Loyola of Los Angeles Law Review

Volume 52 | Number 4 Article 3

Spring 5-1-2019

Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale

Jennifer S. Granick
American Civil Liberties Union

Patrick Toomey
American Civil Liberties Union

Naomi Gilens
Electronic Frontier Foundation

Daniel Yadron Jr.
Stanford Law School

MISSION CREEP AND WIRETAP ACT 'SUPER WARRANTS': A CAUTIONARY TALE

Jennifer S. Granick, Patrick Toomey,** Naomi Gilens*** & Daniel Yadron, Jr.*****

Congress enacted the Wiretap Act in 1968 in an effort to combat organized crime while safeguarding the privacy of innocent Americans. However, the Act instead served to legitimize wiretapping, and its privacy protections have eroded over time. As a result, there has been a significant increase in wiretapping in the decades since the Act's passage. As technology evolves, the Wiretap Act does less to protect Americans' private communications from government interception. Nevertheless, policy makers see the Wiretap Act, with its "super-warrant" procedures, as the gold standard for statutory privacy protection. To the contrary, when considering how to regulate new and powerful surveillance technologies, advocates must not reflexively rely on the language of the Wiretap Act as a model for adequate privacy safeguards. They must consider whether, given the Act's apparent flaws, it is possible to meaningfully balance the invasiveness of a new technique with the preservation of individual privacy. If so, drafters should focus on crafting statutory language that better implements the intended safeguards of the Act than the Act itself has. This Article describes the deterioration of the Wiretap Act's protections and should serve as a cautionary tale to advocates as they propose new legislation in the face of modern surveillance tools.

* Surveillance and Cybersecurity Counsel, ACLU Speech, Privacy, and Technology Project. Special thanks to Nicolas Aramayo (ACLU Legal Admin Assistant) for all their work on and contributions to the article. The views reflected here are solely those of the authors.

** Senior Staff Attorney, ACLU National Security Project.

*** Frank Stanton Fellow, Electronic Frontier Foundation.

**** J.D., June 2019, Stanford Law School.

TABLE OF CONTENTS

INTRODUCTION

As new surveillance capabilities proliferate, civil liberties advocates strive to protect individuals' privacy rights in the face of novel and intrusive investigative tools. Often, advocates hold up the "super warrant" procedures required to conduct a wiretap as the gold standard for strong privacy protections. A review of the history of the Wiretap Act, however, shows that even a super warrant can fail to adequately protect privacy in the face of new surveillance techniques. Advocates need to think more broadly about additional safeguards. And, some investigative techniques may be so dangerous that there are no regulations that could balance their invasiveness with civil liberties and the public's safety.

The Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also called "Title III") requires a super warrant to authorize government wiretapping. In addition to the traditional warrant requirements of probable cause and particularity, Title III limits wiretapping to investigations of certain predicate offenses; it requires that investigators show necessity; and it mandates minimization of intercepted communications. Often, advocates see these additional Title III elements as providing strong protection for personal civil liberties. However, the evolution of Title III's protections and the exponential growth of wiretapping is a cautionary tale. More skepticism about the adequacy of a Title III "super-warrant" requirement is warranted.

This Article assesses the conditions and frequency of wiretapping before and after Congress passed Title III. Part I describes how wiretaps were used, and how they were regulated, in the decades leading up to Congress's passage of Title III. Part II assesses Congress's purpose in passing Title III. Using both qualitative assessments and historical wiretap data, Part III assesses how law enforcement's use of wiretapping changed following Title III's passage. Part IV examines how Title III's privacy-protective measures have developed and functioned in practice over the past five decades.

The lesson that emerges from this survey is significant. Though intended to provide a set of strong privacy protections that would limit wiretapping to only the most serious investigations, and would ensure that it was used only as a tool of last resort, Title III legitimized a practice that President Lyndon B. Johnson, many lawmakers, and the ACLU wanted to outlaw in all but the most sensitive national security

investigations. The data available and qualitative assessments suggest that wiretapping became exponentially more common after 1968. Moreover, the privacy safeguards imposed by Congress in Title III have eroded over time or have been demonstrably less effective than initially imagined. Title III may not be the cause of this dramatic increase in law enforcement's reliance on wiretapping, but it didn't prevent it, either.

Privacy advocates therefore cannot be confident that a Title III warrant requirement always will be an adequate safeguard. Currently, the Wiretap Act is falling short of the goal of constraining eavesdropping. Privacy-seeking proposals will have to take the failures of the current statutory regime into account. It will be difficult to ensure that regulation will stop invasive law enforcement techniques from metastasizing over time. Civil libertarians need to look beyond the current language of Title III for additional or different tools to constrain invasive surveillance.

DISCUSSION

I. WIRETAPPING WAS SPORADIC AND CONTROVERSIAL BEFORE TITLE III

This Part assesses the frequency and conditions of wiretapping before Title III. First, it assesses government wiretapping policies before 1968. Second, it provides an overview of efforts by President Johnson, lawmakers, and the ACLU to outlaw wiretapping for all but the most serious national security investigations. Ultimately, through Title III, Congress sought to serve law enforcement needs while mitigating widespread privacy concerns about wiretaps by regulating—rather than banning—the invasive investigatory tool. Nevertheless, the regulations have not stopped wiretapping from becoming a widely-used investigation technique.

A. 1928–1946: Wiretapping Grows Through a Loophole

Warrantless federal wiretapping grew in fits and starts during the first half of the twentieth century. To some extent, its use depended "on the personal convictions of those in office."[1] Though federal

1. NAT'L COMM'N FOR THE REVIEW OF FED. & STATE LAWS RELATING TO WIRETAPPING & ELEC. SURVEILLANCE, NWC REPORT at 36 (Apr. 30, 1976), https://www.hsdl.org/?view&did=728874 [hereinafter NWC Report].

agents had used wiretapping to track down bootleggers,[2] in early 1928, Attorney General John G. Sargent prohibited agents at the Bureau of Investigation—the precursor to the Federal Bureau of Investigation (FBI)—from wiretapping for "any reason."[3] Months later, the U.S. Supreme Court, in *Olmstead v. United States*,[4] held that wiretapping did not constitute "a search or seizure within the meaning of the Fourth Amendment."[5] Although the Court invited Congress to prohibit wiretapping via statute,[6] lawmakers did not immediately do so.[7]

Not long after, in 1931, the Department of Justice (DOJ) announced a new policy allowing agents to wiretap, provided that they obtain a bureau chief's approval, "after consultation with the assistant attorney general (AAG) in charge of that case,"[8] and show probable cause (at least internally).[9] The policy was intended for use in investigations targeting "syndicated bootleggers,"[10] but mission creep appeared by year's end. In December 1931, Attorney General William D. Mitchell expanded wiretapping to "exceptional cases where the crimes are substantial and serious, and the necessity is great."[11] The bureau chief and AAG on the case also needed to be satisfied that "the persons whose wires are to be tapped are of the criminal type."[12] This DOJ policy lasted for the remainder of the 1930s.[13]

During this period, Congress passed the Federal Communications Act of 1934.[14] The Communications Act prohibited persons from intercepting communications or divulging or publishing the contents of intercepted communications, except with authorization by the

2. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928), *overruled in part by* Berger v. New York, 388 U.S. 41 (1967), *and overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

3. NWC Report, *supra* note 1, at 35.

4. 277 U.S. 438 (1928).

5. *Id.* at 466.

6. *Id.* at 465.

7. NWC Report, *supra* note 1, at 35 ("Bills were introduced in Congress in 1929 and 1931 to prohibit wiretapping, but were never enacted.").

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.* n.22 (citing *Intelligence Activities Senate Resolution 21: Hearing on the National Security Agency and Fourth Amendment Rights Before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 67 (1975) (prepared statement of Edward H. Levi, Att'y Gen. of the United States)).

13. NWC Report, *supra* note 1, at 35.

14. 47 U.S.C. §§ 151 *et seq.* (1934).

sender.[15] The Communications Act did not explicitly address wiretapping by law enforcement specifically.[16] In *Nardone v. United States*,[17] the Supreme Court interpreted it to prohibit government agents from intercepting communications as well.[18] Speaking in moral terms, the Court held that the statute applied to federal agents, in part because "[f]or years controversy has raged with respect to the morality of the practice of wire-tapping by officers to obtain evidence. It has been the view of many that the practice involves a grave wrong."[19] The Court doubled down two years later, holding that evidence *derived* from intercepted communications was inadmissible at trial.[20] By 1940, Attorney General Robert H. Jackson again completely banned wiretapping by federal agents, describing it as an "unethical tactic[]."[21]

The pause in eavesdropping was short-lived.[22] In May 1940, President Franklin D. Roosevelt wrote Jackson a confidential memo arguing that the *Nardone* decisions did not apply to national security investigations.[23] Roosevelt then authorized DOJ to use wiretapping in investigations of alleged "subversive activities of the United States government," asking Jackson to limit the investigations "insofar as possible to aliens."[24] A year later, Jackson—just before his nomination to the Supreme Court—informed Congress of a statutory loophole DOJ had exploited.[25] The Communications Act, Jackson wrote, only proscribed *divulging* intercepted communications—not *collecting* intercepted communications.[26] DOJ policy post-*Nardone* was to use wiretapping for intelligence purposes.[27]

DOJ wiretaps grew quickly during World War II. DOJ conducted six wiretaps in 1940.[28] In 1944: 517.[29] Though initially justified by

15. 47 U.S.C. § 605 (2012).
16. NWC Report, *supra* note 1, at 35.
17. 302 U.S. 379 (1937).
18. *Id.* at 384.
19. *Id.*
20. Nardone v. United States (*Nardone II*), 308 U.S. 338, 340–41 (1939).
21. NWC Report, *supra* note 1, at 36.
22. *Id.* ("This total ban lasted only about two months, however.").
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.* (quoting 47 U.S.C. § 605 (1934)).
28. *Id.*
29. *Id.*

wartime needs, wiretapping did not go away when the war ended. In 1946, Attorney General Tom C. Clark—another future Supreme Court Justice—warned President Harry Truman of a "very substantial increase in crime."[30] He proposed expanding federal wiretaps to cases "vitally affecting the domestic security, or where human life is in jeopardy."[31] Truman approved the proposal set forth in Clark's letter.[32]

B. 1956–1967: The Public and the President Revolt Against Wiretapping

Between World War II and the passage of Title III, government wiretapping faced such a backlash that it was nearly outlawed.[33] In 1956, the Pennsylvania Bar Association Endowment commissioned a nationwide study of "wiretapping practices, laws, devices, and techniques."[34] The study's authors went on to write *The Eavesdroppers*, a 1959 nonfiction best-seller that convinced many Americans that "in some ways Orwell's fictitious world is already in existence."[35] The book detailed how telephone companies voluntarily provided secret wiretaps in "Boston, Chicago, and New Orleans, with the understanding that the police would not disclose the telephone companies' cooperation to the public."[36] Still the number of wiretaps—at least at the federal level—remained relatively stable during this period.[37]

---

30. *Id.*

31. *Id.*

32. *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) (citing Letter from Tom C. Clark, Att'y Gen. to President Harry S. Truman (Jul. 17, 1946)). Truman's handwritten approval, appended to the bottom of Clark's letter, is dated July 17, 1947. That seems to have been an error. *Cf.* United States v. United States District Court (Keith), 407 U.S. 297, 310 (1972) (treating 1946 as the date of Truman's authorization).

33. NWC Report, *supra* note 1, at 38–39.

34. Brian Hochman, *Eavesdropping in the Age of* The Eavesdroppers*; or, The Bug in the Martini Olive*, POST45 (Feb. 3, 2016), http://post45.research.yale.edu/2016/02/eavesdropping-in-the-age-of-the-eavesdroppers-or-the-bug-in-the-martini-olive/.

35. Mairi MacInnes, The Eavesdroppers*, by Samuel Dash, Robert E. Knowlton, and Richard F. Schwartz*, COMMENTARY (Mar. 1960), https://www.commentarymagazine.com/articles/the-eavesdroppers-by-samuel-dash-robert-e-knowlton-and-richard-f-schwartz/.

36. Brief for the Rutherford Institute as Amici Curiae Supporting Petitioners at 9, Dahda v. United States, 138 S. Ct. 1491 (2018) (No. 17-43).

37. Federal agents initiated 285 wiretaps in 1952, 300 wiretaps in 1953, and 322 wiretaps in 1954. *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearing Before the S. Select Comm. on Intelligence*, 94th Cong. 86 (1975) (testimony of Edward H. Levi, Att'y Gen. of the United States),

In the meantime, the Supreme Court again limited the use of wiretapping in federal courts.[38] While the fruits of federal wiretapping remained inadmissible under *Nardone*, federal agents had developed a workaround. Many states, most famously New York, had permissive government wiretap statutes. Because *Nardone* did not apply to the states, federal prosecutors had started using evidence from state wiretaps in federal courts.[39] In 1957, the Court held this, too, was unlawful.[40]

During the late 1950s, California, Florida, Indiana, Illinois, and New Jersey either banned wiretapping or "made moves to shore up old statutes that had the same effect."[41] In 1965, President Johnson reinstated a ban on federal wiretapping barring a threat to national security and approval from the Attorney General.[42]

To be sure, eavesdropping had support during this era. Many in law enforcement and the Kennedy Administration supported wiretapping, at least in the context of organized crime.[43] The President's Commission on Law Enforcement and Administration of Justice famously said restrictive wiretapping laws were "intolerable" because of the telephone's "relatively free use" by mobsters.[44] New York, in the meantime, had made prodigious use of its own state wiretap statute. In 1962, the District Attorney of New York told Congress "that 'without [wiretaps] my own office could not have convicted' 'top figures in the underworld.'"[45]

In 1967, however, three key things happened that created a real prospect of a United States free from prolific government wiretapping. First, President Johnson proposed in his State of the Union address that the U.S. "should outlaw all wiretapping—public and private—

https://www.intelligence.senate.gov/sites/default/files/hearings/94electronic_surveillance.pdf [hereinafter Levi Testimony].

38. NWC Report, *supra* note 1, at 37–38.

39. *See* Benanti v. United States, 355 U.S. 96, 97 (1957) ("The question presented by petitioner is whether evidence obtained as the result of wiretapping by state law-enforcement officers, without participation by federal authorities, is admissible in a federal court.").

40. *Id.* at 105–06.

41. Hochman, *supra* note 34.

42. NWC Report, *supra* note 1, at 39; *see also* Levi Testimony, *supra* note 37, at 87 (stating that nonconsensual wiretapping is permitted in national security investigations with consent of the Attorney General).

43. NWC Report, *supra* 1, at 39.

44. PRES. COMM'N ON LAW ENFORCEMENT & THE ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 201, 203 (1967), https://www.ncjrs.gov/pdffiles1/nij/42.pdf.

45. Berger v. New York, 388 U.S. 41, 61 (1967) (quoting Congressional testimony).

wherever and whenever it occurs, except when the security of this Nation itself is at stake—and only then with the strictest governmental safeguards."[46]

Second, the Johnson Administration then proposed and lobbied for a national ban on government wiretapping—state and federal—through the Right of Privacy Act of 1967.[47] There is reason to believe the Act's supporters were centrists on privacy. The American Civil Liberties Union expressed "strong reservations" due to the Right of Privacy Act's national security exception.[48]

Third, in *Berger v. New York*,[49] the Supreme Court struck down New York's wiretap statute.[50] The New York wiretap law's privacy controls were lax by contemporaneous standards. Officers needed court approval, but they only had to show "reasonable grounds to believe they could find evidence of crime," rather than probable cause.[51] Police could use the tactic to investigate any crime.[52] The law also allowed officers to extend a two-month wiretap based on a showing of the "public interest."[53] The Court also faulted the statute for not requiring officers to "'particularly describ[e]' the communications, conversations, or discussions to be seized."[54] Six months after *Berger*, the Court decided *Katz v. United States*,[55] explicitly holding that an individual has a reasonable expectation of privacy in his conversations.[56] The Court reiterated what the government would need to do to justify this incursion.[57] In this way, the Court effectively laid out a blueprint for Congress to permit and regulate wiretapping consistent with the Fourth Amendment.

---

46. Annual Message to the Congress on the State of the Union, 1 PUB. PAPERS 2–14 (Jan. 10, 1967).

47. H.R. 5386, 90th Cong., 1st Sess. § 2514 (1967).

48. The ACLU, for instance, lobbied against the national security exception and argued it at least should be more narrowly defined. *House Rewrites and Passes Safe Streets Bill*, CONG, Q. ALMANAC (1967), http://library.cqpress.com/cqalmanac/cqal67-1313006. Congressional media quoted an ACLU spokesman as saying, "a strike by the Teamsters or the steel industry could be held by a court to imperil national security, under the Taft-Hartley Act." *Id.*

49. 388 U.S. 41 (1967).

50. *Id.* at 64.

51. *Id.* at 54.

52. *Id.*

53. *Id.* at 59.

54. *Id.*

55. 389 U.S. 347 (1967).

56. *Id.* at 351–53.

57. *Id*. at 355.

II. CONGRESS PASSED TITLE III TO EMBRACE WIRETAPPING FOR LAW ENFORCEMENT PURPOSES

A. Passage of Title III

In 1968, responding to these developments, Congress enacted Title III. It appears Congress felt squeezed between "being urged to *authorize* eavesdropping in order to combat crime" and "counterpressures to *ban* it in order to protect privacy."[58] Title III, therefore, "was enacted as a compromise" between a "total ban on electronic surveillance" and lax "limit[s] [on] the use of a technique claimed by many to be a vital tool in fighting crime."[59] Though the "major purpose of Title III is to combat organized crime,"[60] Congress identified one of the Act's purposes as "safeguard[ing] the privacy of innocent persons" by placing the issuance of wiretap orders under the continuing supervision of the courts and limiting their use to "certain major types of offenses and specific categories of crimes with assurances that the interception is justified and that the information obtained thereby will not be misused."[61]

The key elements of Title III include:

- The statute generally prohibits interception of wire or radio communications without a warrant.[62]
- To obtain a warrant, investigators must show probable cause that the interception will provide evidence that "an individual is committing, has committed, or is about to commit a particular offense."[63]
- In addition, investigators must show "necessity": that they have already tried other investigative means and failed or that such techniques are likely to be unsuccessful or too dangerous.[64]
- The statute authorizes the use of wiretaps only in investigations of certain offenses, as listed.[65]

58. EDITH J. LAPIDUS, EAVESDROPPING ON TRIAL 13 (1974).
59. NWC Report, *supra* note 1, at xiii.
60. S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2157.
61. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 801(d).
62. 18 U.S.C. § 2511 (2012).
63. 18 U.S.C. § 2518(3).
64. *Id.* § 2518(1)(c).
65. *Id.* § 2516.

- The statute requires investigators to "minimize" communications overheard in the course of a wiretap—that is, to avoid recording, collecting, or retaining innocent or irrelevant conversations.[66]
- The statute requires the government to provide notice of wiretaps in various circumstances, in order to inform individuals when the government has intruded on their private communications.[67]
- The statute provides a mandatory suppression remedy for violations of the wiretapping requirements.[68]
- The statute also provides civil remedies for violations.[69]

Though enacted as a compromise, Title III legitimized and normalized wiretapping as a tool in ordinary criminal investigations.[70] As Senators Hart and Long wrote in their portion of the Senate Report, "the proposed legislation legitimize[d] a practice of law enforcement" that had, until then, been "banned by the courts."[71]

B. Early Assessments of Title III by Policymakers and Law Enforcement

In the decade after Title III's passage, most policymakers came to view the wiretap law as a successful balance between law enforcement and privacy. One of Title III's compromise provisions was the creation of a National Wiretap Commission.[72] The Commission's 1976 report on state and federal wiretapping offered a mostly positive assessment of Title III's effects on law enforcement and privacy.[73] The Report offered the following conclusions:

66. *Id.* § 2518(5).
67. *Id.* § 2518(8)(d).
68. *Id.* § 2515.
69. *Id.* § 2520.
70. *See* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 75 (1997) ("Wiretapping is no longer confined to violent and major crimes. Although Congress recognized in 1968 that wiretapping was an extraordinary technique that should be used only for especially serious crimes, the list of offenses for which wiretapping is permitted has been expanded steadily ever since . . . . [W]iretapping is now authorized for cases involving false statements on passport applications and loan applications or involving 'any depredation' against any property of the United States.").
71. S. REP. NO. 90-1097, at 163 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2225.
72. *Id.* at xiii.
73. *Id.*

- "A majority of the Commission vigorously reaffirmed . . . that electronic surveillance is an indispensable aid to law enforcement . . . ."[74]
- "[T]he procedural requirements of Title III have effectively minimized the invasion of individual privacy in electronic surveillance investigations by law enforcement officers."[75]
- "A majority of the Commission concluded that electronic surveillance could be used with significant success in the investigation of Federal crimes not now included in the enumerated crimes of Section 2516 of Title III . . . ."[76]

Not everyone shared these beliefs. A "substantial minority" of the Commission, viewing the same evidence as the majority, concluded that wiretapping only played a successful role in a limited number of cases.[77] Furthermore, this minority concluded that eight years of legalized government wiretapping had "discouraged" law enforcement's use of traditional investigative techniques and still resulted in "substantial invasions of personal privacy."[78]

In sum, prior to 1968, the country periodically experimented with banning law enforcement wiretapping. The Communications Act meant to outlaw it, Attorneys General periodically gave it up, and evidence obtained from it could not be used in court. Despite growing awareness of surveillance abuses in the civil rights and Vietnam War era,[79] Congress authorized regulated wiretapping via Title III, and law enforcement hasn't looked back. Initially policymakers viewed the legislation as a successful balancing.[80] However, as the next Part explains, in the years following Title III's passage, the number of taps has expanded significantly, electronic communications may now be wiretapped in vast quantity even though the resulting privacy

74. *Id.* at xiv.

75. *Id.* at xvi.

76. *Id.* at xiii. The Report also stated that Title III had decreased the number of wiretaps in some states immediately following the law's passage, though these findings were based on anecdotes rather than data.

77. *Id.*

78. *Id.*

79. *See, e.g.*, Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1091 ("Between 1965 and 1974, the legislature held forty-seven hearings and issued reports on privacy-related issues.").

80. S. REP. NO. 90-1097, at xiii (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2225.

intrusions are more severe, and the remedies for illegal surveillance are hard to obtain.

III. TITLE III HAS NOT NARROWLY RESTRICTED THE USE OF WIRETAPPING

The frequency of wiretapping has increased dramatically since Title III was enacted. Where law enforcement agencies conducted a few hundred wiretaps in 1968, they now conduct thousands of wiretaps each year.[81] Moreover, according to data published by the U.S. courts, a single wiretap today can sweep in millions of communications.[82] While this increase may partly reflect changing communication habits, there is no question that the use of wiretapping has become far more routine in criminal investigations.[83] Over the intervening decades, Congress has expanded the list of predicate offenses that are eligible for wiretaps thirty-one times.[84] What was originally an investigative tool reserved primarily for national security and organized crime investigations, can now be used to investigate a vast range of offenses.

81. *Title III Wiretap Orders - Stats*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/wiretap/stats/wiretap_stats.html (last visited Nov. 26, 2019).

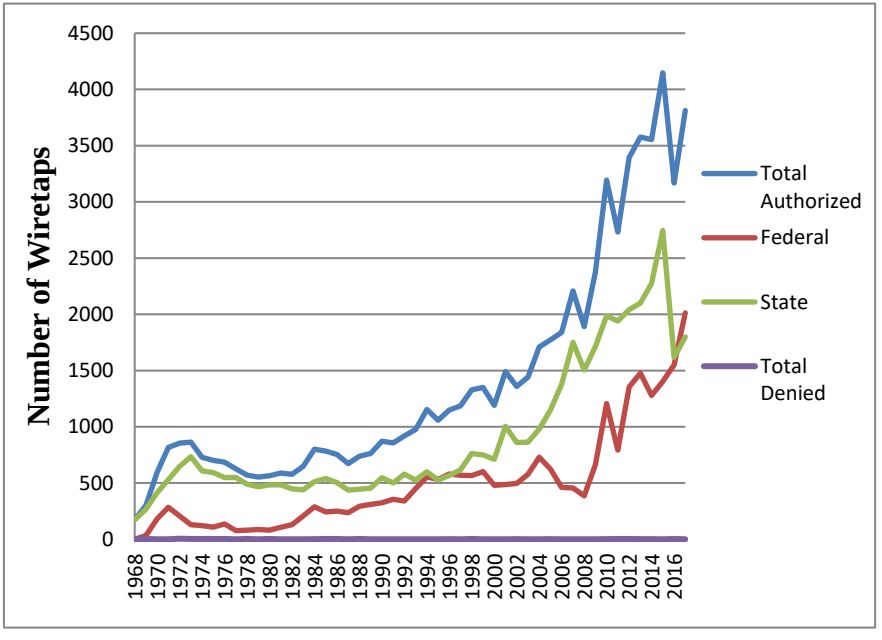
82. *Wiretap Report 2018*, U.S. CTS., https://www.uscourts.gov/statistics-reports/wiretap-report-2018 (last updated Dec. 31, 2018) ("The federal wiretap with the most intercepts occurred during a narcotics investigation in the Southern District of Texas and resulted in the interception of 9,208,906 messages in 120 days.").

83. *Infra* app. A.

84. 18 U.S.C.A. § 2516 (West 2018).

A. Wiretapping Has Increased Significantly in the Decades Since Title III Was Enacted

Chart 1: Federal and State Wiretaps 1968–2017[85]



85. *See Title III Wiretap Orders - Stats*, *supra* note 81 (source of data for years 1968–2016); *Wiretap Report 2017*, U.S. CTS., https://www.uscourts.gov/statistics-reports/wiretap-report-2017 (last updated Dec. 31, 2017) (source of data for year 2017).

Table 1: Federal and State Wiretaps Prior to 1968[86]

Year	Number of Wiretaps
1940	6[87]
1944	517[88]
1952	285[89]
1953	300[90]
1954	322[91]

Using data published by the Administrative Office of the United States Courts, Chart 1 shows the rise in the use of wiretapping in the five decades since Congress enacted Title III.[92]

To assess the extent to which wiretaps are used to intercept Americans' private conversations, however, one must also look at another important measure: the number of communications collected in the course of individual wiretaps. The average number of intercepted communications has steadily increased since 1977.[93] In that year, the average number of communications intercepted was 658.[94] By 2007 and 2017, those numbers had increased to 3,106 and 5,989 respectively.[95] In 2016, a single wiretap resulted in the interception of 3,292,285 conversations or messages.[96] As noted above, this increasing trend is likely a partial function of the changes in the types of devices subject to wiretapping and the use of new

86. Wiretap data from before 1968 is sporadic and limited to offhand disclosures in congressional hearings and committee reports.
87. NWC Report, *supra* note 1, at 36.
88. *Id.*
89. Levi Testimony, *supra* note 37, at 86.
90. *Id.*
91. *Id.*
92. *Title III Wiretap Orders - Stats*, *supra* note 81.
93. *Infra* app. A.
94. *Id.*
95. *Id.*
96. *Wiretap Report 2016*, U.S. CTS., https://www.uscourts.gov/statistics-reports/wiretap-report-2016 (last updated Dec. 31, 2016).

communications technologies, such as text-based messaging.[97] As a result, today's statistics show that wiretaps result in the collection of a staggering number of communications.

Despite the statute's reporting requirements, some scholars have raised concerns that the official number of wiretaps is inaccurately low.[98] Recently, companies have started publishing "transparency reports" about the number and nature of government demands to access their users' data.[99] AT&T, Verizon, Sprint, and T-Mobile publish such reports.[100] In aggregate, just these four companies state that they implemented three times as many wiretaps as the total number reported by the Administrative Office of the Courts.[101]

B. The List of Predicate Offenses for Wiretapping Has Expanded

Following Title III's passage, Congress wasted little time in expanding the number and categories of crimes that could justify wiretapping. In 1968, nearly all of the twenty-four categories of offenses listed in Title III had a clear relationship to national security or organized crime.[102] Since then, Congress has amended 18 U.S.C. § 2516—the section of Title III that enumerates wiretap-worthy offenses—thirty-one times.[103] By 2018, § 2516(c) authorized wiretaps for cases relating to: "transportation for illegal sexual activity and related crimes"; "failure to appear" in court; "mail fraud"; "computer fraud and abuse"; "reproduction of naturalization or citizenship papers"; and "false statements in passport applications."[104] Investigations into obscenity[105] and theft of medical products[106] now qualify, too.

97. *See* Dempsey, *supra* note 70, at 78–80.

98. *See* Albert Gidari, *Wiretap Numbers Don't Add Up*, JUST SECURITY (July 6, 2015), https://www.justsecurity.org/24427/wiretap-numbers-add.

99. *Id.*

100. *Id.*

101. *Id.*; Albert Gidari, *Wiretap Numbers Still Don't Add Up*, STAN. L. SCH.: CTR. FOR INTERNET & SOC'Y (Nov. 29, 2016, 11:15 AM), https://cyberlaw.stanford.edu/blog/2016/11/wiretap-numbers-still-dont-add.

102. *E.g.*, 18 U.S.C. § 2516(a) (effective June 19, 1968) (authorizing wiretaps in investigations "relating to treason"); *id.* § 2516(c) (authorizing wiretaps in investigations relating to "bribery of public officials and witnesses").

103. 18 U.S.C.A. § 2516 (West 2018).

104. 18 U.S.C. § 2516(c) (2012).

105. *Id.* § 2516(i).

106. *Id.* § 2516(s).

In 1969 and 1977, wiretaps were used most often to investigate gambling offenses, making up 30 to 40 percent of the totals, but drug-related offenses were a close second.[107] Since then, drug-related offenses have consistently taken the lead, making up roughly 50 to 80 percent of intercept orders and applications from 1987 to the present.[108]

C. Title III's "Necessity" Requirement Has Not Been Strictly Enforced

Title III requires that every wiretap application include a statement as to other investigative procedures used prior to the application and why other investigative procedures reasonably appear unlikely to succeed, or are too dangerous to be tried.[109] This provision, known as the necessity requirement, is "designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime."[110]

Courts of appeals, however, have not applied the necessity requirement to require a showing that all possible alternatives have failed or are not reasonably likely to succeed. The requirement has proved to be more of an opportunity for reflection than an actual limitation on unnecessary use of a highly invasive investigative technique.[111] The Seventh Circuit, for example, has stated that "[w]iretaps do not have to be used only as a last resort in an investigation," as "[t]he evil" that the necessity requirement is intended to avoid is only "the routine use of wiretaps as an initial step in the investigation."[112] For that reason, the court held that "the government's burden of proving necessity is not extraordinarily high, and our view is not hyper-technical."[113] Other appeals courts have

107. *See* ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS tbl. 3 (1978); ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS tbl. 2 (1970); *infra* app. A.

108. *Infra* app. A.

109. 18 U.S.C. § 2518(1)(c).

110. United States v. Kahn, 415 U.S. 143, 153 n.12 (1974).

111. *See* United States v. Pacheco, 489 F.2d 554, 565 (5th Cir. 1974) ("[T]he purpose of the requirement in section 2518(1)(c) is not to foreclose electronic surveillance until every other imaginable method of investigation has been unsuccessfully attempted, but simply to inform the issuing judge of the difficulties involved in the use of conventional techniques.").

112. United States v. Fudge, 325 F.3d 910, 919 (7th Cir. 2003).

113. *Id.*

similarly concluded that the government's burden to demonstrate necessity "is not great."[114] "All that is required [from the government] is that the investigators give serious consideration to the non-wiretap techniques prior to applying for wiretap authority and that the court be informed of the reasons for the investigators' belief that such non-wiretap techniques have been or will likely be inadequate."[115]

IV. TITLE III'S PRIVACY PROTECTIONS HAVE ERODED OVER TIME

Finally, this Part explains how the various provisions in Title III that were meant to limit privacy intrusions, and to ensure that investigators complied with those protections, have significantly eroded over time.

A. Implementation of the Wiretap Act's Minimization Requirement

Title III mandates that law enforcement wiretaps "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter."[116] Minimization is an important means to protect the privacy of innocent third parties. It also protects the privacy of individuals who are being investigated, implicitly acknowledging their humanity—a person may be suspected of breaking the law, but she still has a right to private conversations with her mother, doctor, etc.

The minimization requirement, however, has not proven as strict or effective as some might suggest. In practice, courts have generally set a low bar in terms of what minimization requires and—as

114. United States v. Armocida, 515 F.2d 29, 38 (3d Cir. 1975).

115. United States v. Alfano, 838 F.2d 158, 163–164 (6th Cir. 1988); *see also* United States v. Canales Gomez, 358 F.3d 1221, 1225–26 (9th Cir. 2004) ("wiretap should not ordinarily be the initial step in the investigation" but "law enforcement officials need not exhaust every conceivable alternative before obtaining a wiretap" (citation omitted)); United States v. Santana, 342 F.3d 60, 65 (1st Cir. 2003) ("government need not demonstrate that it exhausted all investigative procedures"); United States v. Castillo-Garcia, 117 F.3d 1179, 1187 (10th Cir. 1997) (the "'necessity' requirement of Title III is not an 'exhaustion' requirement," and "law enforcement officials are not required to exhaust all other conceivable investigative procedures before resorting to wiretapping" (citation omitted)); United States v. Garcia, 785 F.2d 214, 223 (8th Cir. 1986) (wiretap application "need not explain away all possible alternative techniques because investigators are not required to use wiretaps or eavesdropping devices only as a last resort"); *United States v. Pacheco*, 489 F.2d 554,at 565 (5th Cir. 1974) (purpose of the exhaustion requirement is "simply to inform the issuing judge of the difficulties involved in the use of conventional techniques").

116. 18 U.S.C. § 2518(5) (2012).

discussed further below—courts rarely require suppression even when they find that the minimization requirement has been violated.

Courts give law enforcement significant leeway in what they are required to minimize. In the seminal case examining the minimization requirement, the Supreme Court declined to enumerate clear guidelines regarding minimization, instead emphasizing that the reasonableness of an officer's efforts to minimize wiretapped communications "will depend on the facts and circumstances of each case."[117] Though the officers in that case had intercepted "virtually all" of the target's conversations, only 40 percent of which were related to the criminal investigation, the Court rejected petitioners' bid for suppression.[118] Justices Brennan and Marshall, in dissent, criticized the opinion as contributing to a "process of myopic, incremental denigration of Title III's safeguards."[119] Courts since have given law enforcement a lot of leeway in satisfying the minimization requirement, even when investigators recorded and retained innocent—or even clearly privileged—conversations, such as conversations with lawyers or doctors.[120]

Minimization may be even more lax in the context of "electronic communications." In 1986, the Electronic Communications Privacy Act (ECPA) amended Title III to extend its privacy protections to "electronic" as well as "wire" and "oral" communications.[121] It is not entirely clear how the minimization requirement functions in the electronic context because the type of real-time minimization required

117. *Id.* at 140.

118. *Id.* at 132, 143.

119. *Id.* at 148 (Brennan, J., dissenting).

120. *See, e.g.*, United States v. DePalma, 461 F. Supp. 800, 817 (S.D.N.Y. 1978) (interception of calls between defendant and his wife, lawyer, and doctor were unreasonable, but the government nonetheless observed proper minimization overall); *see also* United States v. Scurry, 821 F.3d 1, 18 (D.C. Cir. 2016) (rejecting minimization challenge on the grounds that "to challenge the reasonableness of the government's minimization efforts, a party must present more than the raw number of non-pertinent intercepted calls and their durations"); United States v. Charles, 213 F.3d 10, 21–23 (1st Cir. 2000) (finding that minimization of phone calls involving attorneys was sufficient based on (1) the nature and complexity of the suspected crimes, (2) the thoroughness of the government precautions to bring about minimization, and (3) the degree of judicial supervision over the surveillance practices); United States v. Nersesian, 824 F.3d 1294, 1307 (2d Cir. 1987) (rejecting minimization challenge where officers intercepted innocent calls because the investigation "involved factors such as the presence of ambiguous or coded language, a conspiracy thought to be widespread, and the fact that the phone tapped was located in the residence of a person thought to be the head of a major drug ring").

121. 18 U.S.C. § 2510 *et seq.* (1986), Pub. L. 99–508.

for wiretapped telephone calls cannot easily be applied to electronic communications. As stated in the ECPA Senate Report:

> [T]he technology used to either transmit or intercept an electronic message such as electronic mail or a computer data transmission ordinarily will not make it possible to shut down the interception and taping or recording equipment simultaneously in order to minimize in the same manner as with a wire interception. It is impossible to 'listen' to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation. For instance, a page displayed on a screen during a computer transmission might have five paragraphs of which the second and third are relevant to the investigation and the others are not. The printing technology is such that the whole page including the irrelevant paragraphs, would have to be printed and read, before anything can be done about minimization.[122]

The Report contemplated that because "minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call, . . . the minimization should be conducted by the initial law enforcement officials who review the transcript."[123] It would then be the role of those officials to "delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation."[124]

Cases examining the minimization requirement in the context of electronic communications appear to be rare. Based on the limited amount of information available on minimization in the context of electronic wiretaps, it seems that generally, law enforcement collects *all* of the intercepted electronic communications, which a designated officer then reviews in order to identify and segregate the pertinent communications.[125] There are no authorities making clear how

122. S. REP. NO. 99-541, at 31.

123. *Id.*

124. *Id.*

125. *See* DEP'T OF JUSTICE, ELEC. SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 14 (2005), https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf (stating that "[a]fter-the-fact minimization is a necessity for the interception of electronic communications such as cell phone or pager text messages, facsimile transmissions, and internet transmissions such as e-mail and images," and explaining that "[i]n such cases, all communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation," and that "[d]isclosure is then limited to those communications by the subjects or their confederates that are criminal in nature"); *see also*

electronic communications that investigators initially deem non-pertinent are treated—*i.e.*, whether they are deleted, sealed in some fashion, retained by the original investigators, or made available for subsequent querying.[126] In sum, permitting seizure of communications in their entirety and letting law enforcement sort out the material for which there is probable cause afterward creates the opportunity for far-wider reaching privacy invasions.

The infrequency of court cases applying the minimization requirement to wiretaps of electronic communications may be due both to inadequacy of notice to affected individuals and to the fact that ECPA did not extend Title III's statutory suppression remedy to electronic communications. Moreover, even when the minimization requirement is violated in the context of telephone calls, courts rarely require suppression (as discussed further in suppression section below), and the statute provides no civil remedy. In the majority of cases, there are no consequences to investigators for a failure to effectively minimize.

B. Implementation of the Wiretap Act's Notice Provisions

The Wiretap Act requires that the court inform an individual who is the target of a wiretap application about the "fact" and "date" of the wiretap, and whether "wire or electronic communications" were or were not intercepted.[127] Notice is supposed to occur "[w]ithin a reasonable time but no later than ninety days" after the wiretap, unless a judge allows for postponing notice.[128] Title III further provides that a judge may determine in his or her discretion that it is "in the interest of justice" to require notice to individuals whose communications are

United States v. McGuire, 307 F.3d 1192 (9th Cir. 2002) (regarding an electronic wiretap of a fax, law enforcement need not mimic minimization of telephone calls by skipping lines if a fax appeared non-pertinent; rather, law enforcement may look at every communication collected by an electronic wiretap and *then* separate out non-pertinent communication); United States v. Harvey, No. 4:02-00482-JCH-DDN, 2003 WL 22052993, at *8 (E.D. Mo. July 28, 2003) (describing minimization process by which email communications were intercepted, copied in their entirety, stored, and reviewed by designated personnel to determine whether communications appeared pertinent to criminal activity, with non-pertinent communications then sealed and made unavailable to the investigators).

126. *See, e.g.*, United States v. Ganias, 824 F.3d 199 (2d. Cir. 2016) (non-responsive materials seized pursuant to a November 2003 warrant still in law enforcement possession and available for querying in April 2006).

127. 18 U.S.C. § 2518 (2012).

128. *Id.* § 2518(8)(d).

incidentally overheard.[129] Notice is critical for public transparency, oversight, and accountability. Finally, Title III also requires notice to any party in a trial or legal proceeding where the government intends to introduce the contents of an intercepted communication "or evidence derived therefrom."[130]

Because wiretaps are conducted in secret, notice is crucial for accountability. Without notice, individuals who have been subject to unlawful wiretaps are generally unable to pursue the remedies for violations of Title III or the Fourth Amendment.

However, some courts have held that notice to the electronic service provider, and not to the intercepted parties, is adequate.[131] Despite the importance of this procedural safeguard, the extent to which courts require notice to individuals who are incidentally overheard is unclear because most jurisdictions do not appear to collect or publish data. Similarly, the extent to which federal and state authorities comply with the statute's notice requirement—both for those who are targeted and those who are incidentally overheard—is difficult to assess.[132] While the federal government keeps records regarding instances of wiretapping,[133] these records do not provide information about whether notices were sent to those who have been wiretapped.[134] As a result, publicly available information about wiretap notices derives mostly from individuals and attorneys sharing their firsthand accounts.[135]

---

129. *Id.*

130. *Id.* § 2518(9).

131. *In re* United States, 665 F. Supp. 2d 1210, 1221–22 (D. Or. 2009).

132. For example, the Department of Justice has refused to disclose how it interprets Title III's requirement that it provide notice to criminal defendants when evidence is "derived" from a wiretap. An unjustifiably narrow interpretation of this requirement would allow the government to conceal wiretaps in criminal cases, depriving individuals who face prosecution of the opportunity to challenge those wiretaps and the resulting evidence. In 2016, DOJ sent all federal prosecutors a policy memorandum titled, "Determining Evidence is 'Derived From' Surveillance Under Title III or FISA." Although this memorandum sets forth DOJ's official interpretation of its duty to provide notice, DOJ has refused to release the document publicly. *See* Complaint for Injunctive Relief, Am. Civil Liberties Union v. Dep't of Justice, No. 4:17-cv-03571-JSW, 2019 WL 2619664 (N.D. Cal. Apr. 15, 2019).

133. *Wiretap Report 2017*, *supra* note 85.

134. Fred P. Graham, *Can You Find Out if Your Telephone Is Tapped?*, ESQUIRE (May 1973), http://www.bugsweeps.com/info/esquire_5-73.html.

135. Bill Torpy, *DeKalb Wiretap Notices Causing Consternation*, ATLANTA J.-CONST. (Sept. 7, 2013), https://www.ajc.com/news/local-govt—politics/dekalb-wiretap-notices-causing-consternation/OoH4BnUGlzUBB7GerWP1JI/; Jeff German, *DA Sends 230 Wiretap Notices Amid Nevada Assembly Extortion Probe*, LAS VEGAS REV.-J. (June 10, 2015, 2:39 PM),

Similarly, most states that have their own wiretap provisions and notice regulations decline to publish records of wiretap notices. California appears to be the only state that makes data concerning the number "inventory notices" provided publicly available—and even California's records do not appear to go back before 2009.[136]

California's reports show that, in many instances, only a small fraction of the individuals whose communications are intercepted receive notice that they were subject to surveillance.[137] For example, in 2018, one series of wiretaps intercepted the communications of 1,739 people—ensnaring 91,111 communications in the process—but notice was given to only 345 individuals.[138]

Without notice, people whose communications have been intercepted have no way of knowing that investigators have listened in on their private conversations and no way of determining whether that intrusion was lawful or not. Similarly, without notice, the public has limited ability to oversee and to incentivize careful use of wiretapping.

C. Implementation of Title III's Suppression Remedy

1. Congressional Intent and Statutory Background

To incentivize compliance with the Wiretap Act's requirements, the statute includes a mandatory suppression remedy.[139] The Wiretap Act's legislative history indicates that Congress believed the suppression remedy was necessary to protect privacy and enforce the Act's limitations. Congress was clear that the prohibition on unauthorized interception "must be enforced with all appropriate sanctions."[140] Congress explained that "[t]he perpetrator [of unlawful interception] must be denied the fruits of his unlawful actions in civil

https://www.reviewjournal.com/local/local-las-vegas/da-sends-230-wiretap-notices-amid-nevada-assembly-extortion-probe/.

136. *Publications*, ST. OF CAL. DEP'T OF JUST., https://oag.ca.gov/publications#electronic (last visited Nov. 26, 2019).

137. Due to the timing of these annual reports, it can be difficult to determine the degree to which notice was ultimately provided to affected individuals, if at all, because delayed notice orders remained in effect when the report was issued. This gap represents another flaw in the available data.

138. OFFICE OF THE ATTORNEY GEN. CALIFORNIA ELECTRONICS INTERCEPTIONS REPORT 7, 30 (2018), https://oag.ca.gov/sites/all/files/agweb/pdfs/publications/annual-rept-legislature-2018.pdf (providing statistics for interception number 2019-CC-19).

139. 18 U.S.C. § 2515 (2012).

140. S. REP. NO. 90-1097, at 69 (1968).

and criminal proceedings."[141] The suppression remedy was intended to "sharply curtail the unlawful interception of wire and oral communications."[142] The legislative history also suggests that the remedy was meant to reflect constitutional interpretations of suppression remedies as they existed at the time. Congress sought to roughly codify the "suppression role" as it was understood in the prevailing "search and seizure law" in 1968.[143]

2. Implementation with Regard to Wire and Oral Communications

Since the Wiretap Act's enactment, judicial interpretations have narrowed the suppression remedy's scope in three ways. Although some of these interpretations parallel efforts to narrow the *judicially created* exclusionary rule for Fourth Amendment violations, the Wiretap Act's suppression remedy has an independent basis in the statute.[144] As a result, some of these rulings appear at odds with the compulsory language of the Wiretap Act[145] and with Congress's view that suppression would be an integral remedy to protect privacy.[146]

First, some circuits have grafted the Fourth Amendment's good-faith exception onto the Wiretap Act's statutory suppression remedy.[147] They have done this even though the Supreme Court case that established the good-faith exception, *United States v. Leon*,[148] came after the 1968 Wiretap Act, and thus Congress could not have intended to incorporate it.

141. *Id.*
142. *Id.*
143. S. REP. NO. 90-1097, at 96 (citing Walder v. United States, 347 U.S. 62 (1954)).
144. 18 U.S.C. § 2515.
145. *Id.* §§ 2515, 2518(10)(a).
146. S. REP. NO. 90-1097, at 69.
147. *See, e.g.*, United States v. Brewer, 204 F. App'x 205, 208 (4th Cir. 2006) (reasoning that Fourth Amendment good-faith exception can justify rejection of an otherwise valid suppression motion); United States v. Moore, 41 F.3d 370, 376 (8th Cir. 1994) (acknowledging that the *Leon* good faith exception pertains to the Fourth Amendment, but interpreting the legislative history of the Wiretap Act as instructing courts to "adopt suppression principles developed in Fourth Amendment cases"). *But see* United States v. Giordano, 416 U.S. 505, 524 (1974) (where there exists a statutory suppression remedy, the terms of the statute govern, as opposed to the terms of the "judicially fashioned" Fourth Amendment exclusionary rule); United States v. Glover, 736 F.3d 509, 515–16 (D.C. Cir. 2013); United States v. Rice, 478 F.3d 704, 711–13 (6th Cir. 2007) (holding that the good faith exception does not apply to Wiretap Act suppression motions due to differences between legislative and judicial exclusionary rules); United States v. Spadaccino, 800 F.2d 292, 296 (2d Cir. 1986).
148. 468 U.S. 897 (1984).

Second, some courts have developed a plain view-type exception for the suppression remedy. In *United States v. Carey*,[149] the FBI obtained an intercept order for a particular individual's phone number, but the FBI later learned the phone was used by another person.[150] Before realizing the error, the FBI intercepted a number of incriminating phone calls.[151] The user of the phone, after being charged with a crime based on some of the intercepted communications, moved to suppress the evidence because the intercept order related to a separate individual.[152] Relying on the plain view doctrine from Fourth Amendment case law, the court reasoned that incriminating evidence obtained prior to the discovery that the target was not using the phone was admissible.[153]

Third, the Supreme Court has instructed lower courts to distinguish between "material" and "immaterial" deviations from the warrant requirements.[154] That has created two classes of statutory violations—ones that lead to suppression, and ones that do not. Only a "failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of [the] extraordinary investigative device" justify suppression.[155]

Similarly, in *Scott v. United States*,[156] the Court rejected the petitioners' argument that an agent's failure to make subjective, good-faith efforts to comply with minimization procedures required suppression.[157] The Court held that courts should look only to agents' actions, not motives, and those actions should be evaluated based on a reasonableness requirement.[158] The Court further noted that the interception of a high number of non-incriminating calls is not in itself sufficient to show a failure to comply with minimization

149. 836 F.3d 1092 (9th Cir. 2016).
150. *Id.* at 1094.
151. *Id.*
152. *Id.*
153. *See also* United States v. Ramirez, 112 F.3d 849, 851 (7th Cir. 1997).
154. United States v. Chavez, 416 U.S. 562 (1974).
155. *Id.* (quoting United States v. Giordano, 416 U.S. 505, 526 (1974)).
156. 436 U.S. 128 (1978).
157. *Id.*
158. *Id.* at 139–40.

procedures.[159] It is odd that good faith can justify dispensing with the suppression remedy, but bad faith doesn't warrant suppression.

There does not appear to be any empirical research on the number of suppression motions that are granted or denied. Recently, the Administrative Office of the United States Courts began publishing data, as part of its statutory reporting requirements, that shows whether suppression motions are pending, denied, or granted in cases where intercepts led to arrests and criminal proceedings.[160] But this information appears to be incomplete because it depends on reports filed by prosecutors.

One clear trend in interpretations of the suppression remedy, however, is that many courts have diluted the strength of this remedy over time. For example, as discussed above, some circuit courts have created a good-faith exception, borrowing from Fourth Amendment case law that did not exist when Congress passed the Wiretap Act.[161] As the Supreme Court appears to be increasingly hostile to the exclusionary rule, the statutory suppression remedy could be further diluted.

3. No Suppression Remedy for Illegal Interception of Electronic Communications

Congress, also, has declined to extend the statute's suppression remedy to new types of communications.[162] While a person may move to suppress "the contents of any wire or oral communication" intercepted pursuant to Title III, or evidence derived therefrom, if the wiretap did not comply with Title III's requirements, no such remedy exists in regards to the contents of electronic communications.[163] The decision not to extend the suppression remedy to electronic communications was, according to the Senate Report, made "as a result of discussions with the Justice Department."[164]

159. *Id.* at 140.

160. *See, e.g.*, *Table Wire A1—Appendix Tables Wiretap*, U.S. CTS. (Dec. 31, 2018), https://www.uscourts.gov/statistics/table/wire-a1/wiretap/2018/12/31.

161. *E.g.*, United States v. Brewer, 204 F. App'x 205, 208 (4th Cir. 2006).

162. S. REP. NO. 99-541, at 23 (1986).

163. 18 U.S.C. § 2518(10)(a) (2012) (emphasis added); *see also* United States v. Steiger, 318 F.3d 1039, 1052 (11th Cir. 2003) ("The Wiretap Act does not provide a suppression remedy for electronic communications unlawfully acquired under the Act."); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461 n.6 (5th Cir. 1994) (same); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (same).

164. S. REP. NO. 99-541, at 23 (1986).

The absence of a mandatory suppression remedy under the statute reduces the government's incentive to comply with the statutory safeguards and may disincentivize criminal defendants from litigating privacy rights in electronic communications, potentially masking illegal surveillance that affects other private citizens.

D. Civil Remedies and Criminal Penalties

While Congress has long recognized the importance of providing civil remedies to victims of Wiretap Act violations and imposing criminal sanctions on violators, the remedies provided are primarily directed at private citizens who engage in unlawful wiretapping.[165] They do little to disincentivize violations by law enforcement except in the most egregious cases.

In enacting the Wiretap Act, Congress recognized that "[i]t is not enough . . . just to prohibit the unjustifiable interception, disclosure, or use of any wire or oral communications."[166] "Criminal penalties have their part to play."[167] Accordingly, a Wiretap Act violation is a Class D felony, and, subject to specific exceptions, violations of the Act may result in fines and/or imprisonment for up to five years.[168] Congress also noted that "remedies must be afforded the victim of an unlawful invasion of privacy," including "civil recourse."[169] Victims of Wiretap Act violations may therefore generally seek equitable or declaratory relief and damages from violators.[170]

The exact contours of the civil remedy have changed over time. For example, the civil remedy originally provided for a civil suit for injunctive relief and damages against "any person" who violated the Wiretap Act, then extended liability to "any person or entity," and later narrowed the scope of the remedy contained in section 2520 to provide a cause of action against "any person or entity, other than the United States."[171] Today, civil suits for money damages against the United States for Wiretap Act violations are authorized by 18 U.S.C. § 2712.

---

165. *See* Pub. L. No. 107-56, Oct. 26, 2001, 115 Stat. 272 (extending liability under the Wiretap Act to "any person or entity, other than the United States").

166. S. REP. NO. 90-1097, at 2156 (1968).

167. *Id.*

168. 18 U.S.C. § 2511 (setting penalties); *id.* § 3559(a)(4) (classifying sentence).

169. S. REP. NO. 90-1097, at 2156 (1968).

170. *See* 18 U.S.C. § 2520.

171. *Compare* Pub. L. No. 90-351, June 19, 1968, 82 Stat. 197 ("any person"), *with* Pub. L. No. 99-508, Oct. 21, 1986, 100 Stat. 1848 ("any person or entity"), *and* Pub. L. No. 107-56, Oct. 26, 2001, 115 Stat. 272 ("any person or entity, other than the United States").

Nonetheless, neither the civil nor criminal remedies have functioned to effectively remedy the vast majority of Wiretap Act violations by government actors.

This is partly due to carve-outs that shield government actors from liability except for the most flagrant violations of the statute. Most notably, good faith is a complete defense against any criminal or civil action, providing a safe harbor for law enforcement officers and individuals acting at the behest of law enforcement officers who act in good faith reliance on legal process, such as a court warrant or order.[172] Accordingly, remedies are unlikely to apply where law enforcement officers obtain a court order, so long as the officer had a reasonable, good-faith belief that he acted legally pursuant to a court order.[173] Civil remedies are generally off the table when officers have a court order but subsequently violate the Act's core requirements, such as by failing to minimize the collection of private communications.[174] Additionally, the Act's prohibition on the use of a "device" to intercept an oral communication explicitly excepts devices that are "used by an investigative or law enforcement officer in the ordinary course of his duties."[175] In addition, to the extent that the government fails to provide notice of wiretapping to targets or others, victims of unlawful wiretaps have no way to even attempt to obtain a remedy. Perhaps for this reason, the civil remedy provisions that theoretically allow victims to seek remedies for wiretap violations are rarely utilized against government actors.

Further, it appears that criminal prosecutions are initiated against government actors for Wiretap Act violations only in cases of blatant abuse—for example, where a law enforcement officer has forged wiretap orders to spy on a love interest.[176]

Ultimately, then, while private actors who violate the Wiretap Act may face civil or criminal penalties, law enforcement officials who

172. 18 U.S.C. § 2520(d); *see* GINA STEVENS & CHARLES DOYLE, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 18–19 (2003), https://www.epic.org/privacy/wiretap/98-326.pdf.

173. Jacobson v. Rose, 592 F.2d 515, 523 (9th Cir. 1978). A defendant may assert a good-faith defense where: (1) "he had a subjective good faith belief that he acted legally pursuant to a court order"; and (2) "this belief was reasonable." *Id.*

174. 18 U.S.C. § 2520(d)(1).

175. *Id.* § 2510(5)(a)(ii).

176. *See* Staci Zaretsky, *Ex-Prosecutor Disbarred for Forging Wiretap Orders to Spy on Love Interest*, ABOVE L. (Jan. 4, 2018), https://abovethelaw.com/2018/01/ex-prosecutor-disbarred-for-forging-wiretap-orders-to-spy-on-love-interest/.

violate the statute or court wiretapping orders face few effective penalties.

V. GOING FORWARD

Going forward, advocates should be aware that a Title III-style super-warrant is not a panacea for privacy concerns—and may ultimately expand the use of an invasive investigative technique by legitimizing it. As the experience with wiretapping shows, initially strong limits can quickly erode. Merely parroting current Title III language in legislative proposals will not constitute strong limits, given current judicial interpretations of Title III. Should super-warrant procedures be considered, advocates will have to draft new language to effectively implement the intended safeguards behind Title III. In particular:

- The requirement that investigators show "necessity" before employing an intrusive technique should be demanding and should rely on clear, objective criteria.
- Minimization requirements should be strict, should impose concrete default rules, and should require that non-responsive data or data belonging to innocent third parties be promptly purged.
- Notice to affected parties should be required by default. Judges should have to explain in writing, on the basis of case-specific facts, when there is an exception or when notice is temporarily delayed. The number of affected parties who receive and who do not receive notice should be tracked and publicly reported.
- Statutory suppression remedies should be clearly defined and, where appropriate, should be stated in unambiguous, mandatory terms. A statute should be precise in identifying the specific violations that can justify suppression. A statute should also be clear that its suppression remedy is independent of any Fourth Amendment remedies or exceptions. A statute may have to state, for example, that there is no good-faith exception.
- A statute may need to provide for civil remedies and provide standing to sue.

- Transparency reporting may often be helpful, but it is far from sufficient in preventing the widespread use of novel surveillance techniques.

VI. CONCLUSION

The raw number of wiretap orders has increased dramatically since 1968. At the same time, the limitations built into the statute have been watered down or have otherwise proven to be less effective over time than many may assume at first glance. This history offers critical lessons as privacy advocates and policymakers consider regulations for face surveillance, familial DNA searches, government hacking, and other new surveillance technologies. The history of American wiretap law suggests that existing Wiretap Act protections are not a turn-key model for mitigating privacy risks in the face of new surveillance technologies.

APPENDIX A

Wiretap Report Data Comparison Sample						
Category	**2017**[177]	**2007**[178]	**1997**[179]	**1987**[180]	**1977**[181]	**1969**[182]
Total Intercept Applications Approved	3,813	2,208	1,186	673	626	304
Most Common Major Offense Specified (Number) [Percentage of Total]	Narcotics (2,027) [53%]	Narcotics (1,792) [81%]	Narcotics (870) [73%]	Narcotics (379) [50%]	Gambling (265) [42%]	Gambling and Book-making (102) [34%]
Most Common Location of Authorized Intercepts (Number)	Portable Device (3,584)	Portable Device (2,078)	Other (529)	Single Family Dwelling (285)	Single Family Dwelling (253)	Residence (135)
Total Intercepts Installed	2,421	2,119	1,094	634	601	271

177. *Wiretap Reports*, U.S. CTS., https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports (last visited Nov. 26, 2019).

178. *Id.*

179. *Id.*

180. STAT. ANALYSIS & REP. DIVISION, ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 24, tbl.7 (1990), https://www.ncjrs.gov/pdffiles1/Digitization/125933NCJRS.pdf.

181. ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 21 tbl.7 (1985), https://www.ncjrs.gov/pdffiles1/Digitization/98312NCJRS.pdf.

182. NWC Report, *supra* note 1, at 36, 277.

Wiretap Report Data Comparison Sample (continued)						
Category	**2017**[183]	**2007**[184]	**1997**[185]	**1987**[186]	**1977**[187]	**1969**[188]
Average Number of Persons Intercepted	149	94	197	104	72	152 (Federal)
Average Number of Intercepted Communications	5,989	3,106	2,081	1,299	658	1,498 (Federal)
Average Number of Incriminating Intercepted Communications [Percentage of Average Number of Intercepted Communications]	1,178 [20%]	920 [29%]	418 [20%]	230 [17%]	268 [40%]	1,228 (Federal)

183. *Wiretap Reports*, U.S. CTS., https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports (last visited Nov. 26, 2019).

184. *Id.*

185. *Id.*

186. STAT. ANALYSIS & REP. DIVISION, ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 24, tbl.7 (1990), https://www.ncjrs.gov/pdffiles1/Digitization/125933NCJRS.pdf.

187. ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 21 tbl.7 (1985), https://www.ncjrs.gov/pdffiles1/Digitization/98312NCJRS.pdf.

188. NWC Report, *supra* note 1, at 36, 277.