VANDERBILT LAW REVIEW

VOLUME 66 OCTOBER 2013 NUMBER 5

The Fourth Amendment's National Security Exception: Its History and Limits

*L. Rush Atkinson**

* U.S. Department of Justice, National Security Division. A.B., University of Chicago; M.Phil., University of Cambridge; J.D., New York University. For suggestions and guidance, I am grateful to Barry Friedman, Sam Rascoff, Trevor Morrison, Emily Berman, Jon Gannon, Stu Evans, Nick Lyon, Margot Pollans, Matt Lawrence, Michael Pollack, and Jessica Collins. For assistance with historical sources, I am indebted to Tim Nenniger and Christina Jones at the National Archives; John Fox at the FBI; and John Jacob at the Lewis F. Powell, Jr. Archives at Washington and Lee University. A portion of this Article was completed while the author served as a fellow at the Center for the Administration of Criminal Law at New York University School of Law. This Article has been cleared for prepublication review pursuant to 28 C.F.R. § 17.18 (2013). The views expressed here are the author's personal opinion and do not necessarily reflect those of the Justice Department or the federal government. Nothing in this Article should be construed as implying U.S. government authentication of information.

I. INTRODUCTION

Since 2001, federal prosecutors have indicted and convicted hundreds of defendants for terrorism, espionage, and other national

security crimes.[1] And for every prosecution, there are dozens of investigations into foreign threats that never result in a trial. Between 2001 and 2010, for example, the federal government obtained 16,306 foreign intelligence warrants in the course of its security operations.[2] Between 2004 and 2011, the Federal Bureau of Investigations ("FBI") issued 119,192 National Security Letters for records deemed to be pertinent to national security investigations.[3]

Despite these numbers, security investigations and prosecutions proceed on uncertain constitutional footing. The rights of terrorism suspects to receive *Miranda* warnings,[4] confront accusers,[5] and obtain civilian trials are unclear.[6] Similar constitutional questions surround the Fourth Amendment and its application to national security matters. The balance between the Fourth Amendment's protections and the President's inherent power to defend the nation

---

1. *See, e.g.*, David S. Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SECURITY L. & POL'Y 1, 14 & n.47 (2011) ("Since 9/11, the DOJ has convicted hundreds of defendants as a result of terrorism-related investigations."); CTR. ON LAW & SECURITY, N.Y. UNIV. SCH. OF LAW, TERRORIST TRIAL REPORT CARD 4 (2010), *available at* http://www.lawandsecurity.org/Portals/0/documents/01_TTRC2010Final1.pdf (calculating 998 indicted defendants in terrorism-related prosecutions); U.S. DEP'T OF JUSTICE, SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES (2012) (identifying over 250 cases of export and espionage cases between 2007 and 2012); Letter from Ronald Weich, Assistant Att'y Gen., U.S. Dep't of Justice, to Senators Patrick Leahy and Jeff Sessions 1 (Mar. 26, 2010) (on file with author) (citing conviction of over 400 international terrorism defendants between 2001 and 2010).

2. *See* ELEC. PRIVACY INFO. CTR., FOREIGN INTELLIGENCE SURVEILLANCE ACT COURT ORDERS 1979–2012 (May 4, 2012), *available at* http://epic.org/privacy/wiretap/stats/fisa_stats.html (compiling statistics based on annual Justice Department reports to Congress). In 2011 alone, the government obtained 1,745 orders. *Id.*

3. *Id.* National Security Letters, authorized under a variety of statutes, function in most cases like administrative subpoenas, allowing authorized law enforcement to access certain identified types of information. *See* CHARLES DOYLE, CONGR. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT AMENDMENTS 5 tbl.1 (2010), *available at* http://www.fas.org/sgp/crs/intel/RS22406.pdf (summarizing different National Security Letter statutes).

4. Charlie Savage, *Holder Backs a* Miranda *Limit for Terror Suspects*, N.Y. TIMES, May 9, 2010, at A1 (reporting proposal to "carv[e] out a broad new exception to the Miranda [sic] rights" in terrorism cases); *see also* Ryan T. Williams, *Stop Taking the Bait: Diluting the* Miranda *Doctrine Does Not Make America Safer from Terrorism*, 56 LOY. L. REV. 907 (2010).

5. *See, e.g.*, United States v. Abu Ali, 528 F.3d 210, 238–41 (4th Cir. 2008) (holding Sixth Amendment permits admission of video testimony by Saudi intelligence officials against defendants); John Scott, *"Confronting" Foreign Intelligence:* Crawford *Roadblocks to Domestic Terrorism Trials*, 101 J. CRIM. L. & CRIMINOLOGY 1039, 1058–72 (2011) (exploring Confrontation Clause's role in national security matters).

6. *See, e.g.*, Neal K. Katyal & Laurence H. Tribe, *Waging War, Deciding Guilt: Trying the Military Tribunals*, 111 YALE L.J. 1259, 1260 (2001) (arguing elements of tribunals are "flatly unconstitutional").

has become a focus of litigation in recent years yet still remains murky.[7]

To clarify the constitutional parameters of national security investigations, this Article examines the Fourth Amendment's historical influence in security affairs.[8] Claims about historical practice pervade debates over modern surveillance programs, including those about the Bush Administration's warrantless wiretapping program and recent amendments to the Foreign Intelligence Surveillance Act ("FISA"). These historical treatments remain cursory, however,[9] and have failed to detail how the Fourth Amendment regulated national security operations in the pre–September 11 era.

Archived materials reveal that the federal government has long embraced the notion that national security constitutes an exception to the traditional rules of the Fourth Amendment. Starting at the end of World War II, federal agents investigating security cases began to conduct warrantless electronic surveillance and physical searches on the theory that a national security exception permitted this otherwise unconstitutional conduct.[10] During the Cold War, leaders in the White House and Justice Department relied on this same exception to authorize aggressive surveillance of suspected foreign threats.[11] Tentative support from the judiciary in the late 1960s and 1970s encouraged greater national security surveillance, in many cases beyond the ordinary constitutional bounds imposed on law enforcement.[12]

The national security exception, however, by no means gave federal agents carte blanche investigatory power. Well into the 1970s, the executive branch assumed that the national security exception permitted only, in the words of FBI Director J. Edgar Hoover, "purely

---

7. *See* Paul Ohm, *The Argument Against Technology-Neutral Surveillance Laws*, 88 TEX. L. REV. 1685, 1704 (2010) (noting unanswered questions about how "Fourth Amendment appl[ies] to national security investigations"); *see also infra* Part I.B.

8. To date, more academic attention has been dedicated to the separation of powers questions implicated in national security investigations. *See, e.g.*, Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1029 (2008) (considering separation of powers relevance of Roosevelt administration practice). This Article, however, focuses on a different question: the constitutionality of executive conduct vis-à-vis the Fourth Amendment. That question is sufficiently distinct that it deserves its own treatment.

9. *See infra* Part II.C.

10. *See infra* Part III.A.

11. *See infra* Part III.B.

12. *See infra* Part III.C.

intelligence" focused investigations.[13] This "pure intelligence" rule meant that evidence gleaned from warrantless searches and surveillance was constitutionally inadmissible in subsequent prosecutions—a limitation with important ramifications. On various occasions, prosecutors concluded that the Fourth Amendment barred the admission of evidence gleaned or derived from security investigations at trial. Prosecutors elected not to present such information; as a result, spies and foreign agents escaped conviction, despite clear evidence of wrongdoing.[14]

Commentators who fail to identify the limits of these early investigations overemphasize the government's power to investigate foreign threats at the expense of liberty interests or, instead, dismiss this period as lawless and irrelevant for purposes of legal precedent. In reality, a clear legal framework regulated the scope of national security investigations, and records reveal a palpable *opinio juris*—a sense of legal obligation—that governed the constitutional boundaries of security operations. This Article, contrary to some contemporary assertions, shows that the Fourth Amendment played a pronounced, restrictive role in early national security investigations, even in the face of grave security risks.[15]

The history described in this Article also bears directly on lawsuits challenging the government's newest national security surveillance programs, including the Supreme Court's recent case of *Clapper v. Amnesty International USA*.[16] As explained below, civil litigation has been stalled by the apparent fact that the government has not used data collected from these surveillance programs in subsequent criminal prosecutions.[17] While this issue has only been

13. Memorandum from J. Edgar Hoover, Dir., FBI, for Attorney Gen. J. Howard McGrath (Oct. 6, 1951), *in* ATHAN THEOHARIS, FROM THE SECRET FILES OF J. EDGAR HOOVER 137 (Ivan R. Dee, Inc. 1993).

14. *See, e.g.*, *infra* Parts III.A.2, III.B.2.

15. *See, e.g.*, BRUCE FEIN, CONSTITUTIONAL PERIL 121 (Palgrave Macmillan 2008) (arguing that early surveillance was not limited by "executive scruples about invading privacy or the Fourth Amendment"); Matthew A. Anzaldi & Jonathan W. Gannon, In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: *Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance*, 88 TEX. L. REV. 1599, 1601 (2010) ("For much of the nation's history, the Executive Branch exercised largely unchecked discretion in gathering foreign intelligence."); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19 (2008) (arguing that "courts have largely debilitated the Fourth Amendment to meet the demands of . . . the National Security State"); William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099, 1104 (2007) (arguing that the "Fourth Amendment did not impose any obstacles to electronic surveillance" before 1967).

16. 133 S. Ct. 1138, 1142–43 (2013).

17. *See infra* Part IV.B.

discussed in the context of procedural matters—particularly standing—this Article notes that it has substantive significance as well. Limiting the use of collected information to nonprosecutorial purposes strengthens the government's claim that its conduct to date has complied with the Fourth Amendment by establishing a practice parallel to the restraints imposed upon the early security investigations. Even if the government never formally acknowledges this limitation, the empirical evidence indicating restraint (i.e., the vast amount of intelligence collected versus the marginal amount used at trial) should assure courts that these new programs have not eroded historical protections.

This Article proceeds as follows. Part II summarizes national security investigations, pending Fourth Amendment issues, and the legal relevance of the executive's historical practices. Part III explores the legal framework for earlier national security investigations, focusing on the period between the end of World War II and the passage of FISA in 1978. Specifically, Part III explains the origins of the national security exception, the limits placed on this exception (particularly the pure intelligence rule) and the consequences of those limits (most notably, failed prosecutions). Part IV evaluates the legal and policy merits of the pure intelligence paradigm and juxtaposes early practice with that of modern surveillance programs.

II. SECURITY INVESTIGATIONS AND FOURTH AMENDMENT QUESTIONS

Before assessing the historical record, this Article first provides a background on national security investigations, the current debates about their Fourth Amendment limits, and the relevance of history to these debates.

A. The Unique Paradigm of National Security Investigations

National security investigations, as defined by federal guidelines, mainly involve three types of threats: (1) "[i]nternational terrorism," (2) "[e]spionage and other intelligence activities, sabotage, or assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons," and (3) "[f]oreign computer intrusions."[18]

18. U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 7 (2008) [hereinafter A.G. GUIDELINES]; *see also* U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION (U) 6–7 (2003). Previously, the government defined "national security investigations" broadly in order to take advantage of the leeway afforded such operations. At times, executive officials classified inquiries into organized crime, kidnappings, and political

Federal practice governs national security investigations because they share unique operational considerations not present in traditional crime scenarios.[19] These practical differences also require that security investigations receive distinct legal treatment from traditional law-enforcement investigations.

Law enforcement's ultimate goal, for example, is almost always prosecution. Investigations might have other objectives—interdiction of drugs, retrieving stolen property, and so on—but agents generally envision convicting wrongdoers.[20] For security investigations, however, the likelihood of prosecution remains remote.[21] Political issues—a terrorism financier's presence overseas, a spy's diplomatic immunity, among others—inhibit prosecutions.[22] Operational factors

---

dissidence as "security" investigations. *See, e.g.*, *The National Security Agency and Fourth Amendment Rights: Hearing on S. Res. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 69 (1975) (statement of Edward Levi) [hereinafter Levi, *Church Committee Testimony*], *available at* http://www.intelligence.senate.gov/pdfs94th/94intelligence_activities_V.pdf (noting "internal security or national safety" expanded to include "organized crime, kidnappings[,] and matters wherein human life might be at stake"). Officials later jettisoned these broader terms after the Supreme Court clarified that investigations into domestic threats (i.e., those not involving "foreign powers or their agents") could not invoke the national security exception. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 309 n.8 (1972).

19. The national security exception generally involves federal, not local, investigations. In *United States v. Ehrlichman*, the D.C. Circuit held "the 'national security' exemption can only be invoked if there has been a specific authorization by the President, or by the Attorney General . . . for the particular case." 546 F.2d 910, 925 (D.C. Cir. 1976). However, local law enforcement, of course, plays a critical role in national-security cases. Samuel J. Rascoff, *The Law of Homegrown (Counter)Terrorism*, 88 TEX. L. REV. 1715, 1716 (2010) ("[L]ocal police have once again emerged as a significant constituency in discussions of national security."); Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289, 296 (2012) (describing "expansion of subfederal roles" in counterterrorism efforts). While local efforts often operate under certain other Fourth Amendment exceptions, these exemptions are distinct from the broader national security exception. *See, e.g.*, City of Indianapolis v. Edmonds, 531 U.S. 32, 44 (2000) (suggesting "appropriately tailored roadblock set up to thwart an imminent terrorist attack" would be constitutional); *cf.* Ferguson v. City of Charleston, 532 U.S. 67, 83 n.21 (2001) (noting checkpoint searches are a distinct subset of searches due to reduced expectation of privacy).

20. This generalization has exceptions. *See* Herman Goldstein, *Confronting the Complexity of the Policing Function*, *in* DISCRETION IN CRIMINAL JUSTICE 49–50 (Lloyd E. Ohlin & Frank J. Remington eds., 1993) (describing Chicago police practice of arresting gang members with "no intention to prosecute").

21. *See* H.R. Rep. No. 95-1283, pt. 1, at 36 (1978) ("Prosecution is one way, but only one way and not always the best way, to combat [foreign threats]."); JOHN EARL HAYNES & HARVEY KLEHR, EARLY COLD WAR SPIES 15 (Cambridge Univ. Press 2006) (noting conviction "is only one of the motivations of spy chasers, and not a very important one"); William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 5 (2000) ("It is neither the objective nor the likely result that the target of a foreign intelligence . . . search will be criminally prosecuted.").

22. *See* Nathaniel P. Ward, *Espionage and the Forfeiture of Diplomatic Immunity*, 11 INT'L LAW. 657, 658–59 (1977) (describing spies under diplomatic cover); Darren S. Tucker, Comment,

also affect the calculus. Public trials risk exposing covert assets,[23] and co-opting a spy may be more useful than jailing her.[24] Such considerations are not absent from traditional criminal investigations, but they arise in spades in security matters.

More broadly, security investigations are not necessarily premised on suspicion of criminal activity. Justice Department guidelines explain that such operations are "not limited to 'investigations' in the narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes . . . ."[25] These broader purposes include diplomatic, military, and other foreign policy objectives. Security investigations, therefore, are often "undertaken simply to obtain information on the intentions, capabilities, and activities of those able to harm the United States," rather than for prosecution.[26]

Finally, security threats involve much greater potential costs than everyday criminal enterprises. The costs of international terrorism are obvious, as are those of espionage leading to the loss of military and nuclear secrets.[27] The United States also loses billions of dollars to state-sponsored economic espionage and cyberattacks.[28] While the Fourth Amendment traditionally operates "transsubstantively"—applying the same rules regardless of the

---

The Federal Government's War on Economic Espionage, 18 U. PA. J. INT'L ECON. L. 1109, 1149 (1997) (noting how diplomatic immunity complicates counterespionage).

23. *See* SERRIN TURNER & STEPHEN J. SCHULHOFER, THE SECRECY PROBLEM IN TERRORISM TRIALS 4 (2005), *available at* http://www.brennancenter.org/sites/default/files/legacy/publications/20050000.TheSecrecyProbleminTerrorismTrials.pdf ("The central challenge in using any intelligence as evidence is finding a way to do so without burning extant intelligence assets.").

24. *See, e.g.*, Funk, *supra* note 15, at 1105 n.30 (noting the FBI arrested Soviet spy Rudolf Abel "only after failing to 'double' him").

25. A.G. GUIDELINES, *supra* note 18, at 16.

26. Funk, *supra* note 15, at 1105.

27. *See, e.g.*, Jason Bram et al., *Measuring the Effects of the September 11 Attack on New York City*, FRBNY ECON. POL'Y REV., Nov. 2002, at 5, 5 (estimating 2001 World Trade Center attacks caused between $33 and $36 billion in property damage, $21.6 billion in clean-up costs, between $3.6 and $6.4 billion lost to city industries, and $7.8 billion in decreased workers' prospective lifetime earnings).

28. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-666T, CYBERSECURITY: THREATS IMPACTING THE NATION 1 (2012) (noting "sustained cyber attacks . . . could have a potentially devastating impact on federal and nonfederal systems"). *See generally* KRISTIN M. FINKLEA & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT (2013) (surveying types of cyberattacks and recent cost estimates).

suspected crime—this approach has been tested since the September 11 attacks.[29]

For these reasons and others, national security investigations are sufficiently unique for courts and executives to treat them differently from run-of-the-mill law-enforcement operations. This distinction has required developing a separate legal framework to govern national security investigations: one that can accommodate special governmental interests while honoring constitutional guarantees.

B. The Current Uncertainty About Security Investigations

The growth of national security investigations has spurred new Fourth Amendment challenges to government conduct. Defendants facing terrorism- or espionage-related charges have objected to the procedures by which the government collected its evidence.[30] Concerned citizens have brought civil lawsuits claiming that the government transgressed Fourth Amendment bounds.[31] Corporations have lodged other Fourth Amendment complaints when the government sought to compel their assistance during national security investigations.[32]

Many of these suits challenged amendments to the statutory scheme regulating security surveillance, the centerpiece of which is FISA.[33] The USA PATRIOT Act of 2001, which expanded FISA's coverage, has been subject to dozens of separate challenges.[34] Though

---

29. *See* William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2146 (2002) [hereinafter Stuntz, *Policing After the Terror*]; *see generally* William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842 (2001) [hereinafter Stuntz, *Transsubstantive Fourth Amendment*].

30. *See, e.g.*, *infra* notes 34 and 270 (listing challenges by defendants).

31. *See, e.g.*, Amnesty Int'l USA v. Clapper, 638 F.3d 118, 121 (2d Cir. 2011) (considering a challenge to section 702 of the Foreign Intelligence Surveillance Act of 1978); ACLU v. NSA, 493 F.3d 644, 648–49 (6th Cir. 2007) (considering a challenge to the NSA operation known as the Terrorist Surveillance Program).

32. *See, e.g.*, John Doe, Inc. v. Mukasey, 549 F.3d 861, 864 (2d Cir. 2008) (challenging use of National Security Letters); *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1007–08 (FISA Ct. Rev. 2008) (considering challenge to directives issued "assist in warrantless surveillance of certain customers").

33. 50 U.S.C. §§ 1801–85 (2012).

34. *See, e.g.*, United States v. Duka, 671 F.3d 329, 333 (3d Cir. 2011); United States v. El-Mezain, 664 F.3d 467, 563 (5th Cir. 2011); United States v. Abu-Jihad, 630 F.3d 102, 117 (2d Cir. 2010) (listing Fourth Amendment challenges); United States v. Stewart, 590 F.3d 93, 99 (2d Cir. 2009); United States v. Campa, 529 F.3d 980, 993 (11th Cir. 2008); United States v. Daly, 243 F. App'x 302, 306 (9th Cir. 2007) (unpublished); United States v. Damrah, 124 F. App'x 976, 980 (6th Cir. 2005) (unpublished); United States v. Hammoud, 381 F.3d 316, 331 (4th Cir. 2004); United States v. Medunjanin, No. 10-CR-19-1(RJD), 2012 WL 526428, at *1 (E.D.N.Y. Feb. 16,

most decisions affirm the PATRIOT Act's constitutionality, they have not been unanimous. Two courts have concluded the Act violated the Fourth Amendment,[35] and others have voiced their concern that the Act's new standard "violates the Fourth Amendment."[36]

But FISA is not the only target of Fourth Amendment challenges. After public disclosure of the Bush Administration's Terrorist Surveillance Program, which involved warrantless surveillance initiated outside of the FISA framework and done without judicial approval,[37] the ACLU challenged the program's constitutionality.[38] The judiciary has likewise scrutinized the government's use of material witness warrants[39] after the September 11 attacks. In one recent civil suit, *Ashcroft v. al-Kidd*, three Justices noted that the plaintiff's extended and invasive detention was "a grim reminder of the need to install safeguards against disrespect for human dignity, constraints that will control officialdom even in perilous times."[40]

2012); United States v. Alwan, No. 1:11–CR–13–R, 2012 WL 399154, at *1 (W.D. Ky. Feb. 7, 2012); United States v. Mahamud, 838 F. Supp. 2d 881, 884 (D. Minn. 2012); United States v. Mehanna, No. 09-10017-GAO, 2011 WL 3652524, at *1 (D. Mass. Aug. 19, 2011); United States v. Sherifi, 793 F. Supp. 2d 751, 752 (E.D.N.C. 2011).

35. Mayfield v. United States, 504 F. Supp. 2d 1023, 1042 (D. Or. 2007) ("Therefore, I conclude that 50 U.S.C. §§ 1804 and 1823, as amended by the Patriot Act, are unconstitutional."), *vacated by* 599 F.3d 964, 970 (9th Cir. 2009); *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 625 (FISA Ct.) (amending minimization procedures under FISA), *abrogated by In re* Sealed Case, 310 F.3d 717, 736–37 (FISA Ct. Rev. 2002).

36. United States v. Warsame, 547 F. Supp. 2d 982, 996–97 (D. Minn. 2008); *see also* United States v. Islamic Am. Relief Agency, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *8 (W.D. Mo. Dec. 21, 2009) ("Without deciding whether the 'significant purpose' test violates the Defendants' Fourth Amendment rights, the Court finds, even if the primary purpose test applies, it is satisfied in this case."). The PATRIOT Act expanded FISA's scope by allowing the government to seek FISA warrants whenever "foreign intelligence information"—that is, information about foreign threats—was a "significant" purpose. 50 U.S.C. § 1803. Prior to the amendment, FISA had been understood to only apply to cases where the "primary" purpose of the investigation was foreign intelligence information, thereby restricting its use in cases where prosecutions was a likely outcome. *See* Cedric Logan, Note, *The FISA Wall and Federal Investigations*, 4 N.Y.U. J.L. & LIBERTY 209 (2009).

37. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

38. ACLU v. NSA, 493 F.3d 644, 648–49 (6th Cir. 2007).

39. Material witness statutes allow the detention of a person considered to be "material" to a criminal proceeding. 18 U.S.C. § 3144.

40. Ashcroft v. al-Kidd, 131 S. Ct. 2074, 2089 (2011) (Kennedy, J., concurring). Though al-Kidd's claim against the Attorney General was dismissed on qualified immunity grounds, a district court judge permitted lawsuits against two officers responsible for obtaining the material witness warrant to continue. al-Kidd v. Gonzales, No. 1:05-cv-00093-EJL-MHW, 2012 WL 4470776 (D. Id. Sept. 27, 2012).

Legal challenges to new surveillance programs continue to this day,[41] and questions about the Fourth Amendment's role in national security abound.[42] As one former Assistant Attorney General for National Security acknowledged: "Although the courts have agreed that the executive branch has a right to conduct surveillance and searches for foreign intelligence purposes, developments . . . have not substantially clarified the nature or scope of that right."[43]

C. The Constitutional Gloss of Early Executive Practice

To help address the uncertainty surrounding security investigations, this Article surveys the historical boundaries of such operations. The history examined here primarily involves executive conduct, which can carry precedential weight in matters of constitutional law.[44] In *Youngstown Sheet & Tube Co. v. Sawyer*, Justice Frankfurter explained in his concurrence how executive practice informs our constitutional understanding:

> [A] systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on "executive Power" vested in the President by §1 of Art. II.[45]

Subsequent Supreme Court decisions have embraced the probative value of longstanding executive practice.[46]

When identifying the constitutional parameters of the executive's power, historical moments of restraint are particularly instructive. When congressional prohibition draws executive power to its "ebb," for example, one can identify the executive's core inextinguishable powers.[47] Constitutional boundaries are similarly discernible in some cases where the executive branch limits its own

---

41. *See infra* Part IV.B.2.

42. For an overview of some constitutional issues raised by new surveillance programs, see William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1240–74 (2007).

43. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 3.9 (Thomson/West Publ'g 2007).

44. *See* Michael J. Gerhardt, *Non-Judicial Precedent*, 61 VAND. L. REV. 713, 715 (2008) ("[N]on-judicial actors produce precedents that are more pervasive than those made by courts in constitutional law.").

45. 343 U.S. 579, 610–11 (1952) (Frankfurter, J., concurring).

46. *See* Medellín v. Texas, 552 U.S. 491, 531 (2008) (citing "executive gloss" theory); Dames & Moore v. Regan, 453 U.S. 654, 686 (1981) (same).

47. *See* David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—A Constitutional History*, 121 HARV. L. REV. 941 (2008) (examining significance of legislative restraints on president's war powers); *see also Youngstown*, 343 U.S. at 635–38 (Jackson, J., concurring) (providing famous triptych-of-presidential-power theory).

conduct.[48] Specifically, the executive's self-restraint is precedential when it stems from a sense of constitutional obligation.[49] Such executive branch fealty toward the Constitution might be unprompted by a coordinate branch's action, so there may be no record as evident as a judicial opinion or legislative bill. Nevertheless, where a discernible *opinio juris* shapes executive action, we should consider such legal opinion both for its persuasive power and for its reflection of historical understandings about what protections the Constitution establishes.[50]

Historical conduct is particularly important in the national security context. "National security law and foreign affairs law," Julian Mortenson explains, have a "pronounced concern for post-enactment history as a source of constitutional meaning."[51] Neil Katyal and Richard Caplan note that "[i]n the crucible of legal questions surrounding war and peace, few judicial precedents will provide concrete answers," making executive practice one of the few constitutional guides.[52]

Accordingly, commentators and government officials have deployed the historical record in defending or challenging the constitutionality of national security investigations implemented in the wake of the September 11 attacks. For example, when its warrantless surveillance program became public in 2005, the Bush Administration relied on historical precedent to defend its conduct. "[I]t has long been recognized that the President has the authority to use secretive means to collect intelligence necessary for the conduct of foreign affairs and military campaigns," Attorney General Alberto

---

48. This topic is now receiving an increasing amount of scholarly attention. *See generally* Curtis A. Bradley & Trevor W. Morrison, *Presidential Power, Historical Practice, and Legal Constraint*, 113 COLUM. L. REV. 1097 (2013) (discussing executive reference to historical practice as guide to limits on own power).

49. Of course, not all cases of executive restraint indicate constitutional parameters; political, prudential, moral, and other considerations may govern conduct.

50. *Opinio juris* is a notion much more commonly discussed in relation to international law. For example, that the customary practice of states cannot have legal force without evidence that such practice is driven by a conviction that the law requires such conduct is a widely held notion. *See, e.g.*, ANTONIO CASSESE, INTERNATIONAL LAW 156 (Oxford Univ. Press, 2d ed. 2005). In the domestic constitutional setting, evidence of *opinio juris* is not necessarily required for executive restraint to amount to constitutional "gloss," but such evidence makes the underlying practice more poignant.

51. Julian Davis Mortenson, *Executive Power and the Discipline of History*, 78 U. CHI. L. REV. 377, 378 (2011) (reviewing JOHN YOO, CRISIS AND COMMAND: THE HISTORY OF EXECUTIVE POWER FROM GEORGE WASHINGTON TO GEORGE W. BUSH (Kaplan Publ'g 2009); JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR (Atlantic Monthly Press 2006); and JOHN YOO, THE POWERS OF WAR AND PEACE: THE CONSTITUTION AND FOREIGN AFFAIRS AFTER 9/11 (Univ. of Chicago Press 2006)).

52. Katyal & Caplan, *supra* note 8, at 1024.

Gonzales urged. "Wiretaps for such purposes thus have been authorized by Presidents at least since the administration of Franklin Roosevelt in 1940."[53] Similarly, the Justice Department has defended legislative amendments to FISA by citing past practice. "From the beginning of the 20th Century, the United States conducted warrantless electronic surveillance for the purpose of protecting national security from foreign threats," the government's brief stated in a case challenging the PATRIOT Act's amendments to FISA.[54]

These historical accounts, however, have gone largely unvetted, and the historical record is often misinterpreted due to the absence of context. To illustrate, consider one of the main pieces of evidence cited in debates about recent government surveillance programs and alluded to by Attorney General Gonzalez in his statement quoted above: an executive memorandum authored by Franklin Roosevelt in May 1940.[55] In this memorandum, Roosevelt "authorized and directed" Attorney General Robert Jackson to permit federal officers to wiretap "conversation[s] or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies."[56] While Roosevelt's 1940 memorandum certainly set a precedent for the use of wiretapping in national security investigations, present-day commentators overlook the memorandum's legal and historical context.[57] When Roosevelt issued

53. Letter from Attorney Gen. Alberto R. Gonzales to Senator William H. Frist 7 (Jan. 19, 2006), *available at* http://www.usdoj.gov/ag/readingroom/ surveillance9.pdf; *see also* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 7 (2006), *available at* http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf ("[A] consistent understanding has developed that the President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. Wiretaps for such purposes thus have been authorized by Presidents at least since the administration of Franklin Roosevelt in 1940."); Letter from William E. Moschella, Assistant Att'y Gen., U.S. Dep't of Justice, to Senate and Permanent Select Comms. on Intelligence 3 (Dec. 22, 2005), *available at* http://www.epic.org/privacy/terrorism/fisa/nsaletter122205.pdf ("Presidents have long exercised the authority to conduct warrantless surveillance for national security purposes . . . .").

54. Supplemental Brief for the United States, *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001), *available at* http://www.fas.org/irp/agency/doj/fisa/092502sup.html.

55. Letter from Attorney Gen. Alberto R. Gonzales to Senator William H. Frist, *supra* note 53, at 7; *see also* U.S. DEP'T OF JUSTICE, *supra* note 53, at 6–10 (chronicling warrantless surveillance under Presidents Roosevelt, Truman, and Johnson).

56. Memorandum from President Franklin D. Roosevelt for Attorney Gen. Robert Jackson 2 (May 21, 1940), *reprinted in* Katyal & Caplan, *supra* note 8, at 1076–77.

57. *See, e.g.*, Attorney Gen. Herbert Brownell Jr., Address at the University of Michigan Lecture Course 8 (Mar. 2, 1954), *available at* http://www.justice.gov/ag/aghistory/brownell/1954/03-02-1954.pdf (defending wiretapping in security cases based on Roosevelt memorandum); Memorandum from Attorney Gen. Tom C. Clark for President Harry S. Truman (July 17, 1946) (recommending authorization of security wiretaps and quoting Roosevelt memorandum); *cf. Rejoinder by Mr. Hoover*, 58 YALE. L.J. 422, 423 (1949) ("President Roosevelt had previously, on

the memorandum, wiretapping was constitutionally unregulated. In its 1928 decision *Olmstead v. United States*, the Supreme Court held that wiretapping did not violate the Fourth Amendment because it required no trespass.[58] Of course, the Court overruled *Olmstead* in its 1967 decision *Katz v. United States*.[59] But even before *Katz*, statutory restrictions circumscribed the use of wiretapping information[60]—a fact generally omitted by current commentaries. Without an understanding of this context, however, Roosevelt's memorandum garners greater precedential weight today than it ought to receive.

Historical accounts to date have been one-sided affairs, emphasizing the breadth of the executive's conduct without considering whether any constraint—external or self-imposed—limited such action.[61] These accounts wrongly imply that the Fourth Amendment fails to regulate national security investigations. In truth, as this Article explains, the Fourth Amendment figured prominently in regulating national security efforts in the post–World War II and Cold War eras, and both Justice Department and White House leaders sought to honor the Amendment's constitutional protections.

May 21, 1940, authorized the Attorney General to approve wire tapping [sic] when necessary involving the defense of the nation.").

58. 277 U.S. 438, 457 (1928) (noting wiretaps "were made without trespass upon any property of the defendants").

59. Katz v. United States, 389 U.S. 347, 353 (1967); *see also* Zweibon v. Mitchell, 516 F.2d 594, 616–17 (D.C. Cir. 1975) (noting "Supreme Court's unfortunate decision in *Olmstead*" means "[e]xecutive practice must be considered in its historical context, which illustrates why the 30-year policy of presidentially directed electronic surveillance has no substantial bearing on whether the practice of warrantless surveillance is now constitutional").

60. *See infra* notes 171–177 and accompanying text (describing statutory bar to prosecutorial use of wiretapping information).

61. *See, e.g.*, RICHARD A. POSNER, NOT A SUICIDE PACT 92 (Oxford Univ. Press 2006) (noting "government had long engaged in wiretapping and other forms of electronic surveillance" and "had done these things without seeking warrants or trying to confine surveillance to situations in which there was probable cause"); 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) ("Warrantless electronic surveillance has been used by the Executive to collect intelligence information since at least the mid-1800's . . . . Warrantless physical searches have been used for a much longer period of time . . . ."); Viet D. Dinh & Wendy J. Keefer, *FISA and the PATRIOT Act: A Look Back and a Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC. at iii, vi (2006) ("[W]ith the exception of some curtailment of the use of wiretaps in the latter portion of the Johnson Administration, warrantless electronic surveillance was regularly used . . . for purposes of national security . . . ."); Funk, *supra* note 15, at 1102–03 ("Presidents have authorized various forms of electronic surveillance for intelligence purposes since at least Franklin Roosevelt."); Gregory E. Birkenstock, Note, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 843 (1992) ("Electronic wiretapping, which law enforcement and national security agencies have practiced for almost as long as there have been wires to tap . . . .").

III. EARLY NATIONAL SECURITY INVESTIGATIONS

National security investigations are not a recent phenomenon; the United States has investigated foreign threats since the founding. In 1797, Secretary of State Timothy Pickering hired a private agent to investigate a conspiracy between the British Navy and Senator William Blount.[62] The Lincoln Administration, suspicious of Confederate sympathizers, oversaw the creation of the first intelligence-collection agency, headed by Allan Pinkerton.[63] By the early twentieth century, the newly established FBI spearheaded domestic investigations of foreign threats, a responsibility it maintains today.[64]

Despite the long history of security investigations, a unique legal framework for such operations did not develop until after World War II. Facing a need to ensure that national security investigators had sufficient operational leeway in the postwar era, executive branch officials began to theorize about a "national security exception" to the Fourth Amendment. Even as the national security exception developed, however, the Fourth Amendment continued to circumscribe security investigations. Specifically, while executive branch officials condoned the warrantless use of invasive investigative techniques, they also barred the use of evidence obtained through such techniques—a restriction this Article refers to as the "pure intelligence" rule. Over time, the pure intelligence rule became the most important constitutional boundary for investigators handling security cases during the Cold War.

Part III examines the Cold War era of national security investigations, which can be subdivided into three distinct periods.[65] During the first period, surveyed in Part III.A, federal agents employed invasive investigative techniques, despite misgivings by government lawyers about the constitutionality of such conduct. When these invasive techniques revealed condemning evidence of espionage and other crimes, prosecutors refused to use it at trial, even at the cost

62. *See* SAMUEL EDWARDS, BARBARY GENERAL: THE LIFE OF WILLIAM H. EATON 54–55 (Prentice-Hall 1968) (describing investigation into plot); BUCKNER F. MELTON, JR., THE FIRST IMPEACHMENT 93 (Mercer Univ. Press 1998) (describing plot).

63. *See* EDWIN C. FISCHEL, THE SECRET WAR FOR THE UNION 53 (Mariner Books 1996); DONALD E. MARKLE, SPIES AND SPYMASTERS OF THE CIVIL WAR 9 (Hippocrene Books 2004).

64. *See* Banks & Bowman, *supra* note 21, at 23 (noting by World War II, Bureau of Investigation "had assumed domestic counter intelligence responsibilities").

65. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at 22 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf (describing "three broad periods" marking "expansion of domestic intelligence activity").

of acquittals. The resulting equilibrium—a de facto pure intelligence rule—was more consequence than theory, but it served as an important precedent for later operations. The second and third periods operated under a more stable legal rubric. In the second period, examined in Part III.B, the Justice Department authorized the use of certain invasive surveillance techniques, beginning with microphone surveillance, under the theory that national security provided an exception to traditional Fourth Amendment rules. The third period, outlined in Part III.C, witnessed the broadening of the national security exception in two ways: the exception (1) became tentatively embraced by the judiciary and (2) was expanded to cover other "Fourth Amendment techniques" ordinarily requiring a warrant and probable cause.[66] The exception, however, remained purely intelligence based, with the executive branch defending its conduct by emphasizing the exception's circumscribed, nonprosecutorial nature.

This Part contextualizes the origins of the Fourth Amendment's national security exception and the early executive practices often cited in today's debates about the Fourth Amendment and foreign affairs. While early security investigations operated under a flexible constitutional framework, the Fourth Amendment nonetheless constrained the government in impactful ways that are often forgotten or ignored.

A. The De Facto National Security Exception: 1945–1954

In 1939, President Franklin Roosevelt designated the FBI as the primary civilian body responsible for the "investigation of all espionage, counter espionage, and sabotage matters."[67] These new

66. A word about methodology is in order. To trace the Fourth Amendment's role in early security investigations, this Article primarily examines the context in which the federal government employed "Fourth Amendment techniques"—tactics that normally require the issuance of a judicial warrant. *See, e.g.*, Attorney Gen. William French Smith, U.S. Dep't of Justice, Remarks Before the Los Angeles World Affairs Council 37 (Dec. 18, 1981), *available at* http://www.justice.gov/ag/aghistory/smith/1981/12-18-1981.pdf (identifying "[F]ourth [A]mendment techniques" such as seizures, wiretapping, bugging, and closed-circuit monitoring). Particularly during the period examined here, the scope of qualifying "Fourth Amendment techniques" changed significantly. Evolving Fourth Amendment jurisprudence (moving from a trespass-based theory to a reasonable-expectation-of-privacy model) had operational significance, altering what was or was not constitutionally regulated. Because this Article is concerned foremost with executive practice in the face of constitutional restraints, the Author accounts for this dynamism, and pertinent changes in Supreme Court doctrine are noted in the chronological discussion.

67. Directive from President Franklin D. Roosevelt to J. Edgar Hoover, Dir., FBI (June 26, 1939); *see also* G. Gregg Webb, *New Insights into J. Edgar Hoover's Role*, 48 STUD. INTELLIGENCE 45, 46–47 (2007), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no1/pdf/v48i1a05p.pdf (quoting directive).

responsibilities, however, spurred a number of legal questions about the Fourth Amendment's role in national security investigations. Rather than working off a well-formed policy, practice was forged through series of discussions between the FBI and Justice Department attorneys faced with prosecuting national security crimes.

1. Early Investigative Techniques and Constitutional Red Flags

To fulfill its new "general intelligence" function,[68] the FBI began training its agents in surreptitious surveillance. Starting in the 1940s, the FBI formed the "Sound School" where agents learned how to electronically intercept telephone calls and other communications.[69] An FBI technician also taught agents "lock studies" to facilitate break-ins.[70] As a sign of Allied cooperation, British intelligence officers instructed six FBI agents in the art of chamfering (surreptitious mail opening) in order to help the Bureau launch its own wartime mail-opening program.[71]

The Bureau's various new techniques, however, placed it in uncertain legal waters, particularly as World War II ended.[72] One controversial technique was microphone surveillance, commonly called "bugging,"[73] where agents would place an electronic listening device near the targeted individual to collect sounds in the surrounding area.[74] The FBI began employing microphone surveillance in 1940 to

68. In 1936, Hoover and Roosevelt discussed means by which the Bureau might collect "general intelligence information" pertaining to national security investigations. S. REP. NO. 94-755, at 25.

69. CURT GENTRY, J. EDGAR HOOVER: THE MAN AND HIS SECRETS 286 (W.W. Norton & Co. 2001) ("Wiretapping and bugging were taught at the FBI's 'Sound School' . . . .").

70. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS OF INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 355 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_III.pdf (describing "lock studies").

71. RICHARD E. MORGAN, DOMESTIC INTELLIGENCE 90 (Univ. of Texas Press 1980); W. THOMAS SMITH, JR., ENCYCLOPEDIA OF THE CENTRAL INTELLIGENCE AGENCY 100 (Facts on File 2003) ("British Intelligence operatives actually perfected [chamfering] prior to World War II and began to teach special agents of the [FBI] how to get into the mail of Axis diplomats.").

72. *See* HAYNES & KLEHR, *supra* note 21, at 12 ("As the sense of wartime emergency receded, attitudes regarding what was legal and illegal in security investigations were in flux.").

73. DAVID WISE, THE AMERICAN POLICE STATE 150 (Vintage Books 1976) ("From the very start, the necessity of breaking and entering to plant a microphone caused nagging intellectual and legal problems for the Department of Justice.").

74. *See* Dalia v. United States, 441 U.S. 238, 240 n.1 (1979) (describing "bugging" as "interception of all oral communication in a given location," which is "accomplished by installation of a small microphone in the room to be bugged and transmission to some nearby receiver").

investigate espionage cases.[75] Bugged facilities allegedly included foreign embassies,[76] hotels believed to be used by spies,[77] and certain brothels—the latter purportedly in the hopes of catching diplomats in compromising acts and leveraging this information to turn them into informants.[78]

At the time, though, the Supreme Court's Fourth Amendment jurisprudence raised serious constitutional questions about these bugging operations. Installing the bug often required government agents to trespass into a suspect's constitutionally protected private arena, but this type of trespass rendered a surveillance operation illegal under the Court's precedent.[79] Decisions like *Olmstead v. United States*[80] in 1928 and *Goldman v. United States*[81] in 1942 permitted nontrespassory forms of electronic surveillance, but these opinions also implied that a physical trespass was the sine qua non of a Fourth Amendment violation.[82]

Existing Court decisions also generated concerns about various physical searches the FBI was employing.[83] During the course of national security investigations, the Bureau conducted what it referred to as "black bag jobs": clandestine entries into homes, offices, and other protected places for a variety of purposes, such as photographing or seizing documents.[84] Black bag jobs, however,

---

75. FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 132.

76. GERALD K. HAINES & DAVID A. LANGBART, UNLOCKING THE FILES OF THE FBI: A GUIDE TO ITS RECORDS AND CLASSIFICATION SYSTEM 252 (Rowman & Littlefield Publishers 1993) ("In 1941 the FBI installed a number of surveillance taps on embassies and individuals despite the [great] reluctance of recently appointed Attorney General Francis Biddle to grant such authorization.").

77. *See* GENTRY, *supra* note 69, at 286 (noting "[m]any of the major hotels . . . and some of the chains . . . were especially accommodating, assigning subjects to prebugged rooms").

78. *Id.* at 286–87.

79. FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 132.

80. 277 U.S. 438, 457 (1928) (noting wiretaps "were made without trespass upon any property of the defendants").

81. 316 U.S. 129, 134–35 (1942) (noting "that the trespass did not aid materially in the use of the detectaphone").

82. Memorandum from William Olson, Assistant Att'y Gen. for Internal Sec., U.S. Dep't of Justice, to Attorney Gen. Elliot Richardson, *National Security Electronic Surveillance History, Policy and Procedure, 1924–73*, at 23 (undated) ("[A]s of the date of the *Goldman* decision, the test for the validity of a microphone surveillance was established to be whether or not it involved a trespass."); *National Security Electronic Surveillance History, Policy and Procedure, 1924–73*, *reprinted in Warrantless Wiretapping and Electronic Surveillance—1974: Joint Hearing Before S. Comm. on the Judiciary and S. Comm. on Foreign Relations*, 93d Cong. 23 (1974).

83. Today, FISA defines a "physical search" as "any physical intrusion . . . into premises or property . . . intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property . . . ." 50 U.S.C. § 1821(5) (2012).

84. Although the FBI occasionally counted surreptitious entries to install microphones as "black bag jobs," it largely treated entries for bugging operations as legally distinct from other

usually involved warrantless trespasses into constitutionally protected areas, raising the same concerns as bugging operations. Another type of constitutionally suspect technique involved the chamfering and photographing of sealed mail, a type of personal property that the Supreme Court held was constitutionally protected as early as 1878.[85]

As the FBI's warrantless investigative techniques gave rise to constitutional questions, FBI Director J. Edgar Hoover sought guidance on their legality by submitting a series of "hypothetical questions" to the Justice Department.[86] However, the Justice Department's responses failed to assuage the Bureau's concerns. In 1944, Alexander Holtzoff, Special Assistant to the Attorney General, wrote to Hoover about physical searches, explaining that "[t]he secret taking or abstraction of papers or other property from the premises without force is equivalent to an illegal search and seizure . . . . Consequently, such papers or other articles are inadmissible as against a person whose rights have been violated."[87] Assistant Attorney General T. Lamar Caudle issued similar warnings concerning microphone surveillance in December 1946, writing to Hoover "that where there has been a physical trespass upon the premises occupied by the defendant . . . , the evidence obtained by that means would be inadmissible on the ground that it was obtained by an illegal search and seizure."[88]

---

surreptitious entries. Accordingly, this Article does not include bugging entries in its definition of "black bag job." *See also* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS OF INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 355 n.1 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_III.pdf (defining "black bag job" as "warrantless surreptitious entries for purposes other than microphone installation, e.g., physical search and photographing or seizing documents").

85. *Id.* at 561–677 (discussing domestic CIA and FBI mail openings); *see also* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) ("It has long been held that first-class mail such as letters and sealed packages subject to letter postage . . . is free from inspection by postal authorities, except in the manner provided by the Fourth Amendment."); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (holding sealed mail in transit to be protected).

86. FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, MICROPHONES: POLICY BRIEF 9 (Aug. 17, 1966) (describing "pattern of presenting hypothetical situations" to Justice Department).

87. Memorandum from Alexander Holtzoff, Special Assistant to Att'y Gen., U.S. Dep't of Justice, for J. Edgar Hoover, Dir., FBI (July 4, 1944), *quoted in* S. REP. NO. 94-755, at 366–67. Possibly to avoid any adverse response, when he decided to use bugs during espionage investigations, Hoover did not brief the Justice Department further or seek the Attorney General's approval. FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 132.

88. FED. BUREAU OF INVESTIGATION, *supra* note 86, at 9–10 (quoting brief). In his July 1944 memorandum to Hoover, Holtzoff misinterpreted the Court's *Goldman* decision, concluding that "[m]icrophone surveillance is not equivalent to illegal search and seizure" and that "evidence so obtained should be admissible" even where "an actual trespass is committed." Memorandum from Alexander Holtzoff for J. Edgar Hoover, *supra* note 87; *see also* S. REP. NO. 94-755, at 294

Despite these constitutional red flags, the FBI continued to habitually use bugging, black bag jobs, and mail openings during the course of its security investigations. FBI records reveal hundreds of microphone surveillances conducted in the years immediately following World War II.[89] The Bureau's mail-opening programs were even more dramatic in scope, with federal agents establishing chamfering centers across the country to inspect thousands of letters.[90] Indeed, warrantless investigative techniques became an integral part of the FBI's postwar security operations.

2. Failed Prosecutions and Operational Responses

Though constitutional questions did not stop the FBI from employing warrantless investigative techniques, the Fourth Amendment limited national security operations in other ways. In a series of high-profile espionage trials, federal prosecutors concluded they could not present their best evidence to the jury because those materials had been gleaned from warrantless investigations. The result was a series of failed national security prosecutions, much to the embarrassment of the FBI and Justice Department.

The first evidentiary issue arose during the *Amerasia* trials. In 1945, the Office of Strategic Services (the Central Intelligence Agency's precursor) learned that individuals at the magazine *Amerasia*, a publication sympathetic to Chinese Communism, had obtained classified materials on Chinese-U.S. affairs.[91] Federal agents broke into the magazine's offices and discovered hundreds of protected government documents.[92] This black bag job was followed by months

---

n.74; *id.* at 367 ("[T]he Goldman decision did not support Holtzoff's conclusion, since the microphone surveillance in the case did not involve trespass; and the Court did not address the question of microphone surveillance accomplished by surreptitious entry."). Holtzoff's opinion might have constituted a legal coup for the FBI, but the Bureau does not appear to have actually relied on the errant analysis.

89. *See* Levi, *Church Committee Testimony*, *supra* note 18, at 68 (noting FBI records show hundreds of microphone surveillances were conducted between 1945 and 1952). These numbers do not account for the difference between trespassory and nontrespassory bugging, but other records confirm the FBI never abandoned trespassory bugging during this period. *See infra* note 119 and accompanying text.

90. Between 1940 and 1973, the CIA (or its precursor) and the FBI conducted a total of twelve mail-opening programs; in one program, agents intercepted, opened, and photographed more than 215,000 communications. S. REP. NO. 94-755, at 561.

91. *See* HARVEY KLEHR & RONALD RADOSH, THE AMERASIA SPY CASE (Univ. of North Carolina Press 1996); *see also* HAYNES & KLEHR, *supra* note 21, at 25–34 (describing *Amerasia* investigation).

92. As one agent later testified to Congress about the *Amerasia* investigation: "I don't offer any apologies for the method of entering a property [i.e., the *Amerasia* offices] without due process of law. I am well aware of the restrictions. I decided to take the course of action because

of warrantless wiretapping and bugging.[93] Through one such bug, agents overheard two suspects reveal they had obtained classified materials from Harry Dexter White, the Assistant Secretary of the Treasury.[94] Wiretaps and bugs also recorded John Stewart Service, a State Department official, offering to leak diplomatic materials.

In June 1945, agents arrested six suspects in connection with the *Amerasia* ring.[95] Prosecutors, however, immediately decided that little, if any, of the government's evidence was admissible, given the use of warrantless bugging, wiretapping, and black bag jobs.[96] With prosecutors refusing to use information tainted by constitutionally suspect techniques, they dropped all charges against four defendants and pled the remaining two to counts with no jail sentences.[97] As a result, the Justice Department never charged Harry Dexter White or two other identified spies, Joseph Bernstein and Thomas Bisson.[98] The first major spy prosecution of the postwar era, put simply, collapsed based in part on the executive's conclusions about the Fourth Amendment's continuing influence, even on national security investigations.[99]

---

of the necessities." H.R. Res. 430, 79th Cong. (1946), *published in* 96 CONG. REC. 7438 (daily ed. May 22, 1950) (testimony of Mr. Brooks).

93. *Id.* at 7439 (testimony of Mr. Brooks) (testifying FBI "tapped the telephones," "entered the premises," and "photostated all of the documents" in office); KLEHR & RADOSH, *supra* note 91, at 84 (noting bugging of telephones and hotel rooms).

94. KLEHR & RADOSH, *supra* note 91, at 52.

95. *Id.* at 34. One suspect's discovery of the FBI's hidden microphone apparently accelerated the decision. *Id.* at 84.

96. During a later congressional hearing on the *Amerasia* affair, Justice Department lawyers explained that the Office of Strategic Service's conduct was perceived to be so egregious—the chief prosecutor suggesting agents had "burglarized" Jaffe's office—that prosecutors avoided consulting with the Office in order to avoid tainting their case. 96 CONG. REC. at 7452 (testimony of Mr. McInerny); *see also id.* (statement of Mr. Hitchcock) (explaining "it was impossible to use that in court" which had come when "the Office of Strategic Services got into Jaffe's office"); *id.* at 7436 (statements of Reps. Hobbs and O'Sullivan) (suggesting "all of the evidence produced in the Amerasia case [grew] out of . . . unlawful searches and seizures").

97. HAYNES & KLEHR, *supra* note 21, at 37.

98. *Id.* at 38; KLEHR & RADOSH, *supra* note 91, at 84 (noting "investigators would never have known about Bernstein were not it for their electronic eavesdropping, so . . . any evidence seized might still be inadmissible in court under the 'fruit of the poisoned tree' principle"); JOHN EARL HAYNES & HARVEY KLEHR, VENONA 177 (Yale Univ. Press 1999) ("Although the FBI believed that Bernstein was a Soviet agent, it never arrested him . . . perhaps because the evidence gained by bugging was inadmissible in court."). White was also implicated by the testimony of Elizabeth Bentley, another Soviet spy who turned informant for the United States in 1945. White died in 1948, shortly after Bentley publicly testified about his Soviet relationship before the House Un-American Activities Committee. *See generally* R. BRUCE CRAIG, TREASONABLE DOUBT: THE HARRY DEXTER WHITE SPY CASE (Univ. Press of Kansas 2004).

99. HAYNES & KLEHR, *supra* note 21, at 44 (noting the "first major espionage case of the postwar era . . . fizzled out because of evidentiary problems and political interference"); *see also* Michael Wreszin, *"Gee but I'd Like to Be a G-Man,"* 20 REVS. AM. HIST. 258, 260 (1992)

Prosecutors faced the same evidentiary hurdle in the case of Joseph Weinberg. A graduate student of renowned physicist J. Robert Oppenheimer, Weinberg was selected to work on the U.S. nuclear weapons program commonly known as the "Manhattan Project."[100] In 1943, however, a warrantless FBI bug in the home of Steve Nelson, a political commissar of the Communist Party USA, recorded Weinberg offering to help the Soviet Union and disclosing a variety of specialized information about nuclear technology.[101] In 1949 hearings, the House Committee on Un-American Activities publicly identified the espionage incident and formally recommended that the Justice Department prosecute Weinberg for espionage.[102] The government finally indicted Weinberg in 1952 for perjury based on his sworn testimony denying membership in the Communist Party. The primary evidence proving his perjury (and his espionage), however, was obtained through the warrantless bug in Nelson's home. The Justice Department concluded that the evidence was inadmissible.[103] With the government obligated to withhold its smoking gun, a jury acquitted Weinberg—another embarrassing result covered on the front pages of the national newspapers.[104]

Cases like the *Amerasia* and *Weinberg* trials indicated that the use of warrantless investigative techniques could jeopardize subsequent trials, so the FBI and Justice Department began to shape investigations with these evidentiary issues in mind. In 1949, the FBI internally decided to avoid using electronic surveillance in any criminal case likely to go to trial.[105] Hoover also imposed new filing procedures (codenamed "June") that compartmentalized all sensitive information, including intelligence collected from bugs, physical

(reviewing GENTRY, *supra* note 69) ("In the *Amerasia* espionage case the FBI's illegal burglarizing, planted bugs, black bag jobs, tapped phones and surreptitious entry allowed the principals in the case to escape conviction.").

100. HAYNES & KLEHR, *supra* note 21, at 146–47.

101. *Id.* at 148.

102. *Named 'Scientist X,' He Denies Charge*, N.Y. TIMES, Oct. 1, 1949, at 1, 4. In 1948, a HUAC report had disclosed the espionage incident but did not identify Weinberg, only referring to the culprit as "Scientist X." *Text of Report by the House Committee on Un-American Activities Relating to Atomic Espionage*, N.Y. TIMES, Sept. 28, 1948, at 22 (reproducing report in full).

103. JOHN EARL HAYNES, HARVEY KLEHR & ALEXANDER VASSILIEV, SPIES: THE RISE AND FALL OF THE KGB IN AMERICA 121 (Yale Univ. Press 2009) (noting "the most damning evidence . . . had been gathered by warrantless wiretaps and bugs" and "[t]he Justice Department . . . opposed prosecution because of evidentiary problems").

104. *Weinberg Acquitted*, 9 BULL. OF ATOMIC SCIENTISTS 94, 94 (1953); *Weinberg Is Freed on Perjury Charge*, N.Y. TIMES, Mar. 6, 1953, at 1.

105. HAINES & LANGBART, *supra* note 76, at 253 (describing recommendation by FBI Associate Director Clyde Tolson approved by Hoover).

searches, and similar constitutionally suspicious techniques.[106] Field agents were ordered not to keep their own records of electronic surveillance or black bag jobs but rather to send them to Washington for maintenance in the separate system.[107] Aside from ensuring Hoover's control over potentially sensitive information, these procedures reduced the chance that bugging and tapping reports might taint FBI files that would later be used in criminal prosecutions.[108]

3. A Proposed and Rebuffed Constitutional Exception

At a June 1950 meeting of FBI executives, officials acknowledged that the Bureau was installing and using microphones "on its own authority—without any authorization from the [Justice] Department—and must assume responsibility for them if the issue of their legality were raised at any time."[109] Fears of microphone surveillance tainting impending prosecutions of Communist Party leaders under the Smith Act further compounded the Bureau's risk of political exposure.[110] These worries prompted Hoover to abandon his past practice of posing Cheshire hypothetical questions to Justice Department lawyers.[111] In October 1951, Hoover penned a memorandum to Attorney General J. Howard McGrath setting out the operational details of the FBI's national security investigations, including trespassory bugging. "As you know, in a number of instances it has not been possible to install microphones without trespass," he

106. ATHAN G. THEOHARIS, THE FBI: A COMPREHENSIVE REFERENCE GUIDE 31 (Greenwood 1999) [hereinafter THEOHARIS, REFERENCE]. As early as 1940, Hoover had created records systems that centralized information and allowed particularly sensitive information to be more easily maintained and, if needed, destroyed without attracting notice. ATHAN G. THEOHARIS, THE "DO NOT FILE" FILE, at v (1989), *available at* http://cisupa.proquest.com/ksc_assets/catalog/10754_FBIFileTheDoNotFile.pdf.

107. *See* THEOHARIS, REFERENCE, *supra* note 106, at 31 ("[R]eports were to be routed to the Special File Room at FBI headquarters to be 'maintained under lock and key.' "). Reports of such physical searches were marked as being sensitive collection; the reports were nonserialized, permitting their surreptitious destruction. ATHAN THEOHARIS, SPYING ON AMERICANS: POLITICAL SURVEILLANCE FROM HOOVER TO THE HUSTON PAPERS 126 (Temple Univ. Press 1978) [hereinafter THEOHARIS, SPYING].

108. RONALD KESSLER, THE BUREAU: THE SECRET HISTORY OF THE FBI 432 (St. Martin's Paperbacks 2003) ("Under Hoover's system, because microphone surveillance entailed break-ins, tapes of such surveillance were kept separately from the cases. Because the surveillance involved illegal entry, the material was to help generate leads and not to be used as evidence in court.").

109. FED. BUREAU OF INVESTIGATION, *supra* note 86, at 14–15 (emphasis omitted).

110. *Id.* at 16–17.

111. *See* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 132 (noting Hoover did not brief Attorney General on FBI bugging activities until Smith Act cases).

wrote.[112] Hoover sought "a definite opinion . . . as to whether . . . we should continue to utilize this technique [i.e., microphone surveillance] on the present highly restricted basis [i.e., security matters only], or whether we should cease the use of microphone coverage entirely in view of these issues currently being raised."[113]

McGrath refused to provide Hoover with the legal comfort he sought. In his February 1952 reply, McGrath concluded that trespassory bugging, even in national security matters, violated the Fourth Amendment.[114] Buggings that "involve trespass are in the area of the Fourth Amendment, and evidence so obtained and from leads so obtained is inadmissible," the Attorney General wrote.[115] Accordingly, McGrath refused to bless trespassory bugging operations: "[P]lease be advised I cannot authorize the installation of a microphone *involving a trespass* under existing law."[116]

McGrath's memorandum approached a formal rejection of the notion that national security constituted an exception to the Fourth Amendment. As a result, it momentarily shifted FBI operations. Hoover informed Bureau officials in March 1952 that he would no longer approve microphone surveillance requests requiring a trespass, even for national security purposes.[117] The number of FBI microphone surveillances dropped by approximately one-third over the next two years, a trend attributable to the curtailing of trespassory bugging even though nontrespassory bugs remained permissible.[118]

But despite McGrath's memorandum, some trespassory operations apparently continued. In a 1954 FBI memorandum, one official mentioned "a few instances wherein we had . . . utilized microphone surveillances" after the ban.[119] Hoover's own records hinted that trespassory bugging continued, though he claimed to have received Justice Department approval. In a memorandum for his files,

---

112. *See id.* at 137 (quoting Memorandum from J. Edgar Hoover for Attorney Gen. J. Howard McGrath, *supra* note 13).

113. *Id.* (quoting Memorandum from J. Edgar Hoover for Attorney Gen. J. Howard McGrath, *supra* note 13).

114. Memorandum from Attorney Gen. J. Howard McGrath for J. Edgar Hoover, Dir., FBI 1 (Feb. 26, 1952), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 137.

115. *Id.*

116. *Id.*

117. THEOHARIS, SPYING, *supra* note 107, at 107.

118. Levi, *Church Committee Testimony*, *supra* note 18, at 68 (noting reported operations fell from seventy-five in 1951 to sixty-three in 1952 and fifty-two in 1953). One internal FBI memorandum privately estimated that trespassory bugging comprised about twenty-five percent of total bugging operations. FED. BUREAU OF INVESTIGATION, *supra* note 86, at 29.

119. Memorandum from Louis Nichols, Assistant Dir., FBI, for Clyde Tolson, Assoc. Dir., FBI (Mar. 29, 1954), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 139.

Hoover claimed that McGrath's successor, James McGranery, orally blessed the continuation of trespassory bugging during national security investigations.[120]

This memorialization seems suspect. Other accounts indicate the Justice Department rejected an FBI request to use trespassory bugging only days after McGranery took over as Attorney General in April 1952.[121] Even assuming McGranery assented to trespassory bugging, this was apparently only an *extralegal* understanding; the FBI still lacked official legal backing from the Justice Department.

The equilibrium that emerged during the initial postwar years persisted for decades: national security investigations employed invasive investigative techniques, but the collected information remained out of the courtroom. While trespassory techniques never fully abated,[122] failed prosecutions, congressional inquiries, and Justice Department warnings inspired Hoover to curb certain practices and take precautions in others. Substantial legal uncertainty remained during these years, however, and not until later would this de facto equilibrium be adopted as a de jure rule.

B. The De Jure National Security Exception: 1954–1966

Upon assuming the presidency in 1953, Dwight Eisenhower felt, in the words of his Attorney General Herbert Brownell, "a special need to reassure the public that steps were being taken so that there would be no recurrence of the notorious cases of transmission of classified information to Soviet spies."[123] Encouraged by Eisenhower's focus, FBI officials started lobbying Justice Department officials for, as one Hoover deputy put it, "some backing of the [Justice] Department to utilize microphone surveillances where the intelligence to be gained was a necessary adjunct to security matters and important investigations, in instances when prosecution is not contemplated."[124]

---

120. Memorandum from J. Edgar Hoover, Dir., FBI, for the Director's File (June 9, 1952), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 138–39.

121. WISE, *supra* note 73, at 152 ("On April 10, 1952, the [Justice] Department responded to another Hoover inquiry by warning the FBI chief that installing a mike in a hotel room would invade the privacy 'of the guest and his guests.' ").

122. To be fair, the FBI was also never instructed to cease these activities; the Justice Department's response during these early years was a refusal to authorize such practices, not a direct order to quit their employment. THEOHARIS, SPYING, *supra* note 107, at 107 (noting McGrath "did not explicitly prohibit" warrantless wiretapping).

123. HERBERT BROWNELL & JOHN BURKE, ADVISING IKE 247 (Univ. Press of Kansas 1993).

124. Memorandum from Louis Nichols for Clyde Tolson, *supra* note 119, at 139; *see also* WISE, *supra* note 73, at 151–53 (describing lobbying effort).

The ensuing discussion between the FBI and Justice Department led to the federal government's first formal embrace of a national security exception to the Fourth Amendment. This acceptance continued under successive administrations. The national security exception became a legal keystone for subsequent security investigations. But while a constitutional theory emerged that could justify what was previously considered extralegal conduct, the exception operated within the same circumscriptions that limited earlier FBI operations. Specifically, warrantless investigative techniques, even in national security matters, remained limited to purely intelligence operations, meaning that collected information could only be used in nonprosecutorial manners.

1. Brownell: A Formal, but Limited, National Security Exception

Eisenhower officials initially adhered to McGrath's assessment that warrantless trespassory bugging, even during national security investigations, was unconstitutional.[125] In March 1954, Assistant Attorney General Warren Olney expressed "doubt[] that the Attorney General could authorize a microphone where trespass is clearly indicated."[126] Similarly, Deputy Attorney General William Rogers told FBI officials in that same month that he "did not think much . . . of the idea of having the Attorney General clear microphone surveillances."[127]

Nevertheless, persistent FBI officials ultimately found an ally in Attorney General Brownell. In early 1954, Hoover wrote Brownell ostensibly for the Attorney General's guidance on *Irvine v. California*, in which the Supreme Court squarely held that the warrantless installation of a microphone inside a suspect's house violated the Fourth Amendment.[128]

In May 1954, Brownell responded by memorandum. Recognizing that "in some instances the use of microphone surveillance is the only possible way of uncovering the activities of espionage agents, possible saboteurs, and subversive persons," Brownell believed that "the national interest requires that microphone

125. *See* FED. BUREAU OF INVESTIGATION, *supra* note 86, at 28 (describing 1953 meeting with Justice Department lawyers who told FBI that "it was apparent that the Attorney General, as chief law enforcement officer, could not be placed in the position of authorizing outright trespass").

126. Memorandum from Leland Boardman, Assistant Dir., FBI, for J. Edgar Hoover, Dir., FBI (Mar. 31, 1954), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 140.

127. Memorandum from Louis Nichols, Assistant Dir., FBI, for Clyde Tolson, Assoc. Dir., FBI (Apr. 14, 1954), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 140.

128. 347 U.S. 128, 146 (1954).

surveillance be utilized by the Federal Bureau of Investigation."[129] Though warning that microphone surveillance involving "a trespass . . . must necessarily be resolved according to the circumstances of each case," Brownell blessed the FBI's use of trespassory bugging in national security matters: "[T]he Department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conducive to our national interest . . . . [C]onsiderations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest."[130]

Moreover, Brownell's memorandum made clear that, rather than acknowledging extralegal surveillance as a necessary evil, the Attorney General intended to offer a constitutional justification for trespassory bugging. Under circumstances in which such surveillance was necessary to the national interest, Brownell reasoned, "The installation [of a bug through trespass] is proper and is not prohibited by the Supreme Court's decision in the *Irvine* case . . . ."[131] Since *Irvine* clearly held that a police officer's use of a microphone violated the Fourth Amendment absent special circumstances, the memorandum implied that national security investigations operated under different legal principles than ordinary criminal investigations.[132]

The key to the legal theory outlined in Brownell's memorandum was the distinction between evidence collection and intelligence gathering. "The FBI has an intelligence function in connection with internal security matters equally as important as the duty of developing evidence for presentation to the courts," the memorandum opined.[133] The Brownell memorandum did not mark the first time this distinction was asserted. When Hoover wrote then–Attorney General McGrath in 1952 seeking authorization for trespassory bugging, Hoover urged that such operations were "of an intelligence nature only."[134] Director Hoover conceded that "[t]he

129. Memorandum from Attorney Gen. Herbert Brownell for J. Edgar Hoover, Dir., FBI 1 (May 20, 1954) (copy on file with author).

130. *Id.*

131. *Id.*

132. KRIS & WILSON, *supra* note 43, § 3:4 ("Because the Supreme Court had made clear that a warrantless government trespass to install a microphone violated the Fourth Amendment, Attorney General Brownell's authorization . . . seemed to represent an assertion that 'internal security' allowed government agents to engage in conduct that otherwise would violate the Fourth Amendment.").

133. *Id.*

134. Memorandum from J. Edgar Hoover for Attorney Gen. J. Howard McGrath, *supra* note 13. By contrast, when a microphone was installed without trespassing, Hoover stated, "the

information obtained from [trespassory] microphones . . . is not admissible in evidence" but reasoned that if investigations remained "purely intelligence" operations—in other words, for nonevidentiary purposes—they would not run afoul of the constitutional difficulties the Bureau had previously encountered.[135] McGrath rejected this constitutional distinction, but Brownell accepted and incorporated it into his own memorandum. (The parallels between Hoover's 1952 memorandum and Brownell's 1954 memorandum are unsurprising since, as a later FBI account shows, the Bureau drafted the latter.)[136]

The Brownell memorandum, therefore, deemed trespassory bugging constitutionally permissible so long as it remained for purely intelligence matters. Brownell acknowledged the risk that trespasses posed to "the admissibility in court of the evidence thus obtained."[137] The FBI likewise understood this distinction between intelligence gathering and evidence collection. An internal Bureau analysis of the Brownell memorandum recognized that the authorization therein was not applicable "relative to criminal cases" and concluded that the FBI should continue to avoid trespassory microphones "particularly in cases which might go to prosecution."[138] In other words, the Bureau recognized that the Brownell memorandum authorized only the "purely intelligence" investigations that Hoover described to Attorney General McGrath in 1952. Despite this circumscription, Brownell's memorandum had notable operational significance: reported bugging operations doubled in the two years subsequent to the memorandum's issuance.[139]

More than any other single point in the nation's legal history, Brownell's memorandum marks the origin of the national security exception to the Fourth Amendment. While the FBI already conducted warrantless bugging prior to the 1954 directive, these operations occurred in uncertain legal waters and were sometimes assumed to be outright extralegal affairs. Another two decades would pass before the

---

information obtained . . . is treated as evidence and therefore is not regarded as purely intelligence information." *Id.*

135. *Id.*

136. FED. BUREAU OF INVESTIGATION, *supra* note 86, at 37–40; *see also* THEOHARIS, SPYING, *supra* note 107, at 108 (noting Hoover enclosed a draft memorandum to Brownell in his 1954 letter).

137. Memorandum from Attorney Gen. Herbert Brownell for J. Edgar Hoover, *supra* note 129, at 1.

138. Memorandum from A.H. Belmont, Assistant Dir., FBI, for L.V. Boardman, Assistant Dir., FBI (May 8, 1954), *quoted in* FED. BUREAU OF INVESTIGATION, *supra* note 86, at 38–39 (discussing draft memorandum).

139. Levi, *Church Committee Testimony*, *supra* note 18, at 68 (reporting rise in reported bugging from 52 cases in 1953 to 99 in 1954 and 102 in 1955).

judiciary formally adopted the exception, but the Attorney General's blessing brought bugging back within the fold of legitimacy. At the same time, the Justice Department's authorization rested on a distinction between evidentiary and nonevidentiary searches that limited the FBI's use of trespassory bugging and, later, other warrantless investigative techniques, to pure intelligence gathering.

2. Adherence to the Pure Intelligence Rule

Brownell's memorandum served as precedent for succeeding administrations to authorize warrantless trespassory bugging in national security matters, and subsequent attorneys general expressly authorized warrantless security searches if the Bureau limited their use to intelligence purposes. For example, Brownell's successor, William Rogers, authorized the use of trespassory bugs in national security investigations, despite earlier hesitations he had expressed as Brownell's deputy.[140] According to Justice Department memoranda, however, Rogers restricted his authorization to searches "for purposes of intelligence and not for the purpose of prosecution," the same caveat imposed by the Brownell memorandum.[141]

After John F. Kennedy's election in 1961, the FBI continued to use trespassory bugging circumscribed by the pure intelligence rule. The Bureau informed the Kennedy Administration that such operations were authorized only in security investigations done for intelligence purposes. In May 1961, Hoover wrote to then–Deputy Attorney General Byron White to set forth "[the Bureau's] views on the use of microphone surveillances in FBI cases":[142] "Our policy on the use of microphone surveillances is based upon a memorandum from former Attorney General Herbert Brownell dated May 20, 1954, in which he approved the use of microphone surveillance with or without trespass," Hoover explained.[143] "In light of this policy, in the internal security field, we are utilizing microphone surveillances on a restricted basis even though trespass is necessary to assist in uncovering the activities of Soviet intelligence agents and Communist

---

140. *See supra* note 127 and accompanying text (describing Rogers's earlier hesitancy). Despite later FBI allegations, Rogers also claimed to have never authorized trespassory bugging "outside of the internal security area." Athan G. Theoharis, *The Attorney General and the FBI: A Problem of Oversight*, USA TODAY, May 1979, at 62.

141. Memorandum from Attorney Gen. Nicholas Katzenbach for J. Edgar Hoover, Dir., FBI (May 31, 1966), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 161.

142. Memorandum from J. Edgar Hoover, Dir., FBI, for Byron White, Deputy Att'y Gen., U.S. Dep't of Justice (May 4, 1961), *reprinted in* VICTOR S. NAVASKY, KENNEDY JUSTICE 506 (Scribner 1971).

143. *Id.*

Party leaders."[144] Hoover emphasized, however, that trespassory bugging "is treated . . . not from the standpoint of evidentiary value but for intelligence purposes."[145] After being apprised of this limited use, the Justice Department permitted bugging operations to continue under those same restrictions.[146]

In contrast, the Johnson Administration offered a more critical eye toward the FBI's microphone surveillance. By the time of Johnson's presidency, federal use of trespassory surveillance had seemingly expanded to nonsecurity matters, such as tax evasion and organized crime. Shortly after taking office, Johnson moved to discontinue the growth of this practice.[147] "Utilization of mechanical or electronic devices to overhear nontelephone conversations . . . raises substantial and unresolved questions of Constitutional interpretation," the President wrote to members of his Administration in 1965.[148] Following the President's lead, Johnson's first Attorney General, Nicholas Katzenbach, instructed Hoover to halt warrantless trespassory bugging in organized crime and other nonsecurity investigations.[149] To enforce this restriction, Katzenbach also required the FBI to obtain the Attorney General's authorization before conducting such surveillance.[150] But while Katzenbach curbed what the public increasingly viewed as FBI abuses in bugging, he exempted national security investigations from his prohibitions. When Hoover informed the Attorney General that the FBI had "discontinued completely the use of microphones,"[151] Katzenbach responded that he

144. *Id.*

145. *Id.*

146. JAMES W. HILTY, ROBERT KENNEDY: BROTHER PROTECTOR 235 (Temple Univ. Press 1997) (describing bugging conversations between FBI and Attorney General Robert Kennedy); FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 132 ("In August 1961 Hoover was able to secure Kennedy's blind approval of future FBI bugging."); *see also* Levi, *Church Committee Testimony*, *supra* note 18, at 68–69 (reporting FBI records indicate 441 warrantless bugging operations took place between 1961 and 1965).

147. *No Federal Wiretaps*, N.Y. TIMES, July 19, 1965 ("Apparently Mr. Johnson made known his opposition to wiretapping shortly after he took office in 1963.").

148. Memorandum from President Lyndon B. Johnson for Heads of Executive Departments and Agencies (June 30, 1965) (copy on file with author).

149. Memorandum from Attorney Gen. Nicholas Katzenbach for J. Edgar Hoover, Dir., FBI (Jan. 27, 1966), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 149.

150. THEOHARIS, SPYING, *supra* note 107, at 112–14 (describing "first effective reviewing process" of FBI bugging).

151. Memorandum from J. Edgar Hoover, Dir., FBI, for Attorney Gen. Nicholas Katzenbach (Sept. 14, 1965), *in* FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 147.

saw "no need to curtail any such activities in the national security field."[152]

The Johnson Administration permitted bugging to continue in security investigations but emphasized that the technique was only to be used for nonevidentiary purposes in line with what had become the de jure pure intelligence rule. Katzenbach instructed Hoover that the use of "microphones involving trespass" should be "confined to the gathering of intelligence in national security matters," given "the inadmissibility of any evidence obtained in court cases."[153] "[I]nformation or leads obtained by this means can not [sic] be used for purposes of prosecution," Katzenbach reiterated in a later memorandum.[154] Similarly, a 1966 memorandum from Katzenbach's successor, Ramsey Clark, to all U.S. Attorneys emphasized that "[i]ntelligence data so collected [by national security bugging] will not be available for investigative or litigative purposes."[155]

As before, Justice Department officials kept the intelligence collected from bugging out of the courtroom, even at the cost of criminal convictions. In 1963, for example, federal agents arrested Aleksandr Sokolov, living under the assumed name Robert Baltch, and his wife. The two were indicted for attempting to transmit sensitive military information to the Soviet Union.[156] On the eve of trial in fall 1964, the prosecuting U.S. Attorney, Joseph Hoey, repeatedly denied in open court that the government had used any warrantless investigative techniques during the Baltch investigation. In reality, the FBI had bugged the suspects' apartment and opened their mail.[157]

As the jury trial opened, Katzenbach (then serving as Acting Attorney General) was apprised of the investigative techniques the FBI had used. Outraged, Katzenbach immediately directed Hoey to correct his statement and, it appears, ordered prosecutors not to use evidence derived from the bugging and mail-opening operations.[158] On

---

152. Memorandum from Attorney Gen. Nicholas Katzenbach for J. Edgar Hoover, Dir., FBI (Sept. 27, 1965), *quoted in* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS OF INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 287 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_III.pdf.

153. *Id.*

154. Memorandum from Nicholas Katzenbach for J. Edgar Hoover, *supra* note 141.

155. Memorandum from Attorney Gen. Ramsey Clark for all United States Attorneys (Nov. 3, 1966) (internal quotation marks omitted), *quoted in* S. REP. NO. 94-755, at 288.

156. James P. McCaffrey, *Russian Spy Suspect Identified*, N.Y. TIMES, Dec. 18, 1963, at 12.

157. THEOHARIS, SPYING, *supra* note 107, at 112.

158. *Id.*; *see also* THEOHARIS, SPYING, *supra* note 107, at 112 (describing Baltch trial and attributing dismissal to bugging issue); RICHARD C.S. TRAHAIR & ROBERT L. MILLER,

the afternoon of the first day of trial, Hoey announced to the court that he had "been instructed by the Attorney General that, in the interests of national security, he would not offer any evidence relating to [the major espionage counts] of the indictment."[159] This about-face, which newspapers covered on their front pages, prompted the government to dismiss the charges against the Sokolovs, who were subsequently deported to the Soviet Union.[160]

As the Cold War progressed, the continuing dialogue between the FBI and Justice Department placed the nation's domestic counterintelligence programs on more stable legal footing. By the 1960s, both agents and government lawyers felt comfortable with the principle of the national security exception to the Fourth Amendment but acknowledged the exception's limited nature by referring to security investigations as intelligence—rather than evidentiary—searches.

C. The Judicial National Security Exception: 1966–1978

Beginning in the 1960s, debates about the Fourth Amendment's national security exception moved from the executive branch into the halls of Congress and the chambers of the judiciary; both branches tentatively embraced the exception. Government officials began to apply the rule to a growing number of techniques and security investigations. At the same time, the exception remained within the pure intelligence paradigm.

1. *Black* and *Schipani*: Briefing the Limited Security Exception

For two decades after World War II, executive discussions about the legal framework for national security investigations remained out of the judicial and public eye. In the 1960s, however, events forced the executive branch to disclose its legal justifications. In 1964, the Justice Department successfully convicted lobbyist Fred Black of income tax evasion but learned during Black's appeal that the FBI had bugged his Las Vegas hotel room without a warrant.[161] After the Justice Department disclosed its error, the Supreme Court—likely influenced by congressional investigations of similar bugging

---

ENCYCLOPEDIA OF COLD WAR ESPIONAGE, SPIES, AND SECRET OPERATIONS 86 (Enigma Books 2012) (noting the Baltches were released because "[e]vidence from eavesdropping was not admissible in court").

159. David Anderson, *U.S. Drops Trial of 2 in Spy Case*, N.Y. TIMES, Oct. 3, 1964, at 1, 10.

160. *Id.*

161. FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 13, at 154.

abuses[162]—ordered the government to submit a supplemental brief more fully explicating its use of microphone surveillance.[163] The brief would become the executive's first public disclosure of its surveillance policies.[164]

On July 13, 1966, Solicitor General Thurgood Marshall filed the government's supplemental memorandum, which laid out the scope of authorized microphone surveillance in national security matters:

> Under Departmental practice . . . the Director of the Federal Bureau of Investigation was given authority to approve the installation of devices such as that in question for intelligence (and not evidentiary) purposes when required in the interests of internal security or national safety . . . . Present Departmental practice, adopted in July 1960 in conformity with the policies declared by the President on June 30, 1965, for the entire federal establishment, prohibits the use of such listening devices (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security.[165]

Later that year, Solicitor General Marshall reiterated the limited nature of the government's warrantless surveillance while briefing another nonsecurity bugging case, *Schipani v. United States*:

> Present governmental practice . . . prohibits such electronic surveillance [i.e., microphone surveillance] in all instances except those involving the collection of intelligence with respect to matters affecting national security. Such intelligence data will not be made available for prosecutorial purposes, and the specific authorization of the Attorney General must be obtained in each instance when the national security exception is sought to be invoked.[166]

Though neither *Black* nor *Schipani* involved national security matters, both government briefs emphasized that the Johnson Administration had only allowed electronic surveillance for intelligence purposes in national security cases. Emphasizing this self-circumscription was clearly strategic, aimed to garner judicial support

---

162. The most high-profile congressional investigation, led by Senator Edward Long, revealed various cases of government agents using warrantless wiretaps, particularly by the Internal Revenue Service. National security investigations, however, were not the Committee's focus. ALEXANDER CHARNS, CLOAK AND GAVEL 40–42 (Univ. of Illinois Press 1992).

163. *U.S. Eavesdropping Policy May Be Divulged Today in Answers to Court*, N.Y. TIMES, July 13, 1966.

164. *Id.* (noting government "may acknowledge officially for the first time a practice that has evolved over the last 30 years").

165. Supplemental Memorandum of the United States, Black v. United States, 385 U.S. 26 (1966) (No. 1029), *quoted in* Levi, *Church Committee Testimony*, *supra* note 18, at 69.

166. Supplemental Memorandum for the United States at 4, Schipani v. United States, 385 U.S. 372 (1966) (No. 504). Like Black, Schipani was convicted of income tax evasion. In October 1966, the FBI notified the Acting Attorney General that Schipani participated "in various conversations electronically monitored on a number of occasions in 1961" and that the microphone was installed "by means of a trespass." *Id.* at 2.

for a national security exception to the Fourth Amendment.[167] The briefs also show the degree to which the pure intelligence rule had become the legal foundation for the use of warrantless investigative techniques, and the government's disclosures were likely offered to show that surveillance was circumscribed enough to protect civil liberties.

The Supreme Court did not address the merits of the government's implicit arguments about national security investigations, instead remanding both *Black* and *Schipani* for retrials. But the following year, the Court finally raised the possibility of a national security exception during a series of decisions dealing with another technique vital to national security investigations: wiretapping.

2. *Katz*: A Judicial Nod to the Security Exception

Wiretapping, also known as telephone surveillance, involves the interception of a message during its transmission by wire or radio wave from one party to another.[168] Like bugging and physical searches, wiretapping became frequently employed in national security investigations; as noted above, Franklin Roosevelt authorized wiretapping in security matters as early as 1940.[169] But, while wiretapping was prolific in security investigations, federal officials did not rely on the Fourth Amendment's national security exception because, unlike bugging, wiretapping rarely involves physical trespass. Consequently, in *Olmstead v. United States*, the Supreme Court held such surveillance to be outside the Fourth Amendment's ambit and therefore constitutionally permissible.[170]

---

167. At the time, Katzenbach estimated that fewer than fifty national security buggings were authorized at any time. *Katzenbach Foresees Passage of Fair Housing Bill Eventually*, N.Y. TIMES, Oct. 3, 1966.

168. *See* Dalia v. United States, 441 U.S. 238, 240 n.1 (1979) (describing wiretapping as "confined to the interception of communication by telephone and telegraph and generally may be performed from outside the premises to be monitored"). Like bugging, government agents have long employed "tapping" during security investigations. Union officers tapped telegraph wires during the Civil War. SAMUEL DASH ET AL., THE EAVESDROPPERS 23 (Rutgers Univ. Press 1959). In the lead-up to World War I, the Secret Service installed wiretaps to surveil German and Austro-Hungarian delegations. Banks & Bowman, *supra* note 21, at 20.

169. Memorandum from President Franklin D. Roosevelt to Attorney Gen. Robert Jackson, *supra* note 56, at 2; *see also supra* note 57 and accompanying text (noting reliance on Roosevelt memorandum).

170. 277 U.S. 438, 466 (1928) ("[O]ne who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and . . . the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment.").

Yet, even without constitutional restraints, Congress statutorily imposed the pure intelligence rule on wiretapping. Section 605 of the 1934 Communications Act barred persons from "intercept[ing] any communication and divulg[ing] or publish[ing] the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[171] In *Nardone v. United States*, the Supreme Court read section 605's "interception and divulgence" ban to bar government agents from introducing wiretapped communications or their "fruits" at trial.[172] Since the Communication Act's language only prohibited the combination of intercepting *and* divulging evidence, however, the Justice Department interpreted section 605 to permit wiretapping as long as prosecutors did not introduce the information at trial.[173] The result was a pure intelligence rule parallel to the Fourth Amendment's regulation of early security investigations.[174]

Like the constitutionally imposed pure intelligence rule, section 605's evidentiary ban spoiled some espionage trials. In 1949, for example, the Second Circuit vacated the conviction of Judith Coplon, a Justice Department employee caught spying for the Soviet Union, on the grounds that the FBI violated section 605 by wiretapping Coplon.[175] Executive officials also admitted other cases remained in

171. Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064. Congress's intent with respect to section 605 is somewhat unclear. *To Authorize Wire Tapping: Hearings on H.R. 2266 and H.R. 3099 Before the Subcomm. No. 1 of the H. Comm. on the Judiciary*, 77th Cong. 238–39 (1941) (statement of Alexander Holtzoff, Special Assistant to Att'y Gen., U.S. Dep't of Justice) (claiming section's purpose was to "protect persons . . . against acts such as the divulging of information on the part of switchboard operators or telegraph operators"); *see also* WALTER F. MURPHY, WIRETAPPING ON TRIAL 133 (Random House 1965) (describing section's unclear origins).

172. Nardone v. United States (*Nardone I*), 302 U.S. 379, 381 (1937); Nardone v. United States (*Nardone II*), 308 U.S. 338, 341 (1939). While executive officials condemned the *Nardone* decisions, many members of Congress embraced the evidentiary bar. *Wiretapping for National Security: Hearings on H.R. 408 Before the Subcomm. No. 3 of the H. Comm. on the Judiciary*, 83d Cong. 29 (1953) (statements of Reps. Willis and Rogers) (describing, approvingly, that section 605's wiretapping bar was "common-law rule now").

173. *See* Katyal & Caplan, *supra* note 8, at 1035–46 (describing early interpretations of Section 605).

174. "I do not think . . . the Communications Act, as a matter of law, prevents the executive branches of the government from tapping wires. It does, without any question, prevent the use of the evidence thus obtained," Attorney General Francis Biddle testified. *Authorizing Wire Tapping in the Prosecution of the War: Hearing Before Subcomm. No. 2 of the H. Comm. on the Judiciary*, *Part II*, 77th Cong. 2 (1942).

175. United States v. Coplon, 185 F.2d 629, 640 (2d Cir. 1950). The D.C. Circuit vacated a second conviction on similar grounds. Coplon v. United States, 191 F.2d 749, 760 (D.C. Cir. 1951) (concluding district court "erred in not affording a hearing as to the appellant's allegations that the government listened through a wiretapping device to her telephone conversations with her attorney"); *see also* MARCIA MITCHELL & THOMAS MITCHELL, THE SPY WHO SEDUCED AMERICA

"cold storage"—that is, unprosecuted—due to section 605.[176] Despite these prosecutorial problems, section 605, as interpreted by the Justice Department, still allowed the FBI to conduct pure intelligence wiretapping. Records show that the FBI employed thousands of wiretaps between 1945 and 1966, many of which were aimed at foreign threats.[177]

When the Supreme Court prepared to overrule *Olmstead* and develop a constitutional framework for wiretapping, at least one Justice, Byron White, recognized the possible implications for national security investigations. Before Justice White ascended to the Supreme Court, he served in the Kennedy Justice Department, where he gained familiarity with electronic surveillance and became an advocate for such techniques.[178] White continued his advocacy for national security surveillance from the bench. In the 1967 case *Berger v. New York*, for example, the Court outlined the constitutional parameters for search warrants authorizing electronic surveillance.[179] White, writing in dissent, protested that the majority's rule made no room for Congress to create a "national security exemption."[180] "[I]f electronic surveillance . . . must be circumscribed in the manner the Court now suggests, how can surreptitious electronic surveillance of a suspected Communist or a suspected saboteur escape the strictures of the Fourth Amendment?" he asked.[181] White offered that there "are some purposes and uses of electronic surveillance which do not involve

(Invisible Cities Press 2002) (recounting the Coplon affair); Luther A. Huston, *Judith Coplon Wins a New Trial but Legal Tangle May Prevent It*, N.Y. TIMES, Jan. 29, 1952, at 1, 9; *Court Reverses Conviction of Judith Coplon*, WASH. POST, Dec. 6, 1950, at 1. The FBI also bugged Coplon, though the judiciary never reached that issue. FED. BUREAU OF INVESTIGATION, *supra* note 86, at 14 (noting FBI notified Justice Department that "a microphone was utilized in the espionage case involving Judith Coplon").

176. *Spy Trials Hinged on Wiretap Law*, N.Y. TIMES, Nov. 22, 1953, at 26; *see also* William P. Rogers, *The Case for Wire Tapping*, 63 YALE L.J. 792, 793 (1954) ("[Under section 605,] law enforcement officials possessed of intercepted information vital to the security of the nation may not use such information in bringing spies and saboteurs to justice in our federal courts."); Letter from Attorney Gen. J. Howard McGrath to Emanuel Celler, U.S. Representative, N.Y. (Feb. 2, 1951), *reprinted in Wiretapping for National Security*, *supra* note 172 (noting section 605's effect on "number" of security cases but declining "to identify any of them [cases] by name").

177. Levi, *Church Committee Testimony*, *supra* note 18, at 68–69 (reporting 5,807 wiretaps between 1945 and 1966).

178. DENNIS J. HUTCHINSON, THE MAN WHO ONCE WAS WHIZZER WHITE 308, 497 (Free Press 1998); *see also* Morton Mintz, *Kennedy Hints FBI Wiretapping*, WASH. POST, June 27, 1966 (quoting Justice Department official as saying that " 'Whizzer' White knew a lot about this [electronic surveillance] himself when he was working for Bobby [Kennedy]").

179. Berger v. New York, 388 U.S. 41, 50–64 (1967).

180. *Id.* at 115 (White, J., dissenting).

181. *Id.* at 116.

violations of the Fourth Amendment by the Executive Branch," the first of which was national security investigations.[182]

Though White persuaded no colleagues in *Berger*, he was more successful later that year when the Court finally overruled *Olmstead* in *Katz v. United States*.[183] *Katz* held that nontrespassory electronic surveillance (i.e., wiretapping and nontrespassory bugging) constituted a Fourth Amendment "search" and ordinarily required ex ante judicial approval.[184] *Katz* had nothing to do with national security—the case involved a bookie—and the briefs made no mention of foreign affairs or other security considerations.[185] Nevertheless, in footnote twenty-three, the *Katz* Court expressly reserved the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security."[186]

From the Justices' papers, one can trace footnote twenty-three to Justice White. Early drafts of the *Katz* opinion circulated by Justice Potter Stewart did not contain the national security caveat.[187] After Stewart submitted his draft, however, White circulated an opinion dated November 28, 1967 in which he dissented in part. "I would not erect an impenetrable constitutional barrier to eavesdropping or wiretapping performed without a judicial warrant" in national security cases, White's draft opined.[188] Two days after White sent out his opinion, Justice Abe Fortas wrote to Stewart, suggesting Stewart "insert something reserving national security cases in which maybe the Constitution would permit electronic espionage on authorization by the President or the Attorney General. This is Byron White's idea,

182. *Id.*

183. 389 U.S. 347, 353 (1967).

184. *Katz* itself did not involve a wiretap, but rather a nontrespassory microphone taped on top of a public telephone booth. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 849 (2004).

185. Funk, *supra* note 15, at 1107 n.39 ("[T]here is no mention of national security in the government's brief.").

186. 389 U.S. at 358 n.23.

187. *See* Papers of Justice William O. Douglas (on file with the Library of Congress, Manuscript Division, Box 1414) (containing Stewart's initial draft).

188. *Id.* (containing draft White dissent). Discussion amongst the Justices of national security matters may have preceded the draft. On an undated note attached to the first draft of his *Katz* concurrence, William Douglas's clerk wrote that "Justice White, rather than Justice Black, injects the national security issue into the *Katz* case . . . . You asked me to write a brief response to the national security point if Justice Black raised it, so I assume this stands for Justice White, too. The following is my proposal." *Id.* (containing note). Multiple Justices, therefore, appear to have recognized *Katz*'s security implications before White's circulated dissent.

and I think it would be well to adopt the suggestion."[189] Later that day, Stewart circulated a new draft with footnote twenty-three as it appears in the published opinion.[190] White withdrew his partial dissent.[191]

Katz's footnote twenty-three "proved to have lasting historical significance."[192] Though *Katz* was supposedly agnostic on the issue, the executive branch interpreted footnote twenty-three as a judicial blessing of the national security exception. The FBI, which had officially halted the use of trespassory microphone surveillance in 1967 in light of the technique's legal uncertainty, resumed bugging in 1968 after *Katz* was decided.[193] Government lawyers relied on *Katz* to defend the use of warrantless investigative techniques in national security matters,[194] and lower courts embraced the exception. In 1970, the Fifth Circuit found warrantless wiretapping to be lawful "for the purpose of obtaining foreign intelligence information"—the first court to so hold.[195]

---

189. *Id.* (containing copy of Fortas note).

190. *Id.* (containing subsequent Stewart draft).

191. White concurred in *Katz* but issued an opinion proposing that, in national security cases, the warrant requirement be excused as long as the "President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." *Katz*, 389 U.S. at 364 (White, J., concurring). "[Warrantless w]iretapping to protect the security of the Nation has been authorized by successive Presidents," White argued. *Id.* at 363.

192. Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 800 (1989).

193. Levi, *Church Committee Testimony*, *supra* note 18, at 69 (noting no reported bugging operations in 1967). The FBI's newfound restraint was also attributable to the Johnson Administration's requirement that the FBI obtain the Attorney General's authorization before conducting such surveillance. *See supra* note 150 and accompanying text (discussing Katzenbach's instructions to Hoover to halt warrantless trespassory bugging).

194. After *Katz*, the Justice Department thought the exception excused all warrantless Fourth Amendment techniques, including bugging, wiretapping, and black bag jobs. In 1975, the Justice Department submitted a letter to the D.C. Circuit claiming the exception covered both physical searches and electronic surveillance, reasoning that "[o]ne form of search is no less serious than another." Letter from John C. Keeney, Assistant Att'y Gen., U.S. Dep't of Justice, to Hugh E. Kline, Clerk of the Court, D.C. Cir. (May 9, 1975), *quoted in* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS OF INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 369–70 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_III.pdf. This view ultimately prevailed. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 912–17 (4th Cir. 1980) (applying exception to physical search); United States v. Marzook, 435 F. Supp. 2d 778, 792–94 (N.D. Ill. 2006) (same). *But see* United States v. Ehrlichman, 376 F. Supp. 29, 33–34 (D.D.C. 1974) (distinguishing wiretapping from break-ins, which went to "core of the Fourth Amendment").

195. United States v. Clay, 430 F.2d 165, 170 (5th Cir. 1970); *see also* United States v. Hoffman, 334 F. Supp. 504, 508 (D.D.C. 1971) (finding "defendant's conversations intercepted during . . . electronic surveillance, conducted for the purpose of gaining foreign intelligence information, was not intercepted illegally").

Even after *Katz*, however, the government continued its adherence to the pure intelligence rule. In 1968, for example, the government relied on *Katz* to defend the warrantless wiretapping of two suspected Soviet spies, John Butenko and Igor Ivanov.[196] The Justice Department made a point of reiterating to the Supreme Court that "the government has not claimed that evidence obtained by electronic eavesdropping in the course of a national security investigation is admissible in a criminal trial."[197] While *Katz* gave credence to the national security exception, the exception remained firmly within the pure intelligence paradigm.[198]

3. *Keith*: Maintaining a Limited Security Exception

In 1972, the Supreme Court revisited *Katz*'s reference to a national security exception in *United States v. United States District Court*, commonly called the *Keith* case.[199] The case involved the prosecution of three members of the White Panther Party for the bombing of a CIA office.[200] During pretrial discovery, the government conceded that agents overheard one defendant's conversations on a warrantless wiretap.[201] The government refused, however, to turn over transcripts of the conversations, arguing that the taps were legal and the conversations were irrelevant to the charges at hand. In defense of

196. Brief for the United States at 8–9, Ivanov v. United States, 394 U.S. 165 (1969) (Nos. 11, 197), 1968 WL 129379, at *7. The government supposedly backed away from that position at oral arguments. Justice Stewart later recounted that "[i]n oral argument of the Butenko and Ivanov cases, the Solicitor General, mystifyingly, sought to concede that the surveillances there were in fact unconstitutional, although he was repeatedly invited to argue that they were not." Giordano v. United States, 394 U.S. 310, 313 n.1 (1969) (Stewart, J., concurring). The Solicitor General possibly did not mean that the wiretapping itself was unconstitutional, but rather the prosecutorial use of collected information was impermissible. That position aligns with both the government's briefs and historical practice.

197. Brief for the United States at 8–9, *Ivanov*, 394 U.S. 165 (Nos. 11, 197).

198. *See* Funk, *supra* note 15, at 1107–08 (arguing "because the government itself had only represented that it only used such surveillances for intelligence purposes and not for evidentiary purposes," *Katz* only intended to permit security investigations for intelligence purposes).

199. 407 U.S. 297 (1972).

200. *Id.*; *see also* Trevor W. Morrison, *The Story of* United States v. United States District Court *(*Keith*): The Surveillance Power*, *in* PRESIDENTIAL POWER STORIES 287 (Christopher H. Schroeder & Curtis A. Bradley eds., 2008). Formed to support the Black Panther Party, the White Panthers sought "Cultural Revolution . . . us[ing] every tool, every energy and any media we can get our collective hands on." *Id.* at 292 (quoting manifesto).

201. According to Justice Powell's notes, the conversations were between the defendant and Black Panther members. Papers of Justice Lewis F. Powell, Jr. (on file with Washington and Lee University School of Law), *available at* http://law.wlu.edu/deptimages/powell%20archives/70-153_U.S.%20v.%20U.S.%20District%20Court,%201972March-April.pdf.

the wiretap's legality, the government claimed that the national security exception excused the search.[202]

Keith represents the first effort by an administration to expand the national security exception beyond the pure intelligence paradigm. In the government's reply brief, the Nixon Administration argued that "in the course of such [warrantless national security] surveillance evidence may be obtained that indicates the commission of a crime. In such an event the government contends that it would be fully warranted in using the evidence thus obtained in prosecuting the crime thus disclosed."[203] While *Katz* had only tentatively broached the national security exception, the Nixon Administration sought to dramatically expand its scope by breaking from thirty years of practice—practice that had only just recently been disclosed to the judiciary and was defended by relying on the pure intelligence rule.

The government's arguments in *Keith*, however, found no supporters in the Supreme Court—unsurprisingly, since Nixon's own Solicitor General, Erwin Griswold, refused to argue the case based on his belief that the government's conduct had been unconstitutional.[204] Justice Powell, writing for the Court, held that the government's "domestic security surveillances" program into "internal security matters" and "domestic organizations" did not qualify for the national security exception.[205] At the same time, the *Keith* decision largely affirmed a more restrained version of the national security exception. The Court made clear that the decision did not apply to the warrantless surveillance of threats that "involve[] . . . foreign powers or their agents."[206] It also noted a growing "view that warrantless surveillance, though impermissible in domestic security cases, may be

202. Brief for the United States at 17, *Keith*, 407 U.S. 297 (1972) (No. 70-153).

203. Reply Brief for the United States at 2–3, *Keith*, 407 U.S. 297 (1972) (No. 70-153). In a later filing in *Ivanov v. United States*, the Nixon Administration reiterated this claim—in direct contradiction to the government's statement during Ivanov's first appeal. *Compare* Memorandum for the United States at 13, Ivanov v. United States, 419 U.S. 881 (1974) (No. 73-1648) ("If an electronic surveillance which was authorized for purposes of foreign intelligence gathering incidentally turns up evidence of criminal activity, such evidence may be introduced in a criminal trial because the surveillance itself was constitutional."), *with* Brief for the United States at 8–9, *Ivanov*, 394 U.S. 165 (1969) (Nos. 11, 197), 1968 WL 129379, at *8–9 (conceding "evidence obtained by electronic eavesdropping in the course of a national security investigation is [not] admissible in a criminal trial").

204. *See* Morrison, *supra* note 200, at 305; *see also* LINCOLN CAPLAN, THE TENTH JUSTICE 34–35, 290 n.11 (Knopf 1988) (noting Griswold "believed the Nixon Administration was seeking more authority for the Executive Branch than the laws in question allowed" and "that he would diminish his credibility with the Justices if he made the claims that the Executive Branch wanted him to press").

205. *Keith*, 407 U.S. at 299–300, 318.

206. *Id.* at 321–22.

constitutional where foreign powers are involved."[207] After *Keith*, lower courts held that national security constituted a "recognized exception" to the Fourth Amendment's Warrant Clause.[208] These cases allowed warrantless surveillance solely "for the purpose of gathering foreign intelligence," but none went beyond the pure intelligence rule.[209]

Based on the caveats in *Keith* and *Katz*, the Nixon Administration continued to authorize warrantless surveillance of foreign threats. After *Keith*, Attorney General Elliot Richardson announced he would approve applications for warrantless electronic surveillance if he was "convinced that it is necessary (1) to protect the nation against actual or potential attack or other hostile acts of a foreign power; (2) to obtain foreign intelligence information deemed essential to the security of the United States; or (3) to protect national security information against foreign intelligence activities."[210] The Nixon Administration, however, did not challenge the pure intelligence rule further but instead operated within the paradigm. During Nixon's tenure as President, federal prosecutors never offered any information collected from warrantless investigative techniques in a criminal trial.[211] The pure intelligence rule persisted as the governing standard.

At the same time, the national security exception found greater support in the judiciary. Because the pure intelligence rule ensured that courts never admitted warrantlessly obtained evidence against defendants, the initial judicial debates over the national security

---

207. *Id.* at 322 n.20 (citing United States v. Clay, 430 F.2d 165 (5th Cir. 1970); United States v. Smith, 321 F. Supp. 424, 425–26 (C.D. Cal. 1971)).

208. United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); *see also* United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (holding warrantless search "conducted and maintained solely for the purpose of gathering foreign intelligence information" was constitutional); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding that "President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence"). In 1975, a plurality of the D.C. Circuit, sitting en banc, challenged the notion of a national security exception. Zweibon v. Mitchell, 516 F.2d 594, 651 (D.C. Cir. 1975) (en banc) (plurality opinion) ("[A]bsent exigent circumstances, no wiretapping in the area of foreign affairs should be exempt from prior judicial scrutiny, irrespective of the justification for the surveillance or the importance of the information sought."). That position, however, failed to persuade. Chagnon v. Bell, 642 F.2d 1248, 1259 (D.C. Cir. 1980) ("[W]e cannot accept appellants' position that [*Zweibon*], or any other decision, authoritatively eliminated the foreign agent exception.").

209. *Butenko*, 494 F.2d at 605.

210. Press Release, U.S. Dep't of Justice (Sept. 12, 1973), *reproduced in* 14 CRIM. L. REP. 2042, 2042 (1973).

211. H.R. REP. NO. 95-1283, pt. I, at 92 (1978) (noting government did not "use evidence obtained or derived from an electronic surveillance" in security prosecutions from 1968 through 1978).

exception arose within discovery disputes. The Supreme Court's 1969 decision in *Alderman v. United States* obligated the government to disclose information obtained from illegal searches or surveillance without regard to its relevancy to the case at hand.[212] For national security investigations, had courts deemed warrantless bugging and wiretapping illegal, *Alderman* would have required the government to disclose the contents of its security operations. The U.S. intelligence community believed such disclosures would jeopardize future operations. Relying on *Katz* and *Keith*, government lawyers successfully limited *Alderman*'s application in security cases by arguing that warrantless bugs and wiretaps were permissible under the Fourth Amendment, thereby avoiding potentially compromising discovery obligations. None of these cases, however, questioned the pure intelligence rule.[213]

4. Levi: A Theory of Pure Intelligence

After Nixon's resignation, the Ford Administration also adhered to the pure intelligence paradigm. In 1976, the FBI approached Ford's Attorney General, Edward Levi, after identifying Truong Dinh Hung as a Vietnamese spy working in the United States.[214] Truong employed a courier to transport classified information to a Vietnamese official in Paris,[215] and the courier, an FBI informant, notified the Bureau. Eager to identify Truong's source inside the U.S. government, the FBI sought authority to open the couriered packages. Levi, however, rejected the FBI's request. Operating under the pure intelligence paradigm, Levi believed any warrantless search of a package would jeopardize future prosecutions of Truong.[216] Truong's first packages went unsearched. (The Carter Administration later reversed this directive and ordered searches of subsequent Truong packages.)[217]

---

212. 394 U.S. 165, 181 (1969).

213. *See* United States v. Humphrey, 456 F. Supp. 51, 57 (E.D. Va. 1978) ("The issue before the Court in [*United States v.*] *Brown* was not whether the conversations overheard through the exercise of this power could be admitted into evidence but whether the interception was illegal, thus necessitating their disclosure under the rule of *Alderman*."); H.R. REP. NO. 95-1283, pt. I, at 92 n.49 (noting early cases did not involve prosecutorial use of wiretapping).

214. *See* GRIFFIN B. BELL, TAKING CARE OF THE LAW 108–09 (William Morrow and Company, Inc. 1982) (recounting request to Levi).

215. Scott J. Glick, *FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security*, 1 HARV. NAT'L SECURITY J. 87, 102–03 (2010).

216. BELL, *supra* note 213, at 109 (summarizing Truong episode). The FBI refused to get a criminal warrant because it feared the notice requirement would jeopardize future operations. *Id.*

217. *See infra* note 230 and accompanying text.

Levi also publicly offered a robust defense of the national security exception as tempered by the pure intelligence rule. In 1975, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (commonly called the "Church Committee") called Levi as a witness "to discuss the relationship between electronic surveillance and the Fourth Amendment."[218] In his testimony, the Attorney General surveyed the executive branch's use of electronic surveillance. "As I read the history," Levi offered, "the policy of the Department of Justice has been that electronic surveillance could be employed without a warrant in certain circumstances," specifically those involving the investigations of foreign threats.[219] Levi also emphasized the executive branch's adherence to the pure intelligence rule, quoting the government's supplemental memorandum in *Black*, as well as other cases in which the government had "emphasiz[ed] that the data [from trespassory surveillance] would not be made available for prosecutorial purposes."[220]

Building on this background, Levi explored the reasons for not using data from warrantless security investigations in subsequent prosecutions. First, Levi noted that such a rule guarded against the pretextual use of security investigations. "Exclusion of evidence from criminal trials may help assure that searches undertaken for ostensibly benign motives are not used as blinds for attempts to find criminal evidence, while permitting searches that are genuinely benign to continue," he explained.[221] Levi's mention of pretext was particularly poignant to his audience: during its tenure, the Church Committee publicly documented various government abuses done in the name of national security, including the warrantless bugging of Martin Luther King, Jr.[222] The Attorney General's statement conceded that if left untempered the national security exception was susceptible to abuse.

Levi's second argument assumed that exceptions to the Fourth Amendment needed to be tailored to minimize intrusiveness. In this vein, Levi concluded that any search that *might* allow the government to obtain admissible evidence was, by its very nature, more intrusive than a government search that could not:

---

218. Levi, *Church Committee Testimony*, *supra* note 18, at 66.

219. *Id.*

220. *Id.* at 68–69 (discussing *Black* and *Schipani* briefs).

221. *Id.* at 78.

222. CHURCH COMMITTEE BOOK III, *supra* note 70, at 81–83 (detailing King wiretapping).

> The effect of a Government intrusion on individual security is a function . . . of disclosure and of the use to which its product is put. Its effects are perhaps greatest when it is employed *or can be employed* to impose criminal sanctions or to deter, by disclosure, the exercise of individual freedoms. In short, the use of the product seized bears upon the reasonableness of the search.[223]

Levi herein suggested that even if the government did not originally intend, or even foresee, a search being useful for prosecution, a prophylactic rule barring prosecutorial uses reduced a search's intrusiveness as it was being conducted. Thus, the pure intelligence rule helped satisfy the need to tailor intrusive investigations.[224]

Lastly, Levi offered a pragmatic defense of the pure intelligence rule. "Until very recently—in fact, until the Court's 1971 decision in *Bivens v. Six Unknown Federal Narcotic Agents*—the only sanction against an illegal search was that its fruits were inadmissible at any criminal trial of the person whose interest was invaded," he noted.[225] "In practical effect, a search could only be 'unreasonable' as a matter of law if an attempt was made to use its fruits for prosecution . . . . So long as the Government did not attempt such use, the search could continue and the Government's interests, other than enforcing criminal laws, could be satisfied."[226] The self-restraint of the pure intelligence rule therefore ensured the reasonableness of warrantless surveillance from a historical perspective. "It may be said that this confuses rights and remedies; searches could be unreasonable even though no sanction followed. But I am not clear that this is theoretically so, and realistically it was not so," Levi concluded.[227]

Levi's testimony offers a comprehensive defense of the national security exception as conducted within the pure intelligence paradigm. Warrantless intelligence searches, according to the Attorney General, were permissible under a Fourth Amendment primarily geared toward regulating law enforcement. Adherence to the pure intelligence rule guarded against pretextual abuse of the exception and tailored

---

223. Levi, *Church Committee Testimony*, *supra* note 18, at 78 (emphasis added).

224. At the time, Levi's tailoring emphasis had particular importance in light of *Terry v. Ohio*, which stated searches needed to be "strictly circumscribed by the exigencies which justify [their] initiation." 392 U.S. 1, 25–26 (1968). Some courts initially read *Terry* "as imposing a least intrusive alternative requirement upon all investigative detentions not justified under the traditional probable cause standard." Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis,* 63 N.Y.U. L. REV. 1173, 1216 (1988). The Supreme Court, however, subsequently "refused to declare that only the least intrusive search practicable can be reasonable under the Fourth Amendment." City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) (internal quotation marks omitted).

225. Levi, *Church Committee Testimony*, *supra* note 18, at 78.

226. *Id.* at 101.

227. *Id.*

security investigations to ensure constitutional reasonableness. Though he was not the first to explain the legal theory behind early national security investigations, Levi offered the most cogent argument to defend three decades of investigatory practices geared towards foreign threats.

D. Conclusion: Early Security Investigations and Pure Intelligence

Whether *opinio juris* genuinely guided the practice described here—three decades of significant but circumscribed intelligence gathering using invasive investigative techniques—is worth pondering. In some cases, the government's investigatory conduct preceded its legal theory. The FBI in particular was sometimes guilty of a shoot-first-and-ask-questions-later attitude, failing to seek clear judicial guidance until years after the fact.[228] Despite widespread warrantless surveillance, prosecutors from this era did not knowingly introduce evidence from any warrantless bug or tap at trial.[229] The total number of prosecutions this disrupted is unclear, since the government acknowledged some unidentified cases remained in "cold storage" due to evidentiary issues posed by the pure intelligence rule.[230] The cases identified here, however, show that the rule was more than a theoretical exercise, and the Fourth Amendment remained an influential force in national security matters.

Since the postwar and Cold War periods studied here, the government has occasionally strayed from the pure intelligence rule. During the espionage prosecution of Truong Dinh Hung (mentioned above) and his accomplice, Ronald Humphrey, prosecutors in the Carter Administration proffered evidence obtained through warrantless mail searches and electronic surveillance. The Fourth Circuit accepted the evidence on the theory that the "primary purpose" of the investigation was nonprosecutorial.[231] In 2000, the government submitted evidence against al Qaeda member Wadih El-Hage

228. This attitude predated the early security investigation period reviewed here. Katyal & Caplan, *supra* note 8, at 1038 (noting that during run-up to World War II, "[t]he lack of specific legal authority for such FBI intelligence investigations does not appear to have been a concern to FDR or Hoover").

229. The ratio of identified-to-prosecuted spies during this period is similarly disparate. HAYNES & KLEHR, *supra* note 21, at 11 ("Historical evidence that has become available since the end of the Cold War shows that several hundred Americans spied for the Soviet Union, but only a fraction of these, several dozen, were ever prosecuted."). Two scholars attribute the meager prosecutorial number partially to "bitterly disputed evidence that continued to be challenged as tainted for years after the trials." *Id.*

230. *See supra* note 176 and accompanying text.

231. United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980).

gathered from a warrantless search and wiretap of his Kenyan home.[232] And in 2004, the government presented to a grand jury evidence gleaned from the warrantless search of the Mississippi home of Abdelhaleem Ashqar, who was later indicted for his support of Hamas.[233]

These cases, however, constitute exceptions to general practice. The *Truong* case was the first deviation from the pure intelligence rule since World War II. Since then, less than a half-dozen national security cases have involved evidence from warrantless Fourth Amendment techniques.[234] Out of thousands of investigations and hundreds of trials, only the rarest national security case has involved evidence from warrantless surveillance or searches.[235] Similarly, as described below, the Justice Department has not used information obtained from the government's modern warrantless surveillance programs in subsequent trials.[236]

In those few exceptions to the pure intelligence rule, courts have admitted evidence obtained without a warrant on a basis other than the national security exception. In the *El-Hage* case, for example, the Second Circuit avoided the national security exception altogether, instead deciding the case based on the Fourth Amendment's applicability outside the United States.[237] Similarly, in the *Ashqar* case, the district court concluded suppression was unnecessary based on a mixed rationale of good faith and the fact that Congress had, subsequent to the search, imposed a warrant requirement for domestic physical searches, essentially mooting the relevance of the constitutional question at hand.[238]

United States v. Truong Dinh Hung, the one decision to squarely permit the prosecutorial use of information collected pursuant to the national security exception, has been much maligned.

---

232. United States v. Bin Laden, 126 F. Supp. 2d 264, 268 (S.D.N.Y. 2000).

233. United States v. Marzook, 435 F. Supp. 2d 778 (N.D. Ill. 2006); *see also* Michael Higgins, *Palestinian Found in Contempt Gets 11 Years*, L.A. TIMES (Nov. 22, 2007), http://articles.latimes.com/2007/nov/22/nation/na-activist22 (reporting Ashqar's sentence for contempt); Dan Eggen & Jerry Markon, *Hamas Leader, 2 Others Indicted*, WASH. POST, Aug. 21, 2004, at A4.

234. In addition to *Truong Dinh Hung*, *Bin Laden*, and *Marzook*, see also United States v. Ajlouny, 629 F.2d 830, 840 (2d Cir. 1980) (concluding suppression of evidence from warrantless wiretap was constitutionally unnecessary).

235. *See supra* note 1 and accompanying text.

236. *See infra* notes 291–294 and accompanying text.

237. *In re* Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 171–72 (2d Cir. 2008) (noting "[t]he District Court's recognition of an exception to the warrant requirement for foreign intelligence searches" but "declin[ing] to adopt this view"); *Marzook*, 435 F. Supp. 2d at 788–91.

238. *Marzook*, 435 F. Supp. 2d at 788–91.

One federal court recently concluded that *Truong* imposed "an 'unstable, unrealistic, and confusing' line" in establishing its primary purpose test.[239] Government efforts to comply with the primary purpose test—an arrangement known as the "FISA wall"—led to allegations of intelligence failures and hampered various high-profile investigations, including surveillance of the September 11 attackers.[240] Moreover, *Truong* entirely ignored the extensive record of past executive practice—a record that served as the context to the Supreme Court's opinions in *Katz* and *Keith*.[241] *Truong* therefore does not outweigh the decades of "gloss" generated by the practice of executive branch officials, as recounted in this Article. The next Part of this Article discusses the precedential relevance of this prolonged practice, particularly within the context of the surveillance programs facing legal challenges today.

IV. THE MODERN RELEVANCE OF EARLY SECURITY INVESTIGATIONS

As demonstrated above, national security investigations proceeded under a pronounced limit for decades. Under this paradigm, federal agents conducted thousands of wiretapping, bugging, black bag, and mail-chamfering operations but only used the collected information for intelligence, as opposed to evidentiary, purposes. Records show that this limited use resulted from decisions by the executive branch's leadership to keep such information out of courtrooms and to halt prosecutions apparently tainted by these techniques, in keeping with Fourth Amendment strictures. In sum, the historical record shows a longstanding Fourth Amendment exception for national security but a similarly longstanding circumscription of information gleaned from such searches.

This Part considers the relevance of early executive practice to modern debates about the Fourth Amendment and national security.

---

239. *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008) (quoting *In re* Sealed Case, 310 F.3d 717, 743 (FISA Ct. Rev. 2002)).

240. The "FISA wall" refers to procedures installed by the Justice Department and intelligence community to avoid claims that the executive branch abused FISA authorities as an end-run around the constitutional and statutory restraints on run-of-the-mill law enforcement. The procedures essentially cleaved the FBI into two different bodies—intelligence and law enforcement—and restricted the flow of information-sharing between the two. *See generally* David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006).

241. Instead, *Truong Dinh Hung* concluded cursorily that evidence must be admissible because "almost all foreign intelligence investigations are in part criminal investigations." United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980). As shown here, that statement is incorrect.

First, this Part evaluates the legal significance of the pure intelligence rule and its policy merits as a method for regulating the executive branch. It then juxtaposes modern surveillance programs—particularly those now authorized by FISA—against the surveillance operations of the pure intelligence era.

A. The Legal and Practical Merits of Pure Intelligence

The national security exception and the pure intelligence rule both have ongoing relevance in modern Fourth Amendment jurisprudence. This Section examines the place of both doctrines within the modern legal and policy landscape.

1. National Security, Pure Intelligence, and Special Needs

Sometimes legal debates and practices of the past lose their importance as a doctrine evolves over time. In this domain, however, the interlocking rules that governed early national security cases—the national security exception and the pure intelligence rule—dovetail with modern Fourth Amendment jurisprudence. As discussed above, national security (more commonly referred to now as "foreign intelligence") has become a "recognized exception" to Fourth Amendment rules.[242]

Likewise, the pure intelligence rule has equal jurisprudential relevance, particularly in the context of the "special needs" doctrine. The special needs doctrine holds that "a judicial warrant and probable cause are not needed where the search or seizure is justified by special needs, beyond the normal need for law enforcement."[243] As discussed in Part I, national security investigations extend beyond basic law-enforcement objectives by serving military, diplomatic, and other policymaking functions; and prosecutions are, as a matter of course, a relatively rare outcome of such investigations.[244] Various scholarly proposals have therefore suggested treating national security as a subset of special needs.[245] Some recent judicial opinions also link the national security exception to special needs. In 2002, the FISA Court

242. *See supra* note 208 and accompanying text.

243. Ashcroft v. al-Kidd, 131 S. Ct. 2074, 2081 (2011) (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)) (internal quotation marks omitted).

244. *See supra* notes 25–26 and accompanying text (discussing security investigations' objectives).

245. *See* Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 777–78 (2004) (suggesting courts uphold suspicionless counterterrorism searches based on special needs); Birkenstock, *supra* note 61, at 843 (proposing special needs as justification for warrantless wiretapping in security investigations).

of Review—a specialized court established to deal with FISA-related matters—detailed the parallels between security investigations and special needs searches.[246] Similarly, in 2008, the same court concluded that national security and special needs were "comparable exception[s]," excusing the warrant requirement.[247]

Treating national security as akin to a "special need" also bolsters the pure intelligence rule's relevance. In many special needs cases outside the security context, courts have found governmental practices analogous to the pure intelligence rule to be constitutionally probative. For example, the Supreme Court noted that the drug-testing program challenged in the hallmark special needs case *National Treasury Employees Union v. Von Raab* limited the use of its results to nonprosecutorial purposes: employees who tested positive for narcotics were fired, but regulations forbid handing the results "to any other agency, including criminal prosecutors, without the employee's written consent."[248] In *Vernonia School District 47J v. Acton*, a school drug-testing case, the Supreme Court noted in finding the searches reasonable that "the results of the [drug] tests are disclosed only to a limited class of school personnel who have a need to know; and they are not turned over to law-enforcement authorities or used for any internal disciplinary function."[249] The Supreme Court has therefore found governmental self-restraint in the use of the collected evidence to be probative in evaluating Fourth Amendment challenges.

Conversely, when drug-testing results are used in subsequent prosecutions, the judiciary imposes greater scrutiny and has found certain searches to violate the Fourth Amendment. In *Ferguson v. City of Charleston*, a state hospital tested women receiving prenatal treatment for narcotics use; prosecutors used some positive results in subsequent trials.[250] On appeal, the Supreme Court struck down the program, which the state government sought to justify on special needs grounds. The majority concluded that the involvement of law enforcement rendered the program unconstitutional. "While the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence for *law-enforcement purposes* in order to reach that goal," the majority

246. *In re* Sealed Case, 310 F.3d 717, 745–46 (FISA Ct. Rev. 2002).

247. *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1010–11 (FISA Ct. Rev. 2008).

248. 489 U.S. 656, 662 (1989).

249. 515 U.S. 646, 658 (1995); *see also In re Directives*, 551 F.3d at 1010 (citing *Acton*).

250. 532 U.S. 67, 70–71 (2001). To support prosecutions, officials amended testing procedures to establish a chain of custody. *Id.* at 82.

concluded.[251] "In none of our previous special needs cases have we upheld the collection of evidence for criminal-law-enforcement purposes."[252]

Cases like *Acton*, *Ferguson,* and *Von Raab* indicate how prosecutorial use of information affects the constitutional reasonableness of a search. In the national security context, at least one court has found prosecutorial restraint to be constitutionally relevant to a security program's reasonableness. In *MacWade v. Kelly*, the Second Circuit evaluated New York City's subway search program imposed after the 2005 London tube bombings.[253] The opinion, while describing the program and assessing its constitutionality, noted that the government had not used the searches to pursue normal law-enforcement purposes. "[T]hus far there have been no arrests for general crimes stemming from the seizure of non-explosive contraband discovered during a search conducted pursuant to the [subway search] Program," the court noted favorably.[254] The court ultimately upheld the search because "preventing a terrorist attack on the subway is a special need" and "even though the searches intrude on a full privacy interest, they do so to a minimal degree."[255]

These special needs cases, in and out of the security context, establish that the pure intelligence rule can fit comfortably within modern Fourth Amendment jurisprudence.[256] Nonprosecutorial rules and practices have informed judicial inquiries about the constitutional reasonableness of government searches. Even if the special needs doctrine does not go so far as to totally preclude the prosecutorial use of evidence obtained from warrantless security searches, these decisions indicate that such governmental conduct is nonetheless constitutionally relevant.

2. The Incentives of the Pure Intelligence Rule

Aside from its legal significance, the pure intelligence rule promises significant practical benefits. This Section briefly discusses how the pure intelligence rule incentivizes restraint by the executive

---

251. *Id.* at 82–83 (internal citation omitted).

252. *Id.* at 83 n.20.

253. 460 F.3d 260 (2d Cir. 2006).

254. *Id.* at 265 n.1.

255. *Id.* at 275.

256. The national security exception predates the "special needs" doctrine and so can be thought of as analytically distinct from special needs jurisprudence. Indeed, national security investigations implicate constitutional powers of the president in ways that school searches and drug testing do not. However, for those who wish to fold national security searches within the existing special needs jurisprudence, the pure intelligence rule still holds relevance.

without unnecessarily compromising the efficacy of national security investigations.

In general, the pure intelligence rule reduces the costliness of national security surveillance upon law-abiding citizens. As Edward Levi testified in 1975, the price of a "[g]overnment intrusion on individual security is a function . . . of disclosure and of the use to which its product is put"; a search's effect on the searched is "perhaps greatest when it is employed or can be employed to impose criminal sanctions."[257] Arrest, conviction, and imprisonment—whether imposed on the innocent or the guilty—are some of the highest costs the state can impose upon the citizenry.[258] Circumscribing the prosecutorial uses of intelligence reduces the frequency with which these costs are generated, thereby minimizing the impact of security investigations on the nation.

Additionally, the pure intelligence rule eliminates the incentive for officers to use the national security exception for law-enforcement purposes. As any information collected under the pure intelligence rule is inadmissible in court, such searches serve little purpose to law-enforcement agents focused on prosecution. The pure intelligence rule therefore guards against the pretextual use of security investigations as a means of sidestepping the traditional warrant and probable cause requirements. Reinforcing traditional Fourth Amendment protections, the pure intelligence rule also reduces the number of overall searches as well as the number of "empty searches"—searches of innocent citizens—by limiting law-enforcement searches to cases where the government can establish predicate suspicion. Empty searches impose significant costs upon law-abiding persons (lost time, damages to personal property, loss of bodily integrity, dignity costs, damage to reputation, etc.), and the government should take particular care to protect against such errors.[259]

The pure intelligence rule also helps elucidate how the criminal justice system functions as a dual-use tool, serving both security and nonsecurity purposes. In addition to the government's more traditional national security tools—diplomacy, sanctions, military

257. Levi, *Church Committee Testimony*, *supra* note 18, at 78. Errant arrests and false convictions have extraordinary costs, and national security investigations do not have a perfect record. *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1033 (D. Or. 2007) (describing arrest of innocent citizen mistakenly identified as terrorist).

258. *See, e.g.*, Harry J. Holzer, *Collateral Costs: Effects of Incarceration on Employment and Earnings Among Young Works*, *in* DO PRISONS MAKE US SAFER? 249–51 (Steven Raphael & Michael A. Stoll eds., 2009) (surveying incarceration's effects on wages and employment).

259. *See* L. Rush Atkinson, *The Bilateral Fourth Amendment and the Duties of Law-Abiding Persons*, 99 GEO. L.J. 1517, 1526–27 (2011) (discussing empty searches and related costs).

options, and so on—the government must also be sensitive to the fact that prosecuting foreign threats can have unintended nonsecurity implications.[260] Because criminal law and criminal procedure operate under the "transsubstantive" principles that "treat[] one crime just like another," accommodation of national security prosecutions can generate a variety of nonsecurity externalities.[261] Some commentators, for example, allege that the judiciary relaxed the probable cause standard omnipresent in criminal procedure in the wake of the September 11 attacks out of a fear that a more robust standard would stifle counterterrorism efforts.[262] Rules that cabin security investigations from traditional law-enforcement operations reduce the chances of legal seepage—seepage that risks the erosion of civil liberties in situations beyond those directly involving national security threats.

Of course, the pure intelligence rule is susceptible to a variety of complaints. Civil libertarians could argue that the rule, by itself, does not go far enough to minimize the costs of national security investigations. Even without the prospect of conviction or incarceration, searches impose a variety of dignitary harms, reputational injuries, and other costs, which the pure intelligence rule does little to minimize. From the other side of the aisle, security-minded commentators might note that the merits of the pure intelligence rule do not necessarily outweigh the effectiveness of criminal trials as a national security tool. As many politicians and

260. Developments in nonsecurity sectors carry "security externalities." *See* Joanne Gowa & Edward D. Mansfield, *Power Politics and International Trade*, 87 AM. POL. SCI. REV. 408 (1993) (outlining "security externalities"); *see also* Grutter v. Bollinger, 539 U.S. 306, 330–31 (2003) (discussing affirmative action's military effect). The converse—that security operations have nonsecurity implications—is equally true.

261. Stuntz, *Transsubstantive Fourth Amendment*, *supra* note 29, at 847. Transsubstantivity's strong form argues there is no security exception. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Douglas, J., concurring) (arguing that "spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers"). The Fourth Amendment's "transsubstantivity" has come under heavy fire over the years as leading to inefficient levels of policing. *See* Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness*,*"* 98 COLUM. L. REV. 1642, 1673 (1998) (observing that "the Court has tended to overlook substantive matters in evaluating the reasonableness of a challenged search or seizure"); John Kaplan, *The Limits of the Exclusionary Rule*, 26 STAN. L. REV. 1027, 1046 (1974) (proposing that the exclusionary rule "not apply in the most serious cases," such as murder and other violent crimes); Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 1015 (2003) (championing alternative to viewing probable cause as "single and inflexible standard"); Stuntz, *Policing After the Terror*, *supra* note 29, at 2146 (arguing that Fourth Amendment law should ensure that "in containing the predators, we do not make for even worse predation").

262. *See* Stuntz, *Policing After the Terror*, *supra* note 29, at 2157–58 (discussing Court's deferential attitude in *United States v. Arvizu*, 534 U.S. 266 (2002), a Fourth Amendment case heard by the Supreme Court closely after the September 2001 attacks).

scholars have explained, the criminal justice system can assist general counterterrorism and counterespionage efforts by neutralizing foreign agents and deterring future ones.[263] Reducing the amount of admissible evidence inevitably cuts into the usefulness of prosecutions as a national security tool.

Even with these objections duly noted, the pure intelligence rule regulates security investigations with a clear and appreciable logic. Restricting the government's access to the criminal system in certain security cases installs practical protections for law-abiding persons and avoids some of the largest costs that government searches can generate. Conversely, the pure intelligence rule takes one manner of response from the government's arsenal but leaves others—no-fly lists, visa bans, interdictions, and so on—intact. The rule also does not blind the executive; rather it allows the executive to identify foreign threats and respond. With its practicality and vintage, the pure intelligence rule holds precedential importance, a subject to which this Article now turns.

B. The Constitutional Gloss of the Pure Intelligence Rule

As noted above, the executive's historical practice offers a "gloss" for understanding the scope of its constitutionally permissible and impermissible conduct.[264] Similarly, government officials have explicitly defended modern security surveillance programs by reference to historical practice,[265] but these arguments either overlook or ignore the executive's enduring adherence to the pure intelligence rule. This Article closes by considering how the gloss of the pure intelligence era should affect our view of modern surveillance programs.

To determine the relevance of earlier practice, this Article examines two modern surveillance programs, both authorized under FISA. The first involves the use of judicially issued "intelligence warrants" and the prosecutorial use of information derived therefrom. This practice recently prompted a spate of litigation, particularly after the PATRIOT Act amended the scheme in 2001. The second

263. Many have noted the usefulness of prosecutions as a counterterrorism and counterespionage tool. *See, e.g.*, Kris, *supra* note 1, at 605 ("While our criminal justice system has limits . . . when it is the right [counterterrorism] tool it has an exceptional success rate."); Press Release, President Barack Obama on the Passage of H.R. 6523 (Jan. 7, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/12/31/statement-president-hr-1540 ("The prosecution of terrorists in Federal court is a powerful tool in our efforts to protect the Nation and must be among the options available to us.").

264. *See supra* notes 45–50 and accompanying text.

265. *See supra* notes 53–55 and accompanying text.

surveillance program involves warrantless electronic surveillance of suspects believed to be overseas; this surveillance is authorized under section 702 of FISA, added by statute in 2008. This new program is the subject of pending lawsuits challenging its constitutionality under the Fourth Amendment.

1. Intelligence Warrants and Intelligence-Based Prosecutions

National security investigations changed dramatically in 1978 when Congress passed the first iteration of FISA (now known as Title I of FISA). FISA requires that electronic surveillance during security investigations be conducted pursuant to judicial authorization.[266] To handle the particular needs of security investigations, FISA also established a new "intelligence warrant" regime by creating a specialized federal court called the Foreign Intelligence Surveillance Court. The court is authorized to issue a warrant if there is probable cause to believe that a targeted suspect is a foreign power or its agent.[267]

FISA also provides that the government can use evidence collected pursuant to intelligence warrants in subsequent criminal trials. FISA contemplates that the government may "enter into evidence or otherwise use or disclose in any trial . . . information obtained or derived from an electronic surveillance" conducted pursuant to an intelligence warrant.[268] Over the last thirty years, FISA warrants have become a common source for evidence in security cases, with prosecutors introducing the results of FISA-authorized surveillance in various terrorism, espionage, and other security cases.[269] Defendants, in turn, have lodged a slew of constitutional challenges to the use of FISA-derived evidence at trial.[270]

---

266. 50 U.S.C. § 1812 (2012) (describing extent to which FISA "shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted"). In 1994, that requirement was extended to physical searches conducted in the course of national security investigations, a requirement now found in Title III of FISA. *Id.* § 1825.

267. *Id.* § 1804.

268. *Id.* § 1806(c).

269. *See, e.g.*, United States v. Hovsepian, No. CR 82–917, 1985 WL 5970, at *1 (C.D. Cal. Jan. 25, 1985); United States v. Megahey, 553 F. Supp. 1180, 1182 (E.D.N.Y. 1982); United States v. Falvey, 540 F. Supp. 1306, 1307–08 (E.D.N.Y. 1982).

270. *See, e.g.*, United States v. Duka, 671 F.3d 329, 337 (3d Cir. 2011); United States v. El-Mezain, 664 F.3d 467, 563 (5th Cir. 2011); United States v. Abu-Jihad, 630 F.3d 102, 117 (2d Cir. 2010) (listing Fourth Amendment challenges); United States v. Stewart, 590 F.3d 93, 99 (2d Cir. 2009); United States v. Campa, 529 F.3d 980, 993 (11th Cir. 2008); United States v. Hammoud, 381 F.3d 316, 331 (4th Cir. 2004); United States v. Miller, 984 F.2d 1028, 1032 (9th Cir. 1993);

Some may argue the practice of early security investigations suggests that the prosecutorial use of FISA-derived information runs afoul of the Fourth Amendment; however, the prolonged adherence to the pure intelligence rule must be viewed in the context of the searches it regulated. During the early era studied in Part III, federal officials conducted national security investigations without any judicial supervision or warrant procedures. When Congress occasionally proposed imposing a warrant requirement on national security investigations during this period, the executive branch successfully opposed those bills by arguing that judicial review would compromise national security.[271] At the same time, executive officials conceded that some curb on security investigations was constitutionally (and politically) necessary; the solution was the pure intelligence rule. That rule, in other words, was intended to regulate *warrantless* surveillance and searches, and the practice helped avoid judicial review. Imposing a *warrant requirement* upon certain security investigations, as Title I of FISA does, reduces the need for self-regulation like the pure intelligence rule.[272]

The significance of the distinction between warrant and warrantless searches is highlighted by the Supreme Court's *Keith* opinion, which addressed both types of searches separately. The Court considered the scope of permissible warrantless surveillance in national security investigations but ultimately refrained from opining on "the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country"—though, as described in Part III.C, the executive interpreted the Court's agnosticism as a blessing of the exception.[273] The *Keith* opinion, however, also discussed the possibility of intelligence warrants, which the Court determined *satisfy*, rather than sidestep, the Warrant

---

United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988); United States v. Badia, 827 F.2d 1458, 1462 (11th Cir. 1987).

271. For example, Congress repeatedly proposed relaxing section 605's prosecutorial bar on wiretapping evidence, provided the executive seek warrants before wiretapping. *See* EDWARD V. LONG, THE INTRUDERS 147–55 (1966) (describing wiretapping bills between 1929 and 1966, including warrant proposals). The FBI and Justice Department responded that "they would rather have no bill [admitting wiretapping evidence] than one requiring a court order." Milton Magruder, *House Action Expected Today on Wiretap Measure*, WASH. POST, Apr. 8, 1954, at 8. Herbert Brownell, Eisenhower's Attorney General, explained later, "I also favored the admissibility of evidence obtained from wiretaps in criminal cases, but I was willing to forgo its use in court if that was necessary so that electronic surveillance in intelligence cases [i.e., warrantless wiretaps] could continue." BROWNELL & BURKE, *supra* note 123, at 233.

272. The same analysis applied to Title III of FISA, which extends the intelligence-warrant requirement to physical searches. *See supra* note 4.

273. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 308 (1972); *see also supra* notes 207–08 (describing lower court interpretations of *Katz* and *Keith*).

Clause's requirements. The Court clarified that, apart from the Fourth Amendment's national security exception, "[d]ifferent standards" for intelligence warrants "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[274]

Similarly, part of FISA's initial appeal to lawmakers was the prospect of using electronic surveillance as trial evidence. In notes from a Situation Room briefing in March 1976 about the prospect of surveillance legislation, Edward Levi (whose support for such legislation was politically vital)[275] listed the "[p]ros" of supporting the new warrant bill. The first pro noted that the "[r]equirement of [a] warrant for surveillance" in security investigations would "eliminate[] question[s] of validity of [the] evidence obtained."[276] In other words, Levi recognized that in exchange for judicial review, prosecutorial use of wiretapping and bugging would be possible. His notes show how FISA's warrant requirement resulted from some horse trading: prosecutorial use of information in exchange for greater oversight over security investigations.

Given this historical and legal context, the FISA intelligence-warrant scheme is constitutionally defensible without relying on the Fourth Amendment's national security exception, which *excuses,* rather than satisfies, the warrant requirement. The use of evidence from intelligence warrants, therefore, is a distinguishable, but not inconsistent, practice compared to that of the earlier eras examined in this Article. The gloss of the pure intelligence era, therefore, does not undermine the prosecutorial use of information gleaned from FISA's intelligence warrants.

2. Warrantless Searches and Modern Pure Intelligence Practice

Not all modern surveillance has been conducted pursuant to warrants. For example, FISA did not authorize warrants for physical searches until 1994, so the FBI conducted some physical searches in the 1990s without judicial authorization.[277] More recently, warrantless

274. *Id.* at 322–23.

275. Though FISA was not passed until 1978, after Levi's tenure as Attorney General, his endorsement was nonetheless vital. *See* Funk, *supra* note 15, at 1111–12 (describing Levi's role in passage of FISA).

276. Talking Points from Meeting Regarding Legislation on Electronic Surveillance for Foreign Intelligence Purposes 1 (Mar. 12, 1976), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv8b.pdf.

277. Government agents, for example, searched Aldrich Ames's home without a warrant during an espionage investigation in 1993. S. REP. NO. 103-296, at 40 (1994). Today, FISA

surveillance has become a significant part of major counterterrorism operations. The Terrorist Surveillance Program, for instance, allegedly collected thousands of transnational calls without judicial approval.[278] And while FISA initially authorized only surveillance pursuant to a warrant, Congress recently amended the statute to permit certain warrantless surveillance. Today that authorization is found in section 702 of FISA, added through the FISA Amendments Act of 2008 ("FAA").[279]

In many important respects, modern warrantless surveillance is analogous to the early national security investigations discussed in Part III. Like earlier operations, today's warrantless surveillance can occur without agents first establishing probable cause. Section 702 of FISA, for example, eliminates the probable cause showing that Titles I and III of FISA require.[280] Instead, section 702 only requires a "reasonabl[e] belie[f]" that the target is a non-U.S. person located outside the United States and that the collection has a foreign intelligence purpose.[281] Modern warrantless surveillance is also conducted with minimal judicial review, much like its historical antecedents. Whereas a court issues FISA warrants based on its review of an individualized application setting forth the things to be searched and the predicate suspicion, section 702 does not require the government to submit such applications for each target of warrantless surveillance. Instead, section 702 only compels judicial review of the surveillance program's general protocols for the collection, retention, and dissemination of information.[282] While these relaxed standards

---

requires an intelligence warrant for physical searches inside the United States. *See supra* note 264.

278. *See* Katyal & Caplan, *supra* note 8, at 1029–34 (describing NSA program). The Author has no personal knowledge of this program.

279. Pub. L. No. 110–261 § 101, 122 Stat. 2436, 2437 (adding Title VII). For background on section 702, see Letter from James R. Clapper, Dir. of Nat'l Intelligence, U.S. Dep't of Defense, and Attorney Gen. Eric A. Holder, Jr. to Representatives John Boehner and Nancy Pelosi and Senators Harry Reid and Mitch McConnell (Feb. 8, 2012), *available at* http://www.justice.gov/ola/views-letters/112/02-08-12-fisa-reauthorization.pdf.

280. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 126 (2d Cir. 2011) ("[W]hereas under the preexisting FISA scheme the FISC had to find probable cause . . . under the FAA the FISC no longer needs to make any probable-cause determination at all.").

281. 50 U.S.C. § 1881a(a) (2012). Similarly, the FAA does not require the government to establish probable cause of a targeted facility's use by the suspect. *Id.* § 1881a(d). While section 702 reduced the probable cause requirement, other parts of the FAA—specifically sections 703 and 704—expanded the warrant requirement to U.S. persons targeted abroad. *Id.* §§ 1881b & 1881c.

282. *See id.* § 1881a(i)(2) (authorizing court to review certification process, targeting procedures, and minimization procedures); *id.* § 1881a(i)(3)(A) (compelling judiciary to permit collection if satisfied targeting, minimization, and certification procedures sufficient); *see also Clapper*, 638 F.3d at 124 ("The FAA, in contrast to the preexisting FISA scheme, does not require

give the government more leeway in investigating foreign threats, there is little question that such surveillance programs do not satisfy the Warrant Clause (even under the relaxed *Keith* standard) and therefore must fall within some exception to that clause.[283]

In recent years, the government's warrantless surveillance programs have faced robust constitutional challenges, and courts have reached different conclusions. Shortly after the government's Terrorist Surveillance Program was revealed in 2005, the ACLU and others filed a lawsuit challenging the program's constitutionality. The litigation was eventually dismissed on standing grounds, but not before a district court issued an opinion finding the program "obviously in violation of the Fourth Amendment."[284] In contrast, another warrantless surveillance regime established by the FAA's predecessor, the Protect America Act of 2007, was upheld by the FISA Court of Review in 2008.[285] That court concluded such surveillance did not violate the Fourth Amendment because it fell within the "foreign intelligence exception to the Fourth Amendment's warrant requirement."[286]

Such litigation continues: in 2013, the Supreme Court issued a five-to-four decision in *Clapper v. Amnesty International USA*, in which the litigants challenged the constitutionality of section 702 on Fourth Amendment grounds.[287] The *Clapper* plaintiffs were "attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad."[288] None of the plaintiffs had any definitive evidence that they had actually been overheard through section 702 surveillance. Rather, their standing claim was based on allegations that they had to take precautions—

---

the government to submit an individualized application . . . identifying the particular targets or facilities to be monitored.").

283. *See In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1010–11 (FISA Ct. Rev. 2008) (assuming Protect America Act did not satisfy Warrant Clause).

284. ACLU v. NSA, 438 F. Supp. 2d 754, 775 (E.D. Mich. 2006), *vacated by* 493 F.3d 644 (6th Cir. 2007). The district court concluded that the program was unreasonable because it lacked "prior-existing probable cause, as well as particularity as to persons, places, and things, and the interposition of a neutral magistrate between Executive branch enforcement officers and citizens." *Id.*

285. *In re Directives*, 551 F.3d at 1008. This case involved a service provider that refused to assist the government's warrantless surveillance of a foreign target, alleging that the surveillance, though statutorily authorized, violated the Fourth Amendment. *Id.* at 1008.

286. *Id.* at 1012, 1016.

287. 133 S. Ct. 1138 (2013).

288. *Id.* at 1145.

avoiding electronic communications, taking meetings in person rather than teleconferencing, and so on—on the chance that their conversations would be monitored.[289] Five Justices, however, found these grounds too "highly speculative" to establish standing and dismissed the claim, overturning the Second Circuit decision.[290]

All of these cases highlight one important parallel between early and recent warrantless surveillance: information from modern warrantless programs remains limited to nonprosecutorial purposes. In *Clapper*, for example, the plaintiffs conceded that "[a]s far as [they were] aware, the government has yet to introduce FAA-derived evidence in a criminal trial, though four years have passed since the statute was signed into law."[291] The *Clapper* majority implicitly acknowledged this fact but rejected the argument that the potential "insulation" of government surveillance was a reason to find standing for the plaintiffs.[292] Similarly, in *ACLU v. National Security Agency*, litigation challenging the Bush Administration's Terrorist Surveillance Program, the Sixth Circuit noted "that the [National Security Agency] has not disclosed or disseminated any of the information obtained via this warrantless wiretapping."[293] There was no evidence, Chief Judge Batchelder noted, that any surveillance had been used in criminal prosecutions or other analogous proceedings.[294] These and similar observations suggest that modern warrantless surveillance programs, like the early investigations described above, have followed a pure intelligence rule.

Modern adherence to the pure intelligence rule appears to be more de facto practice than affirmative policy (much like the initial postwar years described above).[295] The government has not acknowledged any evidentiary self-circumscription in the conduct of its warrantless surveillance programs, as it did in the 1960s in the *Black* and *Schipani* briefs.[296] Nor is the government statutorily prohibited from using such information in criminal proceedings; the

289. *Id.* at 1146.

290. *Id.* at 1148.

291. Brief for Respondents at 58, *Clapper*, 133 S. Ct. 1138 (No. 11-1025), 2012 WL 4361439, at *58. Similarly, during oral arguments before the Supreme Court, plaintiffs' counsel argued that "the government has made clear that it's not going to" use section 702 evidence in a criminal trial because "the main purpose of this statute is not to gather evidence for law enforcement." Transcript of Oral Argument at 42–43, *Clapper*, 133 S. Ct. 1138 (No. 11-1025).

292. 133 S. Ct. at 1154.

293. 493 F.3d 644, 671 (6th Cir. 2007) (Batchelder, J.).

294. *Id.* at 653 (noting plaintiffs did not allege use of surveillance information in "criminal prosecution, deportation, administrative inquiry, [or] civil litigation").

295. *See supra* Part III.A.

296. *See supra* Part III.C.1.

FAA explicitly permits the prosecutorial use of information from warrantless surveillance.[297] On the other hand, the United States did not challenge the plaintiffs' description of the government's (non)use of section 702 information in *Clapper*. Similarly, this Author's review has found no record of the United States notifying a defendant of the government's intention to use section 702 information in a criminal or similar proceeding, as statutorily mandated.[298] Because modern warrantless surveillance programs date back to at least 2002 (with the initiation of the Terrorist Surveillance Program), publicly available evidence suggests that the government's administration of these programs has followed the pure intelligence rule for over a decade.[299]

Just as the government's self-restraint during earlier national security investigations strengthened its claims of compliance with the Constitution, the government's restraint today should factor into Fourth Amendment evaluations of modern warrantless surveillance programs. As described above, adherence to the pure intelligence rule reduces the intrusiveness of national security surveillance upon law-abiding citizens.[300] Similarly, following the pure intelligence rule guards against pretextual use of national security investigations, indicating the government is not using the new provisions of FISA to ease its traditional law-enforcement duties. When balancing the government and privacy interests under the Fourth Amendment, these factors support the constitutionality of national security surveillance.

Even without the government acknowledging any evidentiary self-circumscription, the empirical absence of information obtained without a warrant in criminal trials should weigh into the evaluation of such conduct's constitutional reasonableness. Appellate courts have weighed similar empirical records. In *MacWade v. Kelly* (the subway search case), the government did not acknowledge any policy that

---

297. *See* 50 U.S.C. § 1881e (2012) (providing that the use of FAA-acquired information shall be regulated by same judicial procedures outlined in Title I of FISA). Interestingly, the Protect America Act, which the FAA replaced, did not have any such use provision. *See* 154 CONG. REC. S6132 (daily ed. June 25, 2008) (noting section 706 of FAA "fills a void that has existed under the Protect America Act which had contained no provision governing the use of acquired intelligence").

298. *See* 50 U.S.C. § 1881e (requiring notice to defendant when government intends to use information from section 702 collection in subsequent prosecution).

299. *See* Risen & Lichtblau, *supra* note 37, at A1 (reporting program started in 2002).

300. Adherence to the pure intelligence rule through de facto practice arguably does not reduce the expected costs of surveillance as much as a formal prohibition would, since the government could more easily reverse itself when there is no formal policy committing an executive to a course of action. On the other hand, governments frequently follow the practice of predecessors, and even formal policies can be reversed.

precluded prosecution. Nevertheless, the Second Circuit found the government's prosecutorial record—namely, that information from the subway searches had not been admitted as evidence—to be probative.[301] Adherence to the pure intelligence rule, therefore, is relevant regardless of whether the practice is ad hoc or the result of explicit policy.

The government's self-restraint to date is similar to its conduct throughout much of the Cold War. Relative to decades of earlier practice, in fact, the government's security operations are significantly more restrained: the government follows standardized protocols for the collection, retention, and dissemination of information; it clears these procedures with the judiciary before initiating surveillance; and its surveillance under section 702 only targets non-U.S. citizens believed to be outside the United States (although that is not to say that U.S. citizens within the United States are not incidentally overheard).[302] In contrast, the historical record shows that early use of warrantless investigative techniques—bugging, black bag jobs, mail chamfering, and later, wiretapping—were all pervasively used against U.S.-based targets without any judicial oversight and with fewer protocols designed to protect privacy interests than today. Viewed in light of these precedents, then, the government has a strong case that its current warrantless surveillance programs are constitutionally reasonable.[303]

Similarly, whatever the merits of the *Clapper* majority's opinion vis-à-vis the standing doctrine, *Clapper* permits the executive branch to continue foreign surveillance as a practical matter, as long as it continues to adhere to a de facto pure intelligence rule. *Clapper* does not afford the executive a bold new opportunity to infringe on the liberties of its citizens; rather, the decision simply allows the government to continue foreign surveillance in the same fashion it has conducted such surveillance for over seventy years. In light of the

---

301. MacWade v. Kelly, 460 F.3d 260, 265 n.1 (2d Cir. 2006); *see also supra* notes 251–53 and accompanying text (discussing *MacWade*).

302. The Court of Review, for example, noted that Section 702 instituted a "matrix of safeguards" to constrain executive conduct, including "targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333 § 2.5, and [redacted] procedures [redacted] outlined in an affidavit supporting the certifications." *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1013 (FISA Ct. Rev. 2008).

303. Of course, if federal prosecutors suddenly alter course and utilize evidence from warrantless surveillance programs at trial, this historical parallelism would become moot. Title VII permits the prosecutorial use of information from warrantless surveillance, so no statutory bar to such use exists. *See* 50 U.S.C. § 1881e.

historical practice outlined in this Article, the *Clapper* decision can be viewed as a substantive decision to maintain the general parameters for national security investigations that have existed since World War II.

But while *Clapper* permits such surveillance to continue, it also incentivizes the government to use warrantless surveillance sparingly. There remains great uncertainty about the constitutionality of using such warrantless information in court as well as opinions from multiple attorneys general questioning its constitutionality, so the government could not use such information without placing its warrantless surveillance tools in great jeopardy. The majority decision in *Clapper* therefore effectively corrals the government's warrantless surveillance policies and encourages the use of intelligence warrants whenever possible, given their established constitutionality. In short, *Clapper* maintains the same balance of liberty and security that has existed since World War II, one that affords a real role for the Fourth Amendment during national security investigations.

This analysis about prosecutorial practice to date does not necessarily mean that the government is prohibited from ever using warrantless information in a future prosecution. Indeed, the executive branch may decide that new threats of state-sponsored terrorism and cyber-based attacks require a new prosecutorial strategy using all the evidence available to the government, including FAA-acquired information. Should such a case arise, courts would have to assess whether the Fourth Amendment is satisfied by merely the FAA's targeting and minimization procedures, which strictly define the individuals who may be targeted under the FAA and the retention procedure for information gathered through FAA surveillance. From a historical perspective, the question to be asked is whether the FAA imposes sufficient constraints on government surveillance comparable to the pure intelligence rule.

At minimum, however, this Article establishes that it would be difficult to throw out the FAA in its entirety as unconstitutional since the first five years of its operation have so closely echoed decades of practice dating back to World War II.[304] Executive practice during the last half-decade, along with that over the preceding seventy years, demonstrates there are solutions that both honor the Fourth

304. For example, even if a court found that the prosecutorial use of FAA-acquired information was not permissible under the Fourth Amendment, it could simply strike down 50 U.S.C. § 1881e, which governs the prosecutorial use of FAA-acquired information in a trial, and leave the rest of the FAA statute intact. That severability approach is bolstered by the fact that, as noted above, § 1811e was added after the initial passage of the first FAA-like procedures (those found within the Protect America Act). *See supra* note 297 (discussing § 1881e).

Amendment and afford the executive wide discretion to collect information related to national security threats.

V. CONCLUSION

This Article shows that the FBI, the Justice Department, and others in the executive branch have long recognized that the Fourth Amendment plays a role in national security operations. While the Fourth Amendment is flexible enough to accommodate the peculiarities of national security investigations, such flexibility still requires clear limits on executive power in order to protect civil liberties. The pure intelligence rule described in this Article and that the executive branch followed for decades struck such a compromise. The pure intelligence rule is also defensible on doctrinal and policy grounds, for it installs genuine protections for law-abiding persons while permitting the government to continue to collect intelligence—the lifeblood of national security operations.

In the end, the criminal justice system's usefulness as a national security tool must be a function of, rather than a factor affecting, the Fourth Amendment. The desire to prosecute cannot drive an "end-run around the Fourth Amendment's prohibition of warrantless searches," as one court warned in an early FISA case.[305] Nor need it be. As this Article explains, the results of the government's national security investigations remained out of the courtroom for over three decades, starting at the end of World War II and stretching well into the Cold War, in an effort to accommodate Fourth Amendment protections while maintaining vigilance toward foreign threats. The government's track record since 2001 indicates similar restraint, in a way that makes its practice more constitutionally palatable. Ultimately, then, both historical *and* modern experience demonstrate how, even at times of great peril, constitutional restrictions can maintain the balance between security and liberty through unique legal frameworks.

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