . . is not defined solely in terms of criminal activity").

133. 18 U.S.C. § 2518(3)(b), (d). If the Executive cannot identify a particular person, it must demonstrate a nexus between the device and the crime. *Sealed Case*, 310 F.3d at 740. Thus, both schemes allow surveillance of "unknown" targets sufficiently described. *Compare* 50 U.S.C. § 1805(c)(1) *with* INGA L. PARSONS, FOURTH AMENDMENT: PRACTICE AND PROCEDURE 173 (2005) ("The

surveillance requires probable cause to believe that the target uses the device[134] and a certification—reviewed for only clear error—that the Executive seeks certain national security information.[135] Where Title III demands a nexus between the communication and the offense, and a nexus between the device and the target, FISA requires only a nexus between the device and the foreign threat—a nexus that may demonstrate a link to a criminal offense but does not in all cases require such an association. In addition, FISA mandates a connection between the target and the locus of surveillance.[136] The FISA standard allows surveillance on a much broader scope because it does not demand probable cause regarding particular communications, instead allowing the monitoring of all communications tied to the target. The FISA minimization requirements, however, serve to limit the information the Executive may acquire, retain, and disseminate.

Under Title III, surveillance authorization remains valid for thirty days, while a FISA order lasts for ninety days (or more for surveillance of non-United States persons and foreign powers).[137] Under FISA, unlike Title III, the court monitors the surveillance during this time because the FISC retains oversight of minimization.[138] Further, minimization under Title III typically occurs during acquisition, whereas the norm under FISA emphasizes later stages in the process.[139]

Moreover, Title III favors eventual notice to the target, requiring notification within ninety days following termination of surveillance, but allowing postponement based on an ex parte showing of good cause.[140] In dramatic contrast, FISA provides for notice only upon use by the government in public proceedings.[141] The notice provisions dramatically affect the opportunities for challenging the Executive's conduct. Under Title III, a target who

government can list 'possible interceptees' and others 'unknown.'").

134. § 1805(a)(3)(B).

135. *Id.* § 1804(a)(7); *see* H.R. REP NO. 95-1283, 80-81 (1978) (detailing the standard of review by the FISC).

136. *See Sealed Case*, 310 F.3d at 740 (explaining that "FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications"). For a description of the debate that has erupted over the extent to which the FISA roving surveillance procedures depart from the so-called ascertainment and identification requirements of Title III, see DeRosa, *supra* note 56, at 17-18.

137. *Compare* 18 U.S.C. § 2518(5) *with* 50 U.S.C. § 1805(e).

138. 50 U.S.C. § 1805(e)(3); *Sealed Case*, 310 F.3d at 740.

139. *Sealed Case*, 310 F.3d at 740 (stating that "in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications").

140. 18 U.S.C. § 2518(8)(d).

141. 50 U.S.C. § 1806(c)-(d).

believes the government has violated the Fourth Amendment could file a civil claim—regardless of whether the government pursues prosecution—and, if charged, seek to suppress the evidence. Under FISA, an aggrieved person can obtain relief only when the government uses the information against that person. Further, if an individual does challenge the government regarding the legality of the investigation, under Title III the Executive must divulge the surveillance application, whereas under FISA the application remains secret—subject to potential disclosure by the court hearing the matter ex parte and in camera.[142]

Significant differences also appear in the level of the official who must sign off on the application for surveillance authority; in this regard, FISA contains stricter standards than Title III. For criminal surveillance, at a minimum, a Deputy Assistant Attorney General must approve the application; while under FISA, only the Attorney General and the Deputy Attorney General can approve the application.[143] Additionally, FISA requires certification of a significant foreign intelligence purpose and the inadequacy of normal investigative methods (the so-called "necessity" requirement[144]) by a senior official presidentially designated as involved in national security matters.[145] Although Title III also contains a necessity provision,[146] it does not mandate certification from a senior official.[147]

Some similarities between surveillance under FISA and Title III are worth noting. Both schemes posit judicial preclearance as the norm.[148] Both bodies of law contain emergency exceptions allowing surveillance on the Attorney General's order followed by judicial validation.[149] The two schemes contain reciprocal information-sharing regimes.[150]

142. *Compare* 18 U.S.C. § 2518(9) *with* 50 U.S.C. § 1806(f).

143. *Compare* 18 U.S.C. § 2516(1) *with* 50 U.S.C. § 1801(g).

144. *See Sealed Case*, 310 F.3d at 740.

145. 50 U.S.C. § 1804(a)(7).

146. 18 U.S.C. § 2518(1)(c), (3)(c).

147. *See Sealed Case*, 310 F.3d at 740 (explaining that, "[a]lthough the court's clearly erroneous review under FISA is more limited than under Title III, this greater deference must be viewed in light of FISA's additional requirement that the certification of necessity come from an upper level Executive Branch official").

148. *Compare* 18 U.S.C. § 2518 *with* 50 U.S.C. § 1805; *see also Sealed Case*, 310 F.3d at 738 (explaining that both schemes satisfy the "neutral and detached" magistrate requirement).

149. *Compare* 18 U.S.C. § 2518(7) *with* 50 U.S.C. § 1805(f). FISA also contains a provision allowing surveillance of a foreign power without a FISC order. 50 U.S.C. § 1802.

150. *Compare* 18 U.S.C. § 2517(6) (Supp. I 2001 & Supp. II 2002) *with* 50 U.S.C. § 1806(a) (2000).

Finally, with the exception of the length of time the order remains valid,[151] both criminal law and FISA treat pen register investigation alike. Both schemes require a certification that the surveillance is "relevant" to an ongoing investigation,[152] that the order remain secret,[153] and that any party assisting the Executive maintain that secrecy.[154]

B. Physical Search

A comparison of criminal law and FISA searches is more difficult. Whereas FISA's provisions for physical search parallel those for electronic surveillance, which neatly array against Title III, physical searches under the criminal law are governed by Federal Rule of Criminal Procedure 41 and case law. Nevertheless, a few points are worth consideration.

The standard formula for a search warrant under criminal law is that "two conclusions . . . must be supported by substantial evidence: that the items sought are in fact seizable by virtue of being connected with criminal activity, and that the items will be found in the place to be searched."[155] Under FISA, for a physical search, the Executive needs substantial evidence that the target is a foreign power or agent of a foreign power and that the items belong to the target.[156] Criminal law seeks a nexus between criminal activity and the items, and a nexus between the items and the locus of the search. In contrast, as noted previously, FISA requires a nexus between the items sought and a foreign threat—a nexus that may demonstrate a link to a criminal offense but does not in all cases require such an association.[157] FISA probable cause for a search focuses on the target, while criminal-search probable cause for a search focuses on the items. As with electronic surveillance, this difference results in FISA searches of far greater scope than criminal searches: FISA allows the Executive to search all that belongs to the target, while the criminal law restricts the search to particular items and places.

Under FISA, the Executive also has more time to conduct that search—a FISA physical-search order remains valid for ninety days

151. *Compare* 18 U.S.C. § 3123(c)(1) (2000) (order valid for sixty days) *with* 50 U.S.C. § 1842(e) (2000) (order valid for ninety days).

152. *Compare* 18 U.S.C. § 3123(a) (2000 & Supp. I 2001 & Supp. II 2002) *with* 50 U.S.C. § 1842(c)(2) (2000 & Supp. II 2002).

153. *Compare* 18 U.S.C. § 3123(d)(1) *with* 50 U.S.C. § 1845(c)-(d).

154. *Compare* 18 U.S.C. § 3123(d)(2) *with* 50 U.S.C. § 1842(d)(2)(B).

155. 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 3.3(a), at 84 (1999) (internal citation omitted).

156. 50 U.S.C. § 1824(a)(3).

157. *See supra* note 136 and accompanying text.

(or longer for searches of non-United States persons and foreign powers).[158] In contrast, a criminal search warrant lasts for ten days, and, absent good cause found at time of application, must be executed during daylight.[159]

As with electronic surveillance, criminal-search law favors notice of the search, although with physical searches the norm is contemporaneous notice. Indeed, federal law embodies a "knock and announce" requirement that the officers state their authority and purpose before using physical force to gain entry.[160] Further, the officer executing the warrant must present a copy of the warrant and leave a receipt for any seized property.[161] Notably, following the enactment of the Patriot Act, criminal law allows for a surreptitious entry warrant—a so-called "black bag job" or "sneak and peek" warrant—for extraordinary situations.[162] In such cases, the warrant must provide for notice within a reasonable time, which the court may extend for good cause.[163] In contrast, for physical searches under FISA, as with electronic surveillance, secrecy is the norm, with aggrieved persons receiving notice only if the Executive makes use of information obtained in the search.[164]

C. Tools for Gathering Information from Third Parties

For the most part, the national security tools for gathering information from third parties—orders for the production of tangible things and national security letters—bear a significant resemblance with the closest criminal law parallel, the grand jury subpoena. Under the national security authorities, the Executive may employ these tools as part of an investigation against international terrorism or espionage.[165] In contrast, a grand jury may subpoena any information the grand jurors desire to conduct their investigation.[166]

158. 50 U.S.C. § 1824(d)(1) (Supp. II 2002).

159. FED. R. CRIM. P. 41(e)(2)(A)-(B); *see also* 21 U.S.C. § 879 (2000) (authorizing routine execution of search warrants for narcotics at night).

160. *See* 18 U.S.C. § 3109 (2000); *see also* Richards v. Wisconsin, 520 U.S. 385, 394 (1997) (excusing the knock-and-announce requirement for exigent circumstances).

161. FED. R. CRIM. P. 41(f)(3).

162. 18 U.S.C. §§ 3103a, 2705b (2000 & Supp. II 2002).

163. *Id.* § 3103a(b)(3) (Supp. II 2002).

164. *See* 50 U.S.C. § 1822(a)(4)(A)(i) (2000) (mandating that any landlord or custodian directed to assist in the search "protect its secrecy"); § 1824(c)(2)(B) (same); § 1825(b) (providing for notice if the Attorney General determines there is no longer a need for secrecy).

165. *See* 12 U.S.C. § 3414(a)(5)(A) (Supp. II 2002); 15 U.S.C. § 1681u(a), (b) (Supp. II 2002); 18 U.S.C. § 2709(b) (Supp. II 2002); 50 U.S.C. § 1861(a) (2000).

166. LAFAVE ET AL., *supra* note 155, § 8.3(b), at 25; *see also id.* §§ 8.7(c), 8.8(a) (stating that a grand jury subpoena is invalid if it is overbroad, too

Some differences distinguish the two schemes, leaving national security investigation more powerful in some ways and the grand jury process superior in others. While FISA orders and national security letters must remain secret,[167] grand jury secrecy binds the Executive and grand jurors, but not witnesses.[168] Moreover, the Executive firmly controls a national security investigation, while the Executive may not use the grand jury merely as a tool of law enforcement investigation.[169] Under the national security authorities, the Executive may share information widely,[170] while, for a grand jury, the court supervises the sharing of information.[171] Finally, the court enforces a grand jury subpoena, while no explicit enforcement mechanism exists for national security letters.[172]

V. THE EVOLUTION OF NATIONAL SECURITY JURISPRUDENCE

This Article develops a method of constitutional regulation for national security investigation sufficiently robust to function even if the courts approve the entire apparatus. Accordingly, the Article must first explore the constitutional framework under which courts have analyzed national security investigation. Most generally, courts have upheld FISA because they have recognized a national security exception to the normal Fourth Amendment standards. Without this exception the differences between the two kinds of investigation would be fatal to FISA. Further, courts have attempted to police the boundaries of this exception to prevent the Executive from avoiding the traditional strictures of the Fourth Amendment. This Part explores the development of that jurisprudence and then proceeds to an analysis of its deficiencies with the hope that such a critique will feed the formulation of an

sweeping, or if it has no reasonable possibility of producing relevant evidence); Sara Sun Beale & James E. Felman, *The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the USA PATRIOT Act's Changes to Grand Jury Secrecy*, 25 HARV. J.L. & PUB. POL'Y 699, 700-02 (2002) (explaining the powers of the grand jury). Under some criminal statutes, however, the Executive may issue an administrative subpoena. *See*, *e.g.*, 21 U.S.C. § 876(a) (2000) (narcotics); 18 U.S.C. § 3486(a)(1)(A)(i)(I) (2000) (health care related crimes).

167. 12 U.S.C. § 3414(a)(5)(D); 15 U.S.C. § 1681u(d); 18 U.S.C. § 2709(c); 50 U.S.C. § 1861(d)-(e) (Supp. II 2002).

168. FED. R. CRIM. P. 6(e).

169. LAFAVE ET AL., *supra* note 155, § 8.8(f), at 172-73. Prosecutors also may not employ the subpoena power of Federal Rule of Criminal Procedure 17 as an investigatory tool. *See* United States v. Nixon, 418 U.S. 683, 698 (1974).

170. *See supra* notes 73-82, 108-110 and accompanying text.

171. FED. R. CRIM. P. 6(e)(3); *see also* United States v. Sells Eng'g Inc., 463 U.S. 418, 427, 443 (1983) (permitting disclosure to other government personnel under court approval with "a strong showing of particularized need").

172. Woods, *supra* note 4, at 61.

effective method of regulation for national security investigation.

A. The Origin of the Primary Purpose Test

Although the Executive started to engage in warrantless intelligence monitoring in the middle of the nineteenth century,[173] the jurisprudence of national security investigation did not begin until the early 1970s with *United States v. United States District Court* ("*Keith*").[174] In *Keith*, the Court rejected an exception to the Fourth Amendment's warrant requirement for national security investigation of domestic threats,[175] while leaving undecided the same issue with regard to foreign threats.[176] That holding belies the case's importance, which instead rests in the Court's approach to the problem.

In deciding whether to recognize a national security exception, the *Keith* Court explicitly balanced the Executive's interest in protecting the country against "individual privacy and free expression."[177] Specifically, the Court examined whether the need for judicial preclearance to protect constitutional values would "unduly frustrate" the Executive's efforts to provide security.[178] The Court emphasized the importance of carefully weighing[179] whether the investigation was "necessary,"[180] "require[d],"[181] and "directed primarily to the collecting and maintaining of intelligence . . . and . . . not an attempt to gather evidence for specific criminal prosecutions."[182] Further, in a passage arguably constituting obiter dicta, *Keith* explained that the probable cause or reasonableness prong of Fourth Amendment analysis would modulate depending on the context—especially the legitimate need of the Executive for obtaining intelligence information.[183]

173. William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment,* 35 CATH. U. L. REV. 97, 103 (1985). Even during the years before *Katz v. United States*, 389 U.S. 347 (1967), when the Supreme Court held that electronic surveillance fell beyond the ambit of the Fourth Amendment, the Executive did not treat the matter as unregulated and consign the question to lower-level decisionmakers, but instead required that the President or Attorney General give personal approval. *See* United States v. Ehrlichman, 546 F.2d 910, 937 (D.C. Cir. 1976). Indeed, this requirement of personal approval from the top persisted and migrated explicitly into FISA. *See supra* note 44.

174. 407 U.S. 297 (1972).

175. *Id.* at 321.

176. *Id.* at 308, 309 n.8, 322 n.20.

177. *Id.* at 315.

178. *Id.*

179. *Id.* at 319.

180. *Id.* at 309.

181. *Id.* at 315.

182. *Id.* at 318-19.

183. *Id.* at 322-23 (stating that a "[d]ifferent standard[] [of probable cause]

Several lower courts took up the unanswered question and recognized a foreign intelligence exception to the Fourth Amendment.[184] Many of these decisions treated as crucial, if not dispositive, the *Keith* Court's recurrent weighing of the Executive's claim of necessity and converted that concern into what became known as the "primary purpose test"—the Executive could conduct a warrantless investigation only when its primary purpose focused on the collection of foreign intelligence information rather than information directed toward criminal prosecution.[185] The courts diverged on the exact analytical location of the primary purpose requirement; some used the test as a gatekeeper to guard the exception to the warrant requirement, and others placed it under the probable cause, or reasonableness, prong[186] of the Fourth Amendment.[187]

These opinions weave pragmatic and structural rationales. The structural argument entails separation of powers considerations regarding the Executive's responsibility for foreign affairs and national security.[188] Meanwhile, the pragmatic analysis revolves

may be compatible with the Fourth Amendment if [it is] . . . reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens").

184. United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Clay, 430 F.2d 165, 172 (5th Cir. 1970), *rev'd*, 403 U.S. 698 (1971). *But cf.* Zweibon v. Mitchell, 516 F.2d 594, 633-51 (D.C. Cir. 1976) (en banc) (plurality opinion) (rejecting a national security exception for surveillance of domestic threats and stating in dicta that no foreign threat exception existed either).

185. *Truong*, 629 F.2d at 915; *Butenko*, 494 F.2d at 606; *Brown*, 484 F.2d at 426; *see also* United States v. Bin Laden, 126 F. Supp. 2d 264, 277-79 (S.D.N.Y. 2000) (applying the primary purpose requirement for an extraterritorial search). *But see Clay*, 430 F.2d at 172 (predating *Keith* and approving warrantless foreign intelligence investigation without restriction). The judge-made requirements of primary purpose and necessity both transformed into statutory language with the advent of FISA. *See supra* notes 59-60 and accompanying text (detailing the statutory purpose requirement); *see also supra* notes 61-62 and accompanying text (detailing the necessity and high level certification requirements).

186. Camara v. Municipal Ct., 387 U.S. 523, 534-35 (1967) (equating the probable cause and reasonableness inquiries for warrant clause cases).

187. *Compare Truong*, 629 F.2d at 915 (employing the primary purpose test to define the exception to the warrant requirement) *and Brown*, 484 F.2d at 426 (same) *with Butenko*, 494 F.2d at 606 (employing the primary purpose test as part of the probable cause analysis).

188. *Truong*, 629 F.2d at 914; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d at 426; *Bin Laden*, 126 F. Supp. 2d at 272-73. Again, the foreign versus domestic distinction became part of the FISA structure itself. *See supra* notes 47-48 and accompanying text (detailing the foreign power and agent of a foreign power definitions); *see also supra* notes 59-62 (detailing certifications necessary to ensure a foreign intelligence purpose discrete from, and unachievable through,

around the perceived necessity of investigation into exigent national security threats and the concomitant requirements of efficiency and secrecy to meet complex challenges that demand the expertise only the Executive possesses.[189] Indeed, the preventative nature of national security investigation, its focus on amorphous and incipient threats to the entire society, and its long-term and secret nature have led many commentators to conclude that it would not fit within the traditional criminal law construct.[190]

B. The Primary Purpose Test Applied to FISA

Following the enactment of FISA in 1978, courts continued to recognize the national security exception to the warrant requirement and found that FISA satisfied the Fourth Amendment's reasonableness requirement.[191] Most courts continued to apply the general reasoning adopted in the pre-FISA opinions described above.[192] Curiously, few courts elaborated upon the analysis, despite the dramatic shift in the constitutional structural posture of the matter.[193] Before FISA, the Executive acted alone, based solely on the independent authority of that branch; after FISA, however, the Executive acted with whatever additional authority Congress could confer and subject to all of the regulations of FISA, including judicial preclearance based on a form of probable cause.[194] Nevertheless, and despite FISA's numerous detailed restrictions on Executive authority, many courts continued to apply the primary purpose requirement developed to regulate pure Executive

domestic law enforcement).

189. *Truong*, 629 F.2d at 914; *Butenko*, 494 F.2d at 605; *Clay*, 430 F.2d at 171.

190. RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11, at 174 (2005); Banks & Bowman, *supra* note 13, at 4-9; Banks, *supra* note 4, at 1152.

191. United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991); United States v. Cavanagh, 807 F.2d 787, 790-91 (9th Cir. 1987); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Duggan, 743 F.2d 59, 73-74 (2d Cir. 1984); *see also* United States v. Nicholson, 955 F. Supp. 588, 590 n.3 (E.D. Va. 1997) (collecting cases).

192. *In re* Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

193. For instance, only in *Cavanagh* did the court conclude that FISA comported with the Fourth Amendment's particularity requirements. 807 F.2d at 791.

194. *See Sealed Case*, 310 F.3d at 742 (explaining that FISA cannot encroach on presidential authority but could amplify presidential power); *Duggan*, 743 F.2d at 73 (finding executive and legislative agreement on national security questions highly persuasive); United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982) (finding FISA constitutional, in part, because of oversight and participation by all three branches).

searches.[195] Notably these courts found the primary purpose test embodied in FISA itself[196]—perhaps not surprising considering FISA's requirement until 2001 of a certification that the collection of foreign intelligence information constituted "the purpose" of the investigation.[197]

Nonetheless, a few courts reflected upon the changed nature of national security surveillance after FISA and significantly adjusted their analytical frameworks. For example, in *United States v. Megahey*,[198] the district court detailed the various requirements for a FISA order and explained that compliance with these standards brought FISA within the exception to the warrant requirement, finding the "primary purpose" test practically superfluous because "this requirement is clearly implicit in the FISA standards."[199] In *United States v. Sarkissian*,[200] the Ninth Circuit refused to apply the primary purpose test, explaining that FISA expressly contemplates prosecution and sufficiently distinguishes foreign intelligence investigation from ordinary criminal procedure.[201]

More dramatically, a handful of courts concluded that FISA satisfied the warrant requirement,[202] seemingly obviating the need for a national security exception. For instance, the *Megahey* court offered, as a preferable but alternate analysis, that the FISA order "is a warrant within the meaning of the [F]ourth [A]mendment, since it provides for the interposition of independent judicial magistrates between the executive and the subject of the surveillance."[203] More pointedly, in *United States v. Falvey*,[204] the district court explained that FISA constituted a congressionally imposed warrant requirement.[205]

These two cases cannot mean what they purport to say. If a

195. *Johnson*, 952 F.2d at 573; *Badia*, 827 F.2d at 1464; *Pelton*, 835 F.2d at 1075; *Duggan*, 743 F.2d at 77. *But see* United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988) (refusing to apply the primary purpose test).

196. *Johnson*, 952 F.2d at 573; *Cavanagh*, 807 F.2d at 790-91; *Pelton*, 835 F.2d at 1075; *Badia*, 827 F.2d at 1464; *Duggan*, 743 F.2d at 77.

197. 50 U.S.C. § 1804(a)(7)(B) (2000) (amended by USA PATRIOT Act § 218).

198. 553 F. Supp. 1180 (E.D.N.Y. 1982), *aff'd*, 743 F.2d 59 (2d Cir. 1984).

199. *Id.* at 1188-89.

200. 841 F.2d 959 (9th Cir. 1988).

201. *Id.* at 964-65; *see also* United States v. Falvey, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982) (finding that evidence of criminal activity discovered during surveillance was admissible because the purpose of the surveillance was to gather foreign intelligence information).

202. Certainly, the FISA provisions that entirely excuse preclearance for surveillance and searches of foreign powers would not qualify for this line of analysis. *See* 50 U.S.C. §§ 1802, 1822 (2000).

203. 553 F. Supp. at 1190.

204. 540 F. Supp. 1306 (E.D.N.Y. 1982).

205. *Id.* at 1314.

FISA order literally constituted a warrant and satisfied traditional probable cause, Congress could add normal criminal offenses to its ambit. These cases must mean that FISA constitutes a parallel and constitutionally adequate substitute for the traditional warrant and probable cause formula, but only in the defined category of national security investigation. The two courts might as well have explicitly recognized a national security exception to the warrant requirement and, then, concluded that FISA falls into that exception and meets the Fourth Amendment's reasonableness mandate. Perhaps for these reasons, the Ninth Circuit, in *United States v. Cavanagh*[206] (per then-Judge Anthony Kennedy) and the Fourth Circuit in *United States v. Pelton*,[207] both concluded that FISA satisfied the requirements of the Fourth Amendment without ever explicitly stating that a FISA order constituted a warrant.[208]

Regardless of whether a FISA order constitutes a warrant, many of the courts considering the constitutionality of FISA found that the order satisfied the probable cause, or reasonableness, prong of Fourth Amendment analysis[209] and, in that regard, found the resemblance between a FISA order and a traditional warrant quite important.[210] In each of these cases, the courts followed *Keith*'s dicta regarding a flexible approach to probable cause, or reasonableness, in national security matters.[211] This approach builds on *Camara v. Municipal Court*,[212] an administrative search case in which the Supreme Court explained that in specialized areas probable cause does not have a talismanic, fixed, or static meaning.[213] Instead,

206. 807 F.2d 787 (9th Cir. 1987).

207. 835 F.2d 1067 (4th Cir. 1987).

208. *Cavanagh*, 807 F.2d at 790; *Pelton*, 835 F.2d at 1075.

209. *Cavanagh*, 807 F.2d at 790-91; *Duggan*, 743 F.2d at 73-74; *Falvey*, 540 F. Supp. at 1313; *Megahey*, 553 F. Supp. at 1190. Taken together, these cases have considered the three main levels of probable cause possible under FISA: foreign power, non-United States person acting as an agent for a foreign power, and United States person acting as an agent for a foreign power. This hierarchy entails ascending degrees of probable cause. *See supra* note 47 and accompanying text. Importantly, none of the courts analyzing the issue focused on these different levels of probable cause as significant to the analysis. It would seem, however, that the level of probable cause relates directly to the degree to which the Executive acts within its inherent power over foreign affairs and command of the military against foreign threats. *See supra* note 188 and accompanying text.

210. *See In re* Sealed Case, 310 F.3d 717, 741-42 (FISA Ct. Rev. 2002).

211. *See supra* note 183. As commentators have noted, this translation of probable cause into a sliding-scale analysis, akin to reasonableness, has received full consideration and a firm rejection by the Court in the traditional probable cause context. *See* The Honorable Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 809-11 (2004).

212. 387 U.S. 523 (1967).

213. *See id.* at 534-35.

probable cause takes on the same dimensions as reasonableness and, therefore, depends on the governmental interest at stake.[214] Under this theory, courts have concluded that FISA strikes a reasonable balance between the Executive's vital interest in national security and the individual concern for "freedom from improper government intrusion" because it mandates "prior judicial scrutiny" by a "detached judicial officer," and because it mandates detailed certifications regarding the target and the necessity for investigation.[215] Although some have argued that this balancing should come out differently for surveillance than for physical search,[216] the Supreme Court treats the two symmetrically.[217]

Nevertheless, the primary purpose test became embedded in the jurisprudence of national security investigation. As the FISC explained, the vital animating concern was to "preserve both the appearance and the fact that FISA surveillances and searches were not being used sub rosa for criminal investigations."[218] Similarly, the Third Circuit expressed the fear that the Executive might use the "cloak of foreign intelligence information gathering to engage in indiscriminate surveillance."[219] Or, as the District of Columbia Circuit phrased it, "when the foreign agent exception is invoked to justify warrantless surveillance, courts must be alert to the possible pretextuality of the claim."[220] Underlying this concern is the belief

214. *Id.* at 535, 539.

215. United States v. Cavanagh, 807 F.2d 787, 789-90 (9th Cir. 1987); *accord* United States v. Duggan, 743 F.2d 59, 73-74 (2d Cir. 1984); United States v. Falvey, 540 F. Supp. 1306, 1312-13 (E.D.N.Y. 1982); United States v. Megahey, 553 F. Supp. 1180, 1191-92 (E.D.N.Y. 1982), *aff'd*, 729 F.2d 1444 (2d Cir. 1983); *see also* Rosen, *supra* note 19, at 613 (explaining that FISA "only suspended the ordinary Fourth Amendment requirements of particularity and individualized suspicions after an individual had been identified in advance as unusually suspicious"); Hardin, Note, *supra* note 4, at 292-93 (characterizing FISA's "intricate balance" as achieving a "constitutional and political equilibrium" but sacrificing traditional probable cause).

216. *See* Banks & Bowman, *supra* note 13, at 67.

217. *See* Dalia v. United States, 441 U.S. 238, 248 (1979) (authorizing "covert entry performed for the purpose of installing otherwise legal electronic bugging equipment"); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the reach of the Fourth Amendment "cannot turn upon the presence or absence of physical intrusion"); *see also* 50 U.S.C. § 1805(c)(1)(D) (2000) (including, in a FISA order for electronic surveillance, authorization for physical entry to effect the surveillance); United States v. Nicholson, 955 F. Supp. 588, 591 (E.D. Va. 1997) (rejecting the argument that FISA's search provisions suffered greater constitutional infirmity than the statute's surveillance sections).

218. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002), *rev'd on other grounds, In re* Sealed Case, 310 F.2d 717 (FISA Ct. Rev. 2002).

219. United States v. Butenko, 494 F.2d 539, 605 (3d Cir. 1974).

220. Chagnon v. Bell, 642 F.2d 1248, 1260 (D.C. Cir. 1980).

that FISA is "less stringent" than its criminal law counterparts[221] and that the Executive will attempt an "end-run" around more onerous criminal law standards.[222]

By helping to demarcate the category of investigation legitimately classified as national security investigation, the primary purpose test shielded the exception to the warrant requirement and its attendant special rules for warrants, probable cause, and reasonableness. The test amounted to a judicially created regulatory device designed to prevent the national security exception from swallowing more of the Fourth Amendment. Notably, even those courts not wedded to the primary purpose requirement recognized the need to differentiate national security investigation from criminal investigation.[223] Thus, national security jurisprudence recognizes the need for a categorization tool dividing the FISA and criminal law spheres.

C. The Primary Purpose Test Grows into a "Wall"

As the Executive and the FISC worked with FISA, they began to translate the abstraction of the primary purpose doctrine into practice. This effort led to the erection of the so-called "wall" between intelligence investigation and parallel criminal investigation. The concept and practice of the wall arose because of the dual character of much foreign intelligence information—its usefulness to both intelligence analysts and criminal investigators.[224] The wall ensured that the FISA investigation retained its primary purpose despite ongoing and contemporaneous criminal law enforcement efforts, which often used information disseminated from the FISA investigation.

In reality, the wall did not constitute one administrative structure, but instead a variety of devices to prevent the criminal

221. *E.g.*, United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984). *But see In re* Sealed Case, 310 F.3d 717, 741 (FISA Ct. Rev. 2002) (stating that "while Title III contains some protections that are not in FISA, in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections").

222. *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991).

223. United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) ("The certifications required by the statute are sufficient to ensure that the approved surveillance will fit within the category of foreign intelligence surveillance.").

224. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 617 (FISA Ct. 2002), *rev'd on other grounds, In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) ("[M]ost information intercepted or seized has a dual character as both foreign intelligence information and evidence of crime (e.g., the identity of a spy's handler, his/her communication signals and deaddrop locations the fact that a terrorist is taking flying lessons, or purchasing explosive chemicals) differentiated primarily by the persons using the information." (footnote omitted)).

investigators from usurping, or even partnering with, the intelligence investigators.[225] The wall prevented the commingling of both information and personnel[226] and it prevented cross contamination.[227] The ultimate purpose of the wall corresponded to the driving logic behind the primary purpose test: the need to limit the foreign intelligence exception because of the perception that the Executive would avail itself of FISA to take advantage of lower probable cause standards and greater evidence-gathering power.[228]

D. Validating FISA Absent the Primary Purpose Test and the Wall

The wall came under attack following the events of September 11, 2001. Critics believed that better information sharing between the criminal and intelligence sides could have helped stop the terrorists.[229] Even before September 11, many commentators felt that the wall had eroded the effectiveness of counterintelligence and counterterrorism efforts.[230] The post-September 11 war on terrorism, coupled with these preexisting concerns, drove the dismantling of the wall by the Patriot Act amendments and by the ensuing internal procedures for cooperation and information sharing between intelligence investigators and criminal law enforcement.

Specifically, the Patriot Act lowered the FISA certification

225. *Id.* at 620.

226. Richard B. Schiff, *A Counterintelligence Perspective, Or How I Learned to Stop Worrying and Love the Wall*, 52 FED. LAW. 32, 33 (2005) (describing the reciprocal "protective mechanisms" to restrict information access and the "shielding device" of keeping preventing criminal law enforcement personnel from participating in intelligence collection).

227. *Cf.* Banks, *supra* note 4, at 1162-63 (stating that "the FBI developed a parallel system of 'dirty' teams for intelligence gathering and 'clean' teams for law enforcement . . . [that] could work at the same time on the same targets, yet . . . rarely talk[] to one another").

228. Schiff, *supra* note 226, at 33 ("By keeping law enforcement professionals away from intelligence activities, the wall was able to prevent the appearance that techniques used in intelligence investigations were being invoked to circumvent the more demanding and public requirements for obtaining evidence in criminal cases.").

229. *See*, *e.g.*, SENATOR PATRICK LEAHY ET AL., FBI OVERSIGHT IN THE 107TH CONGRESS BY THE SENATE JUDICIARY COMMITTEE: FISA IMPLEMENTATION FAILURES § III.A (2003) (detailing the mishandling of leads in the weeks leading up to September 11), http://leahy.senate.gov/press/200302/FISA02-03.html; OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION PRIOR TO THE SEPTEMBER 11 ATTACKS (2004) (same); POSNER, *supra* note 190, 25-26 (examining the conclusions of the 9/11 Commission); Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 957-72 (2003) (same).

230. *See*, *e.g.*, *In re* Sealed Case, 310 F.3d 717, 728 (FISA Ct. Rev. 2002); U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 11-12 (2001); *see also* POSNER, *supra* note 190, at 31-32 (explaining resistance to greater information sharing within the FBI and CIA).

standard from its previous requirement that "the purpose" of the investigation was to obtain foreign intelligence information, to the present directive that foreign intelligence collection must be "a significant purpose" of the investigation.[231] The Patriot Act also explicitly authorized consultation and coordination between intelligence and criminal personnel.[232] Further, the Attorney General promulgated internal guidance to ensure cooperation and information sharing between the intelligence and criminal functions.[233]

Many proponents of the wall reacted to the new regime with opprobrium. The FISC itself declared that the new structure allowed criminal prosecutors to direct FISA investigation and gave criminal law enforcement "every legal advantage conceived by Congress" but normally reserved for intelligence gathering.[234] Accordingly, the FISC ordered new minimization procedures designed to regulate the Executive's authority to coordinate intelligence investigation and criminal enforcement.[235]

The Executive appealed to the Foreign Intelligence Surveillance Court of Review ("FISCR"), which overturned the FISC decision.[236] More significantly, the FISCR upheld FISA, as amended,[237] characterizing the efforts to separate intelligence from criminal investigation as the consequence of a "false dichotomy."[238] The FISCR explained that, from its first enactment in 1978, FISA embodied an understanding that foreign intelligence efforts dovetailed with criminal law enforcement.[239] According to the court, the prosecution of counterintelligence and counterterrorism cases represented an exercise of the Executive's foreign policy power.[240] The FISCR explained that the primary purpose standard arose in response to the exercise of pure Executive power and represented an effort "to determine the boundaries of that constitutional authority."[241] Critically, the FISCR explained that FISA posed the reverse analytical problem of whether Congress could expand the

231. *See supra* notes 59-60 and accompanying text.
232. *See supra* note 70 and accompanying text.
233. *See supra* notes 71-72 and accompanying text.
234. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 617, 623-24 (FISA Ct. 2002), *rev'd on other grounds, In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).
235. *Id.* at 625-27 (invoking the court's supervisory power under 50 U.S.C. § 1805(a) and (c), and § 1824(a) and (c)).
236. *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).
237. *Id.*
238. *Id.* at 725.
239. *Id.* (citing FISA's legislative history).
240. *Id.* at 742-43.
241. *Id.* at 742.

Executive's power beyond those boundaries.[242] In sum, the court questioned whether previous decisions should have ever injected the primary purpose test into the statutory scheme. Regardless, the FISCR explained that the Patriot Act amendments, and their limited legislative history, abundantly demonstrated the intent to purge the primary purpose requirement.[243]

The FISCR upheld the amended FISA as constitutionally reasonable based on its application of the *Keith* balancing test.[244] The court found that the primary purpose test created an "unstable, unrealistic, and confusing" system.[245] Further, the court found that, instead of fostering the cooperation necessary to achieve effective counterintelligence or counterterrorism, the wall punished exactly those efforts.[246] Moreover, the court noted that the focus on the subjective intent of the investigators—their primary purpose—stood at odds with the Supreme Court's general rejection of a Fourth Amendment jurisprudence based on the motivation of Executive officials.[247] Finally, the court noted that the wall proved impracticable.[248] Under the *Keith* balancing test, although the individual interest in privacy did not change, the FISCR dramatically recalibrated the weight of the government's concerns, which include an overt interest in prosecution and a need for effective procedures that permit cooperation likely to achieve national security.

The FISCR decision ended with some constitutional ambivalence regarding the precise rationale for upholding FISA.[249] The court found that, because FISA contained judicial preclearance procedures predicated on probable cause findings, it either met or "certainly came close" to meeting minimum Fourth Amendment standards for a warrant.[250] Further, the court suggested that FISA might fit within the Supreme Court's "special needs"

242. *Id.*
243. *Id.* at 732-33, 737.
244. *Id.* at 742.
245. *Id.* at 743.
246. *Id.* (suggesting the wall might even have posed a danger to national security).
247. *Id.* (citing Whren v. United States, 517 U.S. 806 (1996)).
248. *Id.*; *see also supra* note 230 and accompanying text.
249. *Sealed Case*, 310 F.3d at 746 ("We acknowledge, however, that the constitutional question presented by this case—whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment—has no definitive jurisprudential answer.").
250. *Id.* It would appear that this tentative conclusion rested on the *Keith* Court's dictum that an intelligence surveillance warrant might not conform to the same particularity standards as a criminal warrant, but instead could have a more relaxed, or "less precise," description of the scope of the investigation. *Id.* at 744 (quoting *Keith*, 407 U.S. 297, 322 (1972)).

jurisprudence—the rubric under which the Court has approved sobriety checkpoints and border searches.[251] The court found that FISA's "programmatic purpose" of protecting the nation from international terrorism and espionage constitutes the sort of non-crime-control agenda appropriately administered nevertheless by law enforcement under the special needs doctrine.[252] Notably, the court did not hold that FISA constituted a special need. Nevertheless, the court concluded that, taking all considerations into account, FISA satisfied the reasonableness requirement.[253]

While the central analytical device for validating FISA is a balancing test, the underlying constitutional concern entails the scope of an exception from normal Fourth Amendment requirements. The FISCR devoted little attention to this matter, focusing mostly on evaluating the reasonableness of FISA. The deficiency is troubling—some of the early courts to permit warrantless national security investigation found that the primary purpose test derived from the exception itself, not from the balancing test.[254] Under this approach, the primary purpose test served to restrict the scope of the exception and prevent its elastic expansion. Perhaps this explains why the many courts validating FISA read the primary purpose rule into the statute without analysis; the rule constituted an aspect of the very constitutional doctrine that made FISA possible, rather than a component of the reasonableness analysis.[255] Because the FISCR spent its time focused on the reasonableness analysis, it undervalued the concerns that impelled the early courts to develop the primary purpose standard. Indeed, the FISCR treated the primary purpose test as a feature that could come or go depending on reasonableness, rather than examining whether it plays a fundamental, and necessary, role in regulating access to the flexible national security reasonableness test itself.

In any event, the consequence of the FISCR decision is clear. Within the national security exception, virtually no distinction exists between criminal law enforcement and intelligence. So long as the investigation includes a significant foreign intelligence

251. *Sealed Case*, 310 F.3d at 745.

252. *Id.* at 746. Similarly, commentators have proposed an extended special-needs rationale authorizing national security investigation of catastrophic threats. *See* Gould & Stern, *supra* note 211, at 777-78 (proposing a catastrophic threat doctrine); *see also id.* at 813-33 (detailing an expanded special-needs rationale for national security investigation based on less than traditional probable cause).

253. One other post-Patriot Act court has upheld the constitutionality of FISA. *See* United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005).

254. *See supra* note 187 and accompanying text.

255. *See supra* notes 195-196 and accompanying text.

collection purpose, it may also fully embrace the collection of evidence for prosecution. Under this approach, FISA will consume the normal Fourth Amendment process—surveillance under Title III and search under Federal Rule of Criminal Procedure 41—for a significant swath of counterterrorism investigation and enforcement activity currently at the forefront of FBI and Justice Department efforts.

E. Nondisclosure of FISA Applications and Other Constitutional Issues

A number of other constitutional challenges, mostly beyond the scope of this Article, have also arisen. Courts have rejected challenges to FISA under the First Amendment, under equal protection, and on separation of power grounds.[256] Importantly, though, a number of courts have considered and rejected claims that the in camera and ex parte review procedures[257] violate due process, confrontation, and right to counsel guarantees.[258] The only window that the judiciary has opened necessitates rather extraordinary circumstances[259]—either a facial problem with the FISA application (unlikely given the amount of internal review devoted to the document) or evidence introduced by the aggrieved person casting doubt on the application (also unlikely given the impossibility of knowing what evidence to introduce without gaining access to the application first).[260] The ex parte and in camera consideration of FISA applications, however, does not differ markedly from the treatment of electronic surveillance applications under Title III, which the Supreme Court has upheld.[261]

256. *See* United States. v. Cavanagh, 807 F.2d 787, 791-92 (9th Cir. 1987); United States v. Duggan, 743 F.2d 59, 74-76 (2d Cir. 1984); United States v. Nicholson, 955 F. Supp. 588, 590-93 (E.D. Va. 1997); United States v. Megahey, 553 F. Supp. 1180, 1194-98 (E.D.N.Y. 1982), *aff'd*, 729 F.2d 1444 (2d Cir. 1983); United States v. Falvey, 540 F. Supp. 1306, 1314-15 (E.D.N.Y. 1982).

257. *See supra* notes 83-88 and accompanying text.

258. *See Damrah*, 412 F.3d at 624; *In re* Grand Jury Proceedings of the Special April 2002 Grand Jury, 347 F.3d 197, 203 (7th Cir. 2003); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Ott, 827 F.2d 473, 476-77 (9th Cir. 1987); *Duggan*, 743 F.2d at 78; United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982); *Nicholson*, 955 F. Supp. at 592 & n.11; *Megahey*, 553 F. Supp. at 1193-94; *Falvey*, 540 F. Supp. at 1315-16; *cf.* United States v. Sarkissian, 841 F.2d 959, 965-66 (9th Cir. 1988) (reviewing nondisclosure challenge under the Classified Information Procedures Act).

259. One court has conceded that "the alert eye of an advocate might be helpful in discerning defects in the certificates." *Megahey*, 553 F. Supp. at 1194.

260. *Duggan*, 743 F.2d at 78 (explaining that a need for disclosure might arise if "the judge's initial review revealed potential irregularities").

261. Taglianetti v. United States, 394 U.S. 316, 317 (1969); *Falvey*, 540 F. Supp. at 1315 (citing Giordano v. United States, 394 U.S. 310, 314 (1969)).

F. The Status of Tools for Gathering Information from Third Parties

Orders for the production of tangible things, investigations that use pen registers, and national security letters all seek information that the suspect has placed in the hands of third parties—this fact determines the constitutional fate of these three investigatory tools.[262] The three tools fall under the line of Supreme Court authority holding that an individual has no Fourth Amendment privacy interest in information or things given to a third party.[263] Although before the Patriot Act these tools all contained relatively stringent requirements that the Executive demonstrate a nexus with a foreign threat,[264] no constitutional principle mandated that language. Instead, those rules constituted a pale statutory parallel of the primary purpose test. As such, the elimination of those mandates by the Patriot Act did not change the constitutional status of these third-party tools.

While the core constitutionality of these tools is firmly embedded in Fourth Amendment jurisprudence, some of the details are in doubt. In *Doe v. Ashcroft*,[265] the district court declared unconstitutional certain aspects of the national security letter authority over communications providers.[266] Specifically, that court considered the rights of the recipient of a national security letter, not the suspect, and concluded that the statutory scheme lacked an adequate procedure for the recipient to challenge the letter[267] and impermissibly restricted the recipient's ability to discuss the letter with legal counsel.[268] Further, with regard to subscribers to the

262. *See supra* notes 89-94, 100-116 and accompanying text (describing the three tools).

263. *See* Smith v. Maryland, 442 U.S. 735, 742, 744-45 (1979); United States v. Miller, 425 U.S. 435, 443 (1976); *cf.* SEC v. O'Brien, 467 U.S. 735, 741-43 (1984) (holding that adversely affected person had no right to notice of subpoenas issued to third party); *see also* Woods, *supra* note 4, at 53 (explaining that the three national security investigation tools at issue in this Part all fall "outside the protection of the Fourth Amendment"). *But see* Dempsey, *Sections 209, 212, and 220*, *supra* note 4, at 42-43 (arguing that information stored with third parties should receive privacy protection).

264. *See supra* notes 92, 103, 117 and accompanying text.

265. 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

266. *See supra* notes 106-116 and accompanying text (describing national security letters).

267. *Doe*, 334 F. Supp. 2d at 505 ("[T]he Court here concludes that what is, in practice, an implicit obligation of automatic compliance with NSLs violates the Fourth Amendment right to judicial access, even if hypothetically the law were construed to imply such access."); *see also supra* note 172 and accompanying text (noting the difference in enforcement for subpoenas and national security letters).

268. *Doe*, 334 F. Supp. 2d at 511-26; *see also* Swire, *Section 214*, *supra* note 4, at 58-59 (critiquing the "gag rule" as unjustified because a records search

communication provider generally, the court found that the lack of provisions for the provider to challenge the letter chilled the subscribers' free speech rights.[269] More generally, the court explained that, although national security letters bear some similarity to administrative subpoenas, they differ because the constitutionality of administrative subpoenas crucially depends on the availability of post facto judicial review during a possible challenge by the recipient to compensate for the absence of judicial preclearance before the issuance of the subpoena.[270]

While *Doe*, read narrowly, concerns only one species of national security letters, its implications sweep more broadly. The other two national security letter schemes also lack provisions for challenge and contain similar confidentiality requirements.[271] Moreover, the FISA provisions governing orders for the production of tangible things and investigations using pen registers lack a mechanism for challenge by the recipient of the order. Also, the provision governing the production of tangible things contains a confidentiality requirement similar to those in the national security letter statutes.[272] Accordingly, these aspects of the other national security investigation tools may also stand on loose constitutional ground, vulnerable to the same attack leveled against the national security letter at issue in *Doe*.

VI. CONSTITUTIONAL REGULATION OF NATIONAL SECURITY INVESTIGATION

A. Framing the Problem

The jurisprudence of national security investigation initially revolved around constitutional law. Only with the advent of FISA, did that focus subside in favor of a statutory emphasis.[273] For several reasons, this Article proposes returning to the constitutional roots. First, with the elimination of both the wall and the primary purpose test, which constituted internal and systemic barriers to misuse, the danger of pretextual use of FISA takes on new significance.[274] Given the current makeup of the political

does not entail the same sensitivity concerns as electronic surveillance or physical search).

269. *Doe*, 334 F. Supp. 2d at 506-11; *see also* Swire, *Section 214*, *supra* note 4, at 55-56 (critiquing third-party investigation tools because they allow acquisition of anyone's records, rather than just the target's).

270. *Doe*, 334 F. Supp. 2d at 495.

271. *See supra* note 107 and accompanying text.

272. *See supra* note 105 and accompanying text.

273. *See* Breglio, Note, *supra* note 4, at 208.

274. *See* Kreimer, *supra* note 19, at 172 ("[T]he removal of prophylactic

branches,[275] calls for either legislative reform or a return to earlier Executive self-limits seem unlikely to transform into action.[276] Further, although the possibility of using FISA-acquired information in a prosecution has existed since the enactment of the statute, this "dual use" phenomenon has taken on new force during the war on terrorism—an effort in which intelligence information and criminal evidence have lost much of the distinction they may have enjoyed during the Cold War.[277] This pressure is further exacerbated by the FBI's shift in focus from normal criminal law to counterterrorism work.[278]

With these concerns in mind, and recalling the numerous apprehensions about national security investigation previously described,[279] it becomes possible to examine existing legal doctrine to determine whether it offers any possible solution. Knowledge of the problems will allow the reverse engineering of a response.[280] Importantly, this solution must carefully weigh the extent to which it might degrade the effectiveness of counterterrorism and counterintelligence investigation.[281]

B. A Limit on the Use of Information Unrelated to National Security

A limit on the Executive's use of information acquired by FISA, but unrelated to national security, would serve to address many of the problems identified above.[282] For example, consider a judicially

constraints on information sharing will, *ceteris paribus*, make abuse more likely."); Swire, *The System*, *supra* note 4, at 1327, 1339.

275. As of the time of this Article's writing, and at the President's urging, both the House and Senate have renewed, with relatively few amendments, the provisions of the Patriot Act set to expire at the end of this year. *See* Dan Eggen, *Senate Approves Partial Renewal of Patriot Act*, WASH. POST, July 30, 2005, at A3.

276. *See* Banks & Bowman, *supra* note 13, at 68-74 (explaining historic executive branch self-regulation under FISA).

277. *See id.* at 9.

278. *See* Swire, *The System*, *supra* note 4, at 1329; Dan Eggen & Susan Schmidt, *Data Show Different Spy Game Since 9/11*, WASH. POST, May 1, 2004, at A1.

279. *See supra* Part I.

280. *See* Kreimer, *supra* note 19, at 169 ("[I]t is often easier to reverse engineer legal doctrine if one has a clear idea about the threats it seeks to counter.").

281. *See id.* at 172.

282. Indeed, other commentators have noted the attractiveness of the use limit model. *See* Rosen, *supra* note 19, at 612 (stating that "[t]he use-limitation strikes me as a central insight, a tremendous victory for privacy," and describing the use limit added, at the urging of privacy advocates, to the proposed Computer Assisted Passenger Pre-Screening System preventing screeners from forwarding to law enforcement anything but evidence of outstanding warrants for violent crimes).

enforced exclusionary rule that prevents the Executive from using information derived from FISA in a prosecution of a target for selling narcotics because none of the evidence demonstrated that the criminal conduct had any connection to national security.

Such a use limit would remove much of the incentive for the pretextual deployment of a FISA investigation. If the alleged "end run" around the Fourth Amendment yields no usable evidence, then prosecutors would have little incentive to improperly rush toward FISA. Concededly, criminal prosecutors might opt for FISA over Title III for surveillance of a terrorism suspect, but as the FISCR observed, that concern entails a false dichotomy; there is no way to conduct a FISA inquiry of a counterterrorism target without investigating criminal conduct. Instead, the pretext concern is properly located around the possibility that the Executive might use FISA as a substitute for normal criminal law enforcement based on trumped up evidence of a connection to a foreign threat. An unrelated information use limit would remove all motivation for such a tactic.

More importantly, a use limit would serve as a replacement for the primary purpose rule. The primary purpose rule safeguarded the special Fourth Amendment rules for national security investigation by ensuring that they came into play only for genuine national security matters. A use limit would serve the same function ex post that the primary purpose rule served ex ante[283] by ensuring that the Executive could use the information derived from FISA only for genuine national security efforts. Further, it would do so without forcing the dilemma of the wall: keep the wall and lose the sharing of foreign intelligence information; lose the wall and slide down the slope to a surveillance state.[284] Conversely, the use limit would provide less consistent regulation than the primary purpose test because it would come into effect only in select cases, rather than restricting all FISA efforts.

The use limit could achieve, at least in part, many of the other identified goals. First, it would reduce the possibility of abuse by preventing the Executive from vindictively using FISA information against a political foe unless that adversary actually posed a foreign threat. Although the use limit would not eliminate the actual invasion of privacy, it would diminish the Executive's ability to exploit that intrusion. While this will not prevent the chilling of

283. *See* Kreimer, *supra* note 19, at 181 ("In today's environment, ex ante judicial control of surveillance is unlikely. One response lies in strengthening legal doctrines that exert ex post control against abuse of information obtained by surveillance. The effect of such doctrines, even if courts adopt them, however, will be sporadic.").

284. *See* Swire, *The System*, *supra* note 4, at 1362.

dissent completely, it might reassure the public that surveillance is not all-powerful.[285] More pointedly, it would signal an important role for the judiciary in limiting and regulating Executive surveillance. A use limit would retard mission creep by tightly confining the universe of inquiries that FISA investigation could support. It would not halt dataveillance when the Executive intended to mine patterns related national security, but it would check the Executive's use of acquired information for regular crime control.[286] Although a use limit would not address secrecy, it would place the judiciary in a prominent regulatory role and promote accountability.

A court could recognize the use limit in a challenge by an aggrieved person against whom the Executive sought to use FISA information unrelated to national security. A judge favoring a cautious and incremental approach might choose this option, while a judge gravely concerned about privacy and the danger of pretext might choose a more preventative approach: a court contemplating whether to uphold FISA, and concerned about the loss of the primary purpose test, should announce that validation of the statute hinges upon the recognition of a limit on the use of information unrelated to national security.

C. Minimization as the Constitutional Basis for a Use Limit

The natural basis for the use limit is the Fourth Amendment's requirement of minimization during surveillance. Most generally, minimization forces the Executive to make efforts to avoid acquiring private information not relevant to the investigation.[287] As one court explained: "Minimization requires that the government adopt reasonable measures to reduce to a practical minimum the interception of conversations unrelated to the criminal activity under investigation while permitting the government to pursue legitimate investigation."[288]

The origin of minimization as a component of the Fourth Amendment traces back to *Berger v. New York*,[289] in which the

285. *See* Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting) ("Electronic surveillance . . . makes the police omniscient; and police omniscience is one of the most effective tools of tyranny.").

286. *See* Berkower, *supra* note 9, at 2286-87 (describing the use limit in the health privacy statutes that prevents the use of patients' private information in non-health care fraud investigation).

287. *See* United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987) (stating that minimization confines, as narrowly as possible, the Executive's intrusions into the privacy and personal lives of the target and anyone who may innocently come into contact with the target).

288. United States v. McGuire, 307 F.3d 1192, 1199 (9th Cir. 2002).

289. 388 U.S. 41 (1967).

Supreme Court struck down an electronic surveillance statute, in part, because it allowed the acquisition of "the conversations of any and all persons coming into the area covered by the device . . . indiscriminately and without regard to their connection with the crime under investigation."[290] Although *Berger* did not use the word "minimization," Congress responded by enacting Title III, which included a minimization provision designed to comply with *Berger*'s articulation of the "constitutional prerequisite to the validity of all court-ordered electronic surveillance."[291] Accordingly, although many courts note the constitutional imprimatur of minimization,[292] the case law on the subject is uniformly statutory. The Supreme Court has set the standard for compliance with the minimization requirement at objective reasonableness depending "on the facts and circumstances of each case."[293] Failure to correctly minimize subjects the improperly obtained evidence to the workings of the exclusionary rule.[294]

Under Title III, minimization reinforces the Fourth Amendment's particularity requirement that restricts the Executive to conducting surveillance only for information linked to the underlying criminal offense.[295] FISA, in contrast, allows surveillance without particularity,[296] and only minimization, which restricts the Executive to foreign intelligence information, prevents the intrusion from becoming total. Accordingly, minimization under FISA takes on far greater importance in guarding privacy.

Although under Title III minimization focuses primarily on acquisition,[297] under FISA, it has revolved equally around retention

290. *Id.* at 59.

291. LAFAVE ET AL., *supra* note 155, § 4.5(b), at 387

292. *See, e.g.*, United States v. Williams, 737 F.2d 594, 604 (7th Cir. 1984) (noting that the statutory minimization provision "finds its roots in the Fourth Amendment").

293. Scott v. United States, 436 U.S. 128, 140 (1978).

294. *See id.* at 135-36; *see also* S. REP. NO. 95-604 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3956 (explaining, in FISA's legislative history, that "if monitoring agents choose to disregard the minimization standards and thereby acquire evidence of a crime against an overheard party whose conversation properly should have been minimized, that evidence would be acquired in violation of this chapter and would properly be suppressed").

295. *See supra* notes 133-136 and accompanying text.

296. *See* United States v. Cavanagh, 807 F.2d 787, 790-91 (9th Cir. 1987); *see also* Banks, *supra* note 4, at 1152 (explaining how the mosaic theory of intelligence renders the idea of particularity ill-suited).

297. In some cases courts have allowed non-contemporaneous minimization, so long as it occurred reasonably prompt and protects privacy equally. *See*, *e.g.*, United States v. Padilla-Pena, 129 F.3d 457, 464 (8th Cir. 1997); United States v. David, 940 F.2d 722, 729-30 (1st Cir. 1991). Conceivably, the promptness prong alone could result in the suppression of considerable amounts of FISA information. *See* Dan Eggen, *FBI Faulted on Unreviewed Wiretap Recordings*,

and dissemination.[298] The impetus for allowing minimization later in the FISA process stems in part from the intensive approach to intelligence surveillance[299] and from the fact that much of the information acquired through FISA involves a foreign language or the use of code words, making contemporaneous minimization impracticable, and requiring instead the later use of translators and analysts.[300] With noncontemporaneous minimization the Executive must cease examining the information as soon as it becomes apparent that it requires minimization.[301] The use limit would function as a component of the normal minimization process occurring during dissemination—in effect, the use limit would prohibit the Executive from sharing non-national security information for the purpose of employing that information at trial. In minimization argot, the use limit would prevent the Executive from disseminating FISA-acquired information unrelated to national security.[302]

The critical question, though, is how the use limit would come into being. Recall from the analysis of deficiencies in the FISCR decision that the primary purpose test may have its roots in an attempt to police the national security exception to normal Fourth Amendment standards;[303] part of that exception includes lower standards for particularity.[304] While the FISCR may have correctly understood that this exception does not specifically mandate the primary purpose test, it failed to perceive the need for a loosely equivalent regulatory device, especially to perform the same function. The use limit should step into this role. Because the use limit acts as an ex post substitute for the abolished ex ante primary purpose test,[305] the two rules operate as functional, or analytical, parallels.[306] The use limit actually functions better by more directly addressing the particularity concern.

It would serve the general framework of national security jurisprudence, therefore, to replace the missing primary purpose test with the use limit. Although FISA contains a number of

WASH. POST, July 28, 2005, at A11 (detailing a growing backlog of over 8,000 hours of unreviewed audio surveillance from counterterrorism investigation).

298. *See supra* note 139 and accompanying text; *see also* Freiwald, *supra* note 16, at 21 (detailing the stages of a wiretap investigation).

299. *See supra* note 3 and accompanying text.

300. *See In re* Sealed Case, 310 F.3d 717, 740-41 (FISA Ct. Rev. 2002).

301. *See David*, 940 F.2d at 730; *Padilla-Pena*, 129 F.3d at 463-64.

302. *See infra* Part VI.G.3 (explaining the possible sweep of the use limit beyond the prosecution's case-in-chief).

303. *See supra* notes 253-55 and accompanying text.

304. *See supra* notes 133-36, 155-57 and accompanying text.

305. *See supra* note 283 and accompanying text.

306. They both serve as "prophylactics" preventing prosecutors from making improper use of FISA. *See* Banks, *supra* note 4, at 1179-80.

procedural requirements to ensure that it falls within the national security exception, the concern lies not with statutory details, but with constitutional requirements. Accordingly, the use limit would act as a constitutional backstop, or failsafe device, guaranteeing that a FISA investigation did not stray beyond the scope of the national security exception.

Perhaps the route to the development of the use limit needs to depart at this point from an examination of the national security exception and return to the reasonableness analysis. Because the constitutional approval of FISA rests so heavily on *Keith*'s reasonableness approach to evaluating national security investigation,[307] and because minimization rests on reasonableness, it makes sense to view the development of minimization through the lens of *Keith*'s test.

A key question is whether the *Keith* test should include proportionality analysis. Indeed, German intelligence investigation law includes a constitutional proportionality requirement[308] that functions somewhat like the *Keith* balancing test. Generally, that proportionality principle requires the balancing of the "defendant's interests in privacy against the importance of the evidence and the seriousness of the offense charged."[309] This test represents a more precise formula for calculating the relative weights of the individual and societal interests at stake without letting the state's interests dominate. Consequently, national security jurisprudence should include a proportionality component. While the Supreme Court may seem to have rejected proportionality, it did so in a case applying a bright-line formula for probable cause[310]—an approach the Court rejected in *Keith* for the analysis of national security investigation.[311] Therefore, courts should include proportionality in the balancing process and conclude that proportionality powerfully supports the use limit: the national security exception to the Fourth Amendment opens only for the most serious offenses against the nation, not for ordinary crimes.

Three distinct factors, therefore, militate for the proposed use limit: first, when proportionality analysis takes its proper place in the *Keith* balancing test, the analysis favors minimizing information

307. *See supra* note 211 and accompanying text.

308. Craig M. Bradley, *The Exclusionary Rule in Germany*, 96 HARV. L. REV. 1032, 1049, 1054-55 (1983); Rosen, *supra* note 19, at 612; *see also id.* at 617 (explaining that the Canadian courts have also debated a proportionality rule).

309. Bradley, *supra* note 308, at 1034.

310. *See* Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001). *But see id.* at 365-66 (O'Connor, J., dissenting) (arguing for a balancing test under the reasonableness prong rather than a bright-line rule).

311. *See supra* Part III.A.

unrelated to national security; second, in the absence of the primary purpose test, the use limit protects privacy and prevents Executive abuse; third, and most significantly, the use limit prevents the national security exception from expanding in scope. For these reasons, the use limit should become part of the constitutional minimization requirement. As such it would apply to FISA regardless of its absence from the statutory and internal minimization provisions.

D. Operation of the Use Limit

Minimizing the use of information unrelated to national security would have a dramatic effect on the statute and the internal procedures. It would render unconstitutional certain applications of the provisions that allow the "retention and dissemination" of evidence of crime regardless of whether it constitutes foreign intelligence information.[312] Similarly, it would cast into doubt those portions of the information sharing procedures that allow the Executive to disseminate non-national security information.[313]

Clearly, if the Executive employed the information sharing authority of the statute to "disseminate[] for law enforcement purposes"[314] evidence of ordinary crime, it would violate the proposed use limit. If, on the other hand, the statutory authority played a role in the dissemination of information not easily classified as foreign intelligence information, but related somehow, it might survive scrutiny. This distinction hinges upon the definition of "information unrelated to national security."

A prototypical case could involve "an international terrorist [who] is also a drug dealer—not to support terrorist activities but to support himself."[315] While dissemination of information regarding the ordinary crime should fail the use limit in this hypothetical, it would not if the situation involved "international terrorists [who] engage in a bank robbery in order to finance their terrorist activities."[316] In this second case, the information regarding ostensibly ordinary crime constitutes foreign intelligence

312. *See* 50 U.S.C. §§ 1801(h)(3), 1821(4)(C) (2000); *see also* H.R. REP. NO. 95-1283 at 62 (1978) (explaining that this provision applies to evidence of crime "totally unrelated to intelligence matters").

313. *See supra* note 73-82 and accompanying text (detailing the information sharing procedures).

314. *See* 50 U.S.C. §§ 1801(h)(3), 1821(4)(C).

315. *See* Banks, *supra* note 4, at 1179 (proposing this hypothetical).

316. AG GUIDELINES, *supra* note 71, at 34 ("CRIME INVOLVED IN OR RELATED TO A THREAT TO THE NATIONAL SECURITY: both crimes directly involved in activities constituting a threat to the national security, and crimes that are preparatory for or facilitate or support such activities.").

information because of its direct connection to preventing terrorism, despite the fact that the motive of the bank robbers would normally play no role in their criminal prosecution. Accordingly, to the extent the Executive resorted to the questionable statutory authority as a defense to a challenge by the bank robbers, the use limit would not render that application of the statute unconstitutional. Indeed, the FISCR explained that "ordinary crimes might be inextricably intertwined with foreign intelligence," and further distinguished such related crimes from "wholly unrelated ordinary crimes."[317] It would not be difficult for courts to adjudicate this dividing line, in the context of particular facts, as they heard challenges to the use of FISA evidence in cases of ordinary crime.[318]

More broadly, reinvigorating constitutional minimization principles would provide far greater protection for non-United States persons targeted under FISA. Currently, statutory minimization applies only to United States persons,[319] while the Fourth Amendment knows no such restriction. The use limit and the injection of constitutional minimization into FISA would function, therefore, to significantly expand the privacy rights of many targets.

E. Other Common Regulatory Devices Inadequate

Before proceeding further, it makes sense to pause and consider some other common devices that could serve to regulate national security surveillance: traditional suppression challenges to FISA investigation, civil constitutional tort suits, or a host of proposals for legislative reform.

The most straightforward of these options is the one built into FISA, the traditional suppression challenge.[320] This option will not result in significant regulation of national security investigation. Most often the Executive will have tightly crafted the FISA application[321] and it will fare well, especially without adversarial testing in the ex parte and in camera suppression proceeding.[322] Moreover, the Executive possesses prosecutorial discretion to bring only viable cases, further reducing the possibility of the process

317. *In re* Sealed Case, 310 F.3d 717, 736 (FISA Ct. Rev. 2002).

318. *But see* Hardin, Note, *supra* note 4, at 332-33 (arguing that judging the difference between the two categories of ordinary crime is "undoubtedly complex" and "acutely ominous" in light of the implications).

319. *See supra* note 67 and accompanying text.

320. *See supra* notes 83-88 and accompanying text.

321. *See* Lerner, *supra* note 229, at 962-63 (explaining the high success rate of warrant applications as flowing from intense internal deliberations).

322. *See* United States v. Nicholson, 955 F. Supp. 588, 592 (E.D. Va. 1997) (noting that, in every reported case, the court conducted the review in camera and ex parte).

leading to the accumulation of adverse precedent.

Perhaps more importantly, given the national security context, courts reviewing FISA applications will have a tendency to defer to the Executive. As Cicero's maxim states it: "*silent enim leges inter arma,*" or "in times of war the law falls silent."[323] Indeed, on exactly this point, Chief Justice Rehnquist has written: "It is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime."[324] Even if Rehnquist's assessment is merely personal,[325] a recent study confirms that the judiciary defers[326] to the Executive in procedural matters—such as the reasonableness of a FISA application—during times of national crisis.[327] Although some commentators have argued that today's courts have broken that tradition of deference,[328] it seems unwise to expect significant regulatory doctrine to emerge from suppression challenges.

The constitutional tort suit presents an even less likely candidate for regulation of national security investigation. Civil enforcement has the enormous advantage of averting the problems attendant to the exclusionary rule:[329] the demoralization costs of benefiting individuals with dirty hands[330] and the judicial skewing as courts shade their decisions to avoid these costs.[331] Unfortunately, a civil remedy hinges on notice to targeted parties, and FISA—if not national security generally—forecloses that

323. Capt. M. Scott Holcomb, *View from the Legal Frontlines*, 4 CHI. J. INT'L L. 561, 561 (2003) (quoting THE OXFORD DICTIONARY OF QUOTATIONS 204 (Angela Partington ed., 4th ed. 1992)).

324. WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 224-25 (Alfred A. Knopf, Inc. 1998).

325. *See* Kreimer, *supra* note 19, at 152 (noting that, as Assistant Attorney General, Rehnquist argued that Executive self-discipline would answer all complaints of excess information gathering).

326. *See* Steven R. Shapiro, *The Role of the Courts in the War Against Terrorism: A Preliminary Assessment*, 29 FLETCHER F. WORLD AFF. 103, 105-06 (2005) (explaining the tradition of judicial deference as arising from self-doubt about institutional competence, concern about institutional authority, and a lack of Executive candor); *see also* Lobel, *supra* note 4, at 768 (examining the crisis thesis of judicial deference).

327. *See* Lee Epstein et al., *The Supreme Court During Crisis: How War Affects Only Non-War Cases*, 80 N.Y.U. L. REV. 1, 79 (2005) (concluding that criminal defendants lose procedural motions eight percent more often during time of war).

328. *See* Shapiro, *supra* note 326, at 115-16 (arguing that today's legal and political landscape differs from the one present during previous wars, and citing *Hamdi* and *Rasul* as evidence of a shift).

329. *See* Amar, *supra* note 19, at 758, 797-99.

330. *See* Akhil Reed Amar, *The Future of Constitutional Criminal Procedure*, 33 AM. CRIM. L. REV. 1123, 1138-39 (1996).

331. *See id.*

option.[332]

A number of commentators have proposed a variety of legislative or administrative reforms. For instance, Peter Swire suggests a host of excellent reforms, including an adversary system within FISC, delayed notice to targets, and certification of suppression motions to the FISC.[333] While these proposals might well cure the deficiencies previously identified, they all require the will of the political branches. One recurring proposal that would allow the judiciary to act without the support of the political branches is for the FISC to continue to innovate in its control over the minimization procedures.[334] This is, however, the process that led to the reversal of the FISC by the FISCR.[335]

F. A Proper Judicial Role

In order for a court to adopt the use limit, it would need to explain why the creation of such a rule does not offend the proper limits on judicial action.[336] This explanation does not necessarily

332. *See* 50 U.S.C. §§ 1806(c-d), 1825(d-e) (2000); *see also supra* text accompanying note 74; Breglio, Note, *supra* note 4, at 180-81 (advocating ex post adversary proceedings to litigate the reasonableness of national security investigation, but crucially understanding the need for notice to all targets and the elimination of FISA restrictions review process).

333. Swire, *The System*, *supra* note 4, at 1352-68; *see also* Kreimer, *supra* note 19, at 172-81 (advocating a series of "prophylactic constraints," including improved need-to-know access controls on dissemination, audit trails on information use, expanded oversight, and continued use of sunset provisions and reauthorization).

334. *See* Swire, *The System*, *supra* note 4, at 1366-67; *see also* FBI OGC, *supra* note 54, at 2 ("In practice, the FISA Court has found general supervisory powers in this language, and its power to modify minimization procedures has been used as power to influence or control other aspects of investigations."); Banks, *supra* note 4, at 1187 (proposing that Congress grant the FISC rulemaking authority to develop rules of practice and procedure).

335. *See supra* notes 234-36 and accompanying text; *see also In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 623-27 (FISA Ct. 2002), *rev'd on other grounds, In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

336. Both the *Truong* court and the FISCR strongly caution against the invention of extra-statutory procedures by the courts. United States v. Truong, 629 F.2d 908, 914-15 n.4 (4th Cir. 1980) (explaining that the complexity of FISA suggests that the inexpert courts should leave the "intricate balancing" of developing standards for national security investigation to the political branches, rather than "enunciate an equally elaborate structure for core foreign intelligence surveillance under the guise of a constitutional decision" which would rigidly foreclose adjustment by the political branches); *Sealed Case*, 310 F.3d at 730 (stating that the FISA court's efforts to craft new minimization procedures lacked "any constitutional basis"); *id.* at 731 (stating that "the FISA court may well have exceeded the constitutional bounds that restrict an Article III court" by intruding into the internal operation of the Executive and the sphere of the Congress).

require jurisprudential calisthenics. National security investigation rests on a judicially created exception to normal Fourth Amendment procedures, and the use limit constitutes a method for determining and regulating the size and shape of that exception.

As the Court explained in *Keith*, any waiver of the normal Fourth Amendment standards could cause the Executive to "yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[337] The Court continued by stating that a "judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government."[338] Further, *Keith* explained that any exceptions to normal Fourth Amendment standards demanded careful delineation.[339] Accordingly, the use limit based on minimization represents no more than part of the normal robust judicial participation in evaluating reasonableness[340] as part of the system of checks and balances.[341]

G. Implications, Problems, and Issues

This Part of the Article describes a number of implications, problems, and issues arising from the proposed limit on the use of information unrelated to national security matters. The exact contours of these collateral issues depend enormously on the precise reasoning leading a court to adopt the use limit. Accordingly, the following subparts attempt only to sketch a few matters that merit consideration rather than provide precise guidance.

1. An Exigency Exception

To diminish the temptation that a court might refuse to apply the use limit because it would operate to block sharing of information critical to prevent death or serious harm, the rule should contain an exigency exception.[342] Under a proportionality

337. 407 U.S. 297, 317 (1972) (citation omitted).

338. *Id.*

339. *Id.* at 318.

340. *See* Amar, *supra* note 19, at 816-19 (proposing a series of reasonableness regimes to ensure proper exercise of Executive investigatory powers).

341. *See* Solove, *supra* note 10, at 1298.

342. This exception could take, as its pattern, the exception to the minimization of similar information acquired during an emergency investigation that never receives FISC approval. *See* 50 U.S.C. §§ 1801(h)(4), 1821(4)(D) (2000); *see also* AG Memo on Intelligence Sharing, *supra* note 72, at 5 (containing a similar emergency exception for United States Attorneys Offices that apparently conflicts with the statutory requirement of advance approval found in 50 U.S.C. §§ 1806(b), 1825(c)).

analysis, such an exception makes complete sense—although the invasion of privacy would remain the same, the seriousness of the offense and the importance of the information would escalate dramatically.

2. Exculpatory Information

In a similar vein, the use limit should make an exception for the dissemination of exculpatory information[343] under the various constitutional and statutory requirements that the Executive provide such evidence to defendants.[344] Two strands of analysis compel this result. First, affected individuals would, presumably, waive their privacy rights in order to have this information. Second, even if the privacy rights belong to someone other than the party desiring the exculpatory information, under a proportionality analysis, the weighing of the importance of the information would increase significantly, arguing powerfully in favor of disclosure despite the use limit.

3. Exclusion Beyond the Prosecution's Case-in-Chief

Dramatically, the use limit could serve as a vehicle for an expansion of the normal exclusionary rule, which currently operates fully only during the prosecution's case-in-chief in a criminal proceeding.[345] The Supreme Court has explained that its restriction of the exclusionary rule has rested on a calculation of its deterrent effect.[346] Exclusion during the prosecution's case-in-chief provided a powerful deterrent to police officers and traditional law enforcement. With national security investigation, however, the same analysis does not hold.

Criminal prosecution is certainly an important possibility in a national security investigation, but it is not the raison d'etre that it is for traditional law enforcement.[347] National security efforts seek to prevent threats, not just punish completed acts, and accordingly might work toward incapacitating a suspected terrorist by deporting that person.[348] Moreover, recent research reveals that the Executive,

343. *See* Schiff, *supra* note 226, at 35 (describing the challenges of producing exculpatory information under FISA).

344. *See* LAFAVE ET AL., *supra* note 155, § 24.3, at 1016 (explaining the range of requirements regarding exculpatory evidence).

345. *See* Penn. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 362-66, 364 n.4 (1998).

346. *See id.* at 363; INS v. Lopez-Mendoza, 468 U.S. 1032, 1041-50 (1984).

347. *See* Banks, *supra* note 4, at 1175-76 (describing the various programmatic uses of national security information and explaining that criminal prosecution constitutes only one distinct category of possible use).

348. *See In re* Sealed Case, 310 F.3d 717, 735-36 (FISA Ct. Rev. 2002) (noting the Executive's claim that it would achieve a national security purpose

in fact, rarely pursues counterterrorism targets through criminal charges relating to terrorism, preferring instead to prosecute for other offenses or, critically, to pursue immigration charges.[349] Accordingly, the deterrent calculus for national security investigation produces a dramatically different result.

Moreover, the logic of exclusion based on the minimization use limit works differently than exclusion under the criminal law. Under traditional criminal procedure, exclusion deters wrongful police conduct. The Constitution assumes as a baseline that law enforcement may investigate; deterrence focuses only on improper investigation. In the national security sphere, exclusion based on the use limit regulates the scope of the national security exception to the Fourth Amendment, rather than just deterring the pretextual use of FISA investigation. The constitutional baseline in this context rests at a much higher level; it assumes that no investigation may occur outside of the normal processes, and allows national security investigation only under tightly controlled circumstances. Accordingly, deterrence here regulates an exception to the norm, rather than the norm itself. To achieve that regulatory effect, deterrence in the national security context needs to focus on all investigation, not merely on improper ones.

Additionally, in the criminal universe, evidence of impropriety surfaces fairly easily through notice and the adversarial process. In the national security arena, only rare circumstances would produce evidence of pretext. The exception to the normal Fourth Amendment standards, as modulated by the use limit, must therefore presume a danger of pretext whenever the Executive seeks to use information unrelated to national security. The proposed use limit should result in a broader exclusionary rule that applies beyond the criminal case-in-chief. As such, this exclusionary rule should operate in a variety of administrative contexts that might entail the suppression of information, generally, rather than just "evidence."

by using FISA-acquired evidence of ordinary crime to incarcerate an agent of a foreign power in order to prevent espionage or terrorism); AG GUIDELINES, *supra* note 71, at 2 (describing the use of "measures to deal with threats to the national security[,]" including "excluding or removing persons involved in terrorism or espionage from the United States"); *supra* note 80 and accompanying text (describing the sharing of information with the Department of Homeland Security).

349. *See* Dan Eggen & Julie Tate, *U.S. Campaign Produces Few Convictions on Terrorism Charges*, WASH. POST, June 12, 2005, at A1; Mary Beth Sheridan, *Immigration Law as Anti-Terrorism Tool*, WASH. POST, June 13, 2005, at A1.

4. Degrading the Effectiveness of National Security Investigation?

If the use limit results in an exclusionary rule that applies outside the criminal case-in-chief and if the Executive routinely employs information unrelated to national security outside of that venue to incapacitate legitimate targets,[350] then the use limit could seriously undermine the effectiveness of national security investigation.

This situation may arise along several paths. For example, the Executive might employ FISA and investigate a suspected terrorist, gaining valuable but insufficient information to proceed against the individual criminally. At the same time, the Executive may have gained sufficient information to incapacitate the target through deportation on unrelated grounds (perhaps, a VISA violation) or prosecution for an unrelated crime (say, tax evasion). Alternately, the Executive may use FISA and investigate a suspected terrorist gaining little information that either confirms or dispels the suspicions, although it does reveal grounds for deportation or ordinary criminal prosecution. In an abundance of caution, the Executive pursues one of these routes.

In both these cases, the use limit would thwart legitimate uses of information nominally unrelated to national security. Asking the Executive to reveal its motivation could result in an entirely new layer of litigation and could force the exposure of intelligence sources and methods or could alert the target to the extent and true nature of the underlying FISA investigation. Admittedly, these matters could be resolved during the ex parte, in camera suppression hearing, but the result might tip the Executive's hand to the target. For example, if the Executive brought an immigration charge unrelated to national security against an individual, that person would seek suppression based on the use limit. If the Executive won the suppression motion, the individual would know that the Executive not only had used FISA, but actually obtained national security information about that individual.

In the end, these complications are similar, but less worrisome, than parallel problems encountered under the primary purpose test. Before the Patriot Act, defendants raised the primary purpose standard to defeat a criminal prosecution based on FISA information. Courts had to consider these claims even if the defendant faced charges related to terrorism. Under the use limit, courts would similarly need to weed out impermissible uses of FISA,

350. *See* Swire, *The System*, *supra* note 4, at 1361 (noting that "prosecution for crimes can lead to arrest and imprisonment" and that "incapacitation is a powerful tool to disrupt ongoing terrorist operations").

but only if the defendant faced charges unrelated to national security. Further, even with an added layer of litigation or with lost opportunities for incapacitation, the use limit's benefits may outweigh its costs.

5. Conflict with the Plain View Doctrine

One intractable problem with the proposed minimization-based use limit lies in its conflict with the plain view doctrine.[351] Essentially, the plain view doctrine allows the Executive to acquire information so long as it had a legal basis for being in a position to gain the information, the evidentiary value of the information was immediately apparent, and the Executive had a lawful right of access to the information.[352] In more colloquial terms, the plain view doctrine allows the Executive to gain "windfall" evidence. Accordingly, evidence of unrelated crime often qualifies for acquisition under the plain view doctrine, even if it might otherwise face minimization.[353]

Indeed, the plain view doctrine swallows much of the minimization principle.[354] Accordingly, for the proposed use limit to gain any traction, the plain view doctrine simply cannot apply normally to national security minimization.[355] Some logic, rather than just result-driven impulse, may support this conclusion. Criminal law enforcement must either acquire information or not; the dividing line is sharp and the legality is evaluated at the moment of acquisition. In this context, plain view takes place contemporaneously; it literally involves seeing or hearing at the scene. In contrast, during national security investigation, the Executive gathers information broadly, then analyzes it, retaining foreign intelligence information and disseminating it accordingly,

351. Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics,"* 7 HARV. J.L. & TECH. 239, 267 (1994) (describing the fundamental tension between minimization and plain view).

352. These three principles flow from *Minnesota v. Dickerson*, 508 U.S. 366 (1993) (describing the evidentiary value principle), *Horton v. California*, 496 U.S. 128 (1990) (describing the legal basis for gaining the information principle), and *Arizona v. Hicks*, 480 U.S. 321 (1987) (describing the right of access principle).

353. *See* United States v. Williams, 737 F.2d 594, 605-06 (7th Cir. 1984); United States v. Johnson, 539 F.2d 181, 188 & n.26 (D.C. Cir. 1976). Many courts and commentators have referred to the provisions in Title III, 18 U.S.C. § 2517(5), and FISA, 50 U.S.C. §§ 1801(h)(3), 1821(4)(C), that allow the use of unrelated evidence of crime as statutory plain view provisions. *See* Downes, *supra* note 351, at 254.

354. *See id.* at 278.

355. Alternately, the various prongs of the plain view doctrine might provide limited relief in a handful of cases. *See id.* at 269-78 (applying the various plain view tests to electronic communications to determine the sweep of the doctrine).

with minimization duties applying at each stage.[356] The Executive may gain information legally, but routinely need to relinquish it, or decline to use it, later. The process involves no contemporaneous, literal seeing or hearing at the scene. The national security universe routinely recognizes that legal acquisition does not translate into legal retention or use; such a framework does not normally apply to traditional criminal information gathering.[357]

This line of reasoning serves to highlight the fact that minimization, generally, and the proposed use limit, in particular, depart from the standard model under which lawful acquisition translates into lawful use.[358] Considering the emphasis placed on the principle of proportionality in the development of the proposed use limit, the idea of evaluating use based only on legal acquisition loses force in a national security context. Proportionality poses a weighing of privacy interests against the value of the information and the significance of the crime. This weighing will make sense often only at the time the Executive seeks to use evidence because only then will its importance come into focus.

Another distinction between the two contexts may also prove helpful. As explained, under normal criminal principles, investigation must happen and the Fourth Amendment must facilitate. No such parallel applies for national security investigation; that process enjoys a special exception from normal Fourth Amendment standards. Accordingly, its special status may dictate that other normal Fourth Amendment principles, such as the plain view doctrine, also recede. In the end, plain view and a use limit based on minimization cannot be reconciled. For the proposed use limit to function, plain view must give way. If that cannot happen, the idea of the use limit would have to be abandoned.

6. Salvaging the Unrelated Information by Dissipating the Taint

This Article may, so far, have overstated the deleterious effects of the use limit. If the use limit blocked the admission of evidence, the Executive could salvage the information it seeks to use through further investigation. Although, under the use limit, information obtained through FISA, but unrelated to national security, would constitute fruit of the poisonous tree, the Executive could purge the taint through an independent investigation that sufficiently severs

356. *See supra* notes 139, 298 and accompanying text.

357. *See supra* notes 298-301 and accompanying text.

358. *Cf.* Bradley, *supra* note 308, at 1036-37 (explaining the American emphasis on the question of whether the police broke the rules at the moment they acquired the evidence).

the nexus between the problematic acquisition of the information and the information's status at the time the Executive seeks to use it.[359] If the Executive learned during a national security investigation that a target engaged in immigration fraud, the Executive could launch a valid non-FISA investigation to obtain admissible evidence of that fraud. Crucially, the Executive would need to conduct the second inquiry from the ground up, without contravening the use limit and exploiting the original constitutional infirmity. Unless the original FISA investigation flagrantly sought unrelated information, a sufficiently patient independent investigation should purge the taint. The net result is that, even with the use limit blocking the admission of non-national security evidence from FISA, the Executive could gain the ability to introduce that evidence after a sufficiently independent investigation. Ultimately, the Executive ends up in no worse a position than if the use limit had never come into play.[360]

7. The "Standing" Problem

The success of the proposed use limit as a regulatory device, policing the parameters of the national security exception, may well depend on what is often inartfully referred to as Fourth Amendment "standing": an individual may assert a Fourth Amendment claim only if the Executive intruded on that person's privacy interests.[361] Accordingly, if the Executive acquires, through FISA, information about X's involvement in an ordinary crime, but obtains that information by intruding upon Y's privacy interests, then X cannot raise a Fourth Amendment claim and assert a violation of the minimization-based use limit.

Standing problems have arisen in FISA cases. For instance, in *United States v. Ott*,[362] the court weighed whether the defendant could challenge the Executive's minimization efforts with regard to others' conversations that incriminated him.[363] The court found that the defendant lacked standing because he enjoyed no privacy

359. In *Brown v. Illinois*, 422 U.S. 590 (1975), the Court detailed the standards for evaluating whether the Executive has purged the taint. *Id.* at 605. The Court focused on the flagrancy of the violation, the time lapse between the misconduct and the acquisition of the evidence, and the intervening circumstances. *Id.* at 603-04. And, as the Court explained in *Murray v. United States*, 487 U.S. 533 (1988), an independent investigation can also validate the admission of evidence otherwise contaminated by illegality. *Id.* at 537-40; *see also* Segura v. United States, 468 U.S. 796, 813-14 (1984).

360. *See* Nix v. Williams, 467 U.S. 431, 443 (1984).

361. *See* Rakas v. Illinois, 439 U.S. 128, 148-49 (1978).

362. 827 F.2d 473 (9th Cir. 1987).

363. *Id.* at 476.

interest in those conversations.[364]

Further, the Executive will manipulate the legal framework, legitimately, in order to gain an advantage. In *United States v. Duggan*,[365] for instance, the Executive acquired information against the defendant, a United States person, but not the target of the investigation.[366] Apparently, the Executive did not target Duggan because it wished to avail itself of the lower standard of probable cause available for investigations of non-United States persons, such as Duggan's accomplices.[367]

Accordingly, cases in which the use limit fails because a litigant lacks standing allow the national security exception to expand elastically. This possibility creates incentive for the Executive to manipulate FISA investigation, as in *Duggan*, to avoid the ambit of the use limit. One response might be to accept this lack of uniformity—some defendants get prosecuted based on information unrelated to national security, while others do not—as a natural product of a Fourth Amendment jurisprudence resting on privacy. The problem lies in the pressing need to confine the Executive's use of the power to conduct FISA investigation in the vacuum created by the national security exception.

The only general solution lies in the possibility of special standing rules for the use limit.[368] Although the test used in *Alderman v. United States*[369] suggests some balancing of the benefits of extending the exclusionary rule against the public costs,[370] the Court has subsequently clarified that Fourth Amendment privacy is a personal right and cannot be asserted vicariously.[371] Of course, if Congress added a minimization provision to FISA that paralleled the proposed use limit, an aggrieved person could raise a statutory, rather than constitutional claim. Otherwise, this line of concern may just dead-end, leaving the scope of the national security exception under-enforced in cases that present standing problems.[372]

364. *Id.*
365. 743 F.2d 59 (2d Cir. 1984).
366. *Id.* at 78-79.
367. *Id.*
368. One possibility lies in the concept of "target" standing—anyone targeted by the Executive possesses standing to raise a Fourth Amendment claim, even if that claim attempts to vicariously vindicate someone else's privacy rights. *But see* Rakas v. Illinois, 439 U.S. 128, 132-34 (1978) (considering, but rejecting target standing); United States v. Payner, 447 U.S. 727, 731-35 (1980) (same).
369. 394 U.S. 165 (1969).
370. *Id.* at 175-76 (rejecting an elimination of the standing requirement).
371. *Rakas*, 439 U.S. at 133-34.
372. Conceivably, some claimants may have success avoiding the standing limits by reframing the issue as a First Amendment claim alleging a chilling effect. *See* Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 150-51 (D.D.C. 1976).

8. The Third-Party Problem

A similar dead end looms large—the use limit would do nothing to address the various tools for gathering information from third parties. These methods of investigation fall outside the sweep of the use limit because they do not affect the privacy rights of the subject.[373] Recall, moreover, that these tools contained purpose limits before the Patriot Act only as a matter of statutory law.[374] It would be difficult, therefore, for a court to import the use limit into this area, despite the need for such regulation. Indeed, although these tools pose fewer dangers of pretext—because they more closely resemble their criminal cousins—they pose extraordinary dangers to privacy and present dramatic incentives for mission creep.[375] As with standing, only legislation can solve the problem.

VII. CONCLUSION

Ultimately, the question is whether a minimization-based limit on the use of information unrelated to national security would effectively regulate the national security exception, deter pretextual use of national security investigation, prevent the erosion of privacy, and retard mission creep. The use limit would overachieve in some regards and underperform in other areas.[376]

The use limit would over-deter frequently because it would result in the loss of unrelated information even when the Executive acted without pretext. This over-deterrence makes sense only if it significantly props up privacy by limiting Executive intrusions or by instilling public confidence and preventing the inhibiting effects of surveillance from lessening autonomy. On the other hand, the use limit will under-deter markedly in cases that present standing problems and in the entire area of third party investigation. More fundamentally, it will under-deter because it will apply only if the Executive acquires and wishes to use unrelated evidence; it would not prevent the Executive from exploiting a pretextual search that found information related to national security.

As with the traditional exclusionary rule, the use limit would entail demoralization costs and judicial skewing.[377] Additionally, the use limit fails to line up neatly with the substantive goals of criminal law, national security, or privacy.[378] It would let the guilty

373. *See supra* note 263 and accompanying text.
374. *See supra* notes 92, 103, 117, 264 and accompanying text.
375. *See supra* notes 22-27 and accompanying text.
376. *See* Amar, *supra* note 330, at 1136-38 (analyzing competing Fourth Amendment regulatory regimes based on their over- and under-deterrent effects).
377. *See supra* notes 329-31 and accompanying text.
378. *See* Amar, *supra* note 330, at 1139 ("Criminal procedure must work to

go free, make national security efforts less effective, and would still allow significant intrusions on privacy. Indeed, the shortcomings of the use limit should stand as a cautionary tale to any court contemplating constitutional approval of the current system of national security investigation. Of course, statutory or administrative reform could solve the problems resulting from upholding FISA, but a court cannot speculate about actions by the political branches when it weighs the constitutionality of the national security investigation system.

Nevertheless, while the use limit is far from perfect, it achieves a number of objectives: replacing the primary purpose test; protecting privacy; ensuring an important judicial role; and deterring abuse. Any court weighing the constitutionality of FISA should understand the ability of the use limit to serve as an important means of constitutional regulation. Unless scholars, litigators, or the courts themselves can develop superior alternative methods of constitutional regulation for national security investigation, the courts have three options: refuse to uphold the current scheme in favor of retaining the primary purpose test; uphold the current scheme without the use limit and leave the various resultant deficiencies unaddressed; or uphold FISA, as amended by the Patriot Act, and recognize, either immediately or when a suitable case arises, a minimization-based use limit on information unrelated to national security as a necessary regulating device.

vindicate rather than undermine sensible norms of substantive criminal law.").