Vanderbilt Law Review

Volume 64 | Issue 4 Article 7

5-2011

Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement

Seth M. Hyatt

Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement

I. INTRODUCTION

> The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations.
>
> — Justice William O. Douglas[1]

For the past forty years, theory and practice in electronic surveillance have enjoyed an uneasy coexistence. In theory, under Title III of the Omnibus Crime Control and Safe Streets Act of 1968

1. Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring).

("Title III"),[2] government agents must use wire and electronic taps sparingly,[3] and only under strict judicial supervision.[4] In practice, however, federal courts have recognized countless loopholes and exceptions,[5] leading critics to wonder whether Title III meaningfully limits state investigatory power.[6]

Nowhere is this tension more apparent than in the context of "minimization."[7] Under Title III, government agents conducting electronic surveillance must "minimize the interception of communications not otherwise subject to interception under this chapter."[8] They must not listen in on any more private communication than is necessary. But what, exactly, must "minimization" entail? The statute itself does not say, though the Senate Report—which endorsed the Warren Court's reasoning in *Berger v. New York*[9]—suggests that the requirement was meant to apply broadly, against *all* unnecessary interceptions.[10]

The lower courts, however, had different ideas. Instead of adopting a bright-line rule, federal courts since the 1970s have carved out numerous partial exceptions to the minimization requirement. They have largely exempted foreign-language calls,[11] as well as short

---

2. 18 U.S.C. §§ 2510–2520 (2006).

3. § 2518(3)(a) (requiring prosecutors seeking an electronic surveillance warrant to first demonstrate probable cause to believe that the subject of the surveillance has committed a serious felony); § 2518(3)(c) (requiring prosecutors seeking an electronic surveillance warrant to first demonstrate that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous").

4. § 2518(6) (requiring prosecutors conducting electronic surveillance to make regular status reports to the judge who issued the authorization).

5. *See infra* notes 168–80 and accompanying text.

6. *See, e.g.*, 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) ("There is substantial evidence . . . that the protections initially established in 1968 and affirmed in 1986 are not working as intended. It appears increasingly apparent that components of the balanced legislative scheme have been watered down by Congress itself and by the judiciary.").

7. § 2518(5).

8. *Id.*

9. S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.

10. Berger v. New York, 388 U.S. 41, 62–63 (1967) ("[I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than eavesdropping devices.").

11. United States v. Gambino, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990) ("Given the difficulty and expense of providing for simultaneous translation of Sicilian conversations, and the delay in activating the wiretaps that such a requirement might have caused, the Court finds that the government's minimization efforts are acceptable under Title III and the fourth amendment.").

calls,[12] "ambiguous" calls,[13] and calls monitored during the early stages of an investigation.[14] The underlying test—adopted by the Burger Court in *Scott v. United States*—is a test of "reasonableness," and grants a high degree of deference to police and prosecutorial decisions.[15]

Further complicating matters is the fact that Congress passed Title III in 1968, well before the "tech boom" of the 1980s and early 1990s made cell phones, text messages, and e-mail commonplace.[16] The Electronic Communications Privacy Act of 1986 ("ECPA") partially addressed this problem, extending Title III to cover "electronic" as well as "wire" communications.[17] However, the statute provided no clear guidance on *how* to minimize these new types of messages.[18] Phone surveillance had long been governed by a temporal restriction, commonly known as the "two-minute" rule. But this approach was ill-suited for nonverbal communications such as e-mail and text messages.[19] Did Congress intend for the minimization requirement to provide the same level of privacy protection to e-mail and text messages as it did for phone calls? And, regardless of

12. United States v. Segura, 318 F. App'x 706, 712 (10th Cir. 2009) (holding that minimization is not required for any phone calls under two minutes long).

13. United States v. Williams, 109 F.3d 502, 507 (8th Cir. 1997).

14. United States v. Willis, 890 F.2d 1099, 1102 (10th Cir. 1989) ("It has been recognized that monitors may need to listen for longer periods of time in the early stages of such investigations in order to determine the identity of speakers and significance of conversations.").

15. Scott v. United States, 436 U.S. 128, 139–40 (1978) ("Because of the necessarily ad hoc nature of any determination of reasonableness, there can be no inflexible rule of law which will decide every case. The statute does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations.").

16. According to the Senate Report accompanying the Electronic Communications Privacy Act, the Federal Communications Commission approved the use of cellular phones for the first time in 1981. S. REP NO. 99–541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3563.

17. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510(12) (2006) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate of foreign commerce").

18. However, the Senate Judiciary Committee Report did provide some guidance:

> [A]lthough the statutory standards for minimizing wire, oral, and electronic communications are the same under the proposed subsection 2518(5), the 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 minimize in the same manner as with a wire interception.

S. REP. NO. 99–541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585.

19. *See infra* notes 129–32 and accompanying text.

congressional intent, how much protection has the minimization requirement *really provided* for these nonverbal communications?[20]

The following analysis addresses these issues and, more specifically, attempts to answer four closely related questions: (1) How much privacy protection does the minimization requirement provide to nonverbal, electronic communications? (2) How different is this protection from what the law affords to phone calls under Title III? (3) Why, as law-abiding citizens, should we care? and (4) In light of the previous three questions, does it make sense to retain the minimization requirement in the context of electronic intercepts?

Ultimately, this analysis will demonstrate that the minimization requirement makes no sense in the context of nonverbal, electronic interceptions. Courts have spent more than twenty years watering this requirement down, leaving behind a bizarre, hollowed-out protection that serves as a procedural nuisance to law enforcement without providing meaningful protection to individual privacy. In a very real sense, courts have achieved the worst of both worlds.

In reaching this conclusion, this Note is organized into four parts. Part I provides a brief history of electronic surveillance law, with an emphasis on the development and subsequent application of the minimization requirement. Part II examines the current minimization requirement and seeks to discern what privacy protections it provides, if any, for electronic communications such as text messages. Part III compares and contrasts the modern minimization requirement with the "traditional" 1968 version, concluding that the latter does in fact provide more protection to phone calls than the former does to electronic communications. Finally, Part IV asks why we should we care about whether minimization fails to protect electronic communications. In answering that all-important question, Part IV presents and critiques the competing positions of privacy purists ("purists")[21] and privacy

20. The general consensus among legal scholars appears to be that it has provided only modest protection, at best, to nonverbal communications. *See, e.g.*, Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics"*, 7 HARV. J.L. & TECH. 239, 266 (1994) ("Minimization as it has been understood up until now can have no meaning in an increasingly digital world.").

21. For the purposes of this Note, "purists" are scholars and jurists who believe that surveillance is dangerous not only because of its potential to violate due process, but because it necessarily involves government agents observing the private details of an individual's life. Purists believe that surveillance, if allowed at all, must be tightly controlled at every step of the process. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

pragmatists ("pragmatists"),[22] ultimately concluding, however grudgingly, that pragmatists have the better argument and that the minimization requirement makes no sense in the context of electronic interceptions.

II. ACTION AND OVER-REACTION: A BRIEF HISTORY OF ELECTRONIC SURVEILLANCE LAW

The history of U.S. surveillance law is one of dueling philosophies: privacy purity versus privacy pragmatism.[23] As early as the 1860s, state police forces had begun tapping telegraph transmissions in criminal investigations,[24] a technique that would develop into the modern wiretap a generation later.[25] In response, increasing numbers of academics publicly condemned such techniques, arguing for stronger legal protections for individual privacy.[26]

Caught in the middle were Congress and the Supreme Court. Although they sat out the early rounds of the debate,[27] both were eventually forced to act and, in so doing, to take sides between the purists and the pragmatists. By their own accounts, the Court and Congress struggled mightily over the years to carve out middle-ground positions—reconciling, to the extent possible, the interests of law enforcement with those of privacy advocates.[28] But history soon put

---

22. "Pragmatists" are scholars and jurists who look with skepticism on the idea that there is any absolute right to being "let alone" and who look with even greater skepticism at the idea that the government should hamstring its law enforcement officers to protect such a right. *See, e.g.*, Berger v. New York, 388 U.S. 41, 73 (1967) (Black, J., dissenting) ("However obnoxious eavesdroppers may be they are assuredly not engaged in a more 'ignoble' or 'dirty business' than are bribers, thieves, burglars, robbers, rapists, kidnappers, and murderers. . . . And it cannot be denied that to deal with such specimens of our society, eavesdroppers are not merely useful, they are frequently a necessity.").

23. *See infra* Part IV (comparing and contrasting the purist and pragmatist approaches).

24. *See Berger*, 388 U.S. at 45 (discussing an 1862 California statute enacted to put an end to the practice).

25. *Id.* at 46.

26. *See, e.g.*, Samuel Warren & Louis Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890) ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. . . . [N]umerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' ") (quoting COOLEY ON TORTS 29 (2d ed. 1888)). Brandeis, one of the coauthors of this piece, would return to the same theme in his famous *Olmstead* dissent. 277 U.S. at 476 (Brandeis, J., dissenting).

27. *See* S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 (noting that the Supreme Court did not consider the issue until 1928, nor did Congress until 1934).

28. *Compare Berger*, 388 U.S. at 63–64 ("The Fourth Amendment does not make the 'precincts of the home or the office . . . sanctuaries where the law can never reach,' but it does

the lie to such claims of balanced neutrality. Congress, responding to citizens' fears of unchecked government power, placed increasingly tight restrictions on police surveillance.[29] The Court, in turn, took a largely pragmatic approach, interpreting congressional acts as standards rather than rules, and showing a high degree of deference to law enforcement decisions.[30]

From this decades-long tug-of-war between bright-line rules and deferential standards, our current, jumbled system of surveillance law eventually emerged.

A. From the Many, One? The Tentative Emergence of Federal Wiretap Regulation

Prior to the Court's 1928 decision in *Olmstead v. United States*, police wiretaps were regulated, if at all, by state-level authorities.[31] Many states banned the practice outright,[32] though evidence suggests that police departments sometimes just ignored these prohibitions.[33] At the same time, a broader constitutional question loomed in the background: Do wiretaps implicate the Fourth Amendment,[34] or is electronic surveillance beyond the scope of what the Framers would have recognized as "searches" or "seizures"?[35]

---

prescribe a constitutional standard that must be met before official invasion is permissible.") (citations omitted), *with* S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 ("Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.").

29. *See generally* 18 U.S.C. §§ 2510–2520 (establishing numerous procedural requirements that law enforcement officers must meet before and during electronic wiretaps).

30. *See, e.g.*, Scott v. United States, 436 U.S. 128, 139 (1978) ("Because of the necessarily ad hoc nature of any determination of reasonableness, there can be no inflexible rule of law which will decide every case.").

31. Federal law enforcement was in its infancy during this time, so it is not surprising that wiretaps and the rules governing them came primarily from the states. For an overview of early state wiretap laws, see *Berger*, 388 U.S. at 45–46.

32. New York and Illinois banned police wiretaps in 1895. California extended its ban on telegraph surveillance to phone surveillance in 1905. *Id.* at 46.

33. *See id.* ("[A] New York legislative committee found that police, in cooperation with the telephone company, had been tapping telephone lines in New York despite an Act passed in 1895 prohibiting it.").

34. Admittedly, answering this Fourth Amendment question would not have been dispositive of the issue, as the Supreme Court did not formally incorporate that amendment against the states until 1961. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

35. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

After years of silence, the Court finally addressed this question in *Olmstead*.[36] There, seventy-two petitioners challenged their convictions under the National Prohibition Act for transporting and selling intoxicating liquor on grounds that federal agents had illegally obtained evidence by monitoring their phone calls.[37] Petitioners argued that these conversations were the equivalent of sealed letters[38] and that federal agents could not intercept them without first obtaining a warrant.[39] The Court disagreed.

Writing for the majority, Chief Justice Taft argued that the Fourth Amendment protects only "material things" and stated that "[t]he amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of hearing and that only."[40] The Constitution, in other words, could not restrain the power of police to monitor private conversations.[41]

Although the Court rejected petitioners' constitutional claim, it emphasized in its holding that "Congress may, of course, protect the secrecy of telephone messages . . . by direct legislation, and thus depart from the common law of evidence."[42] Six years later, Congress accepted that invitation, enacting the Federal Communications Act of 1934 ("FCA").[43] It provided, in relevant part, that "*no person* not being authorized by the sender, shall intercept any communication and divulge or publish the existence of contents, purport, effect or meaning of such communication to any person."[44] This language effectively banned electronic surveillance by both private citizens and law enforcement.

---

36. Olmstead v. United States, 277 U.S. 438, 455 (1928).

37. *Id.* at 456 ("The information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers.").

38. The Court had ruled in 1877 that police could not search or seize mailed letters without first obtaining a warrant. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

39. *Olmstead*, 277 U.S. at 464.

40. *Id.*

41. The Court abandoned this narrow definition of "search" in its landmark *Katz* decision. Katz v. United States, 389 U.S. 347, 352 (1968). In light of *Katz*, it is clear that electronic surveillance is now considered a search under the Fourth Amendment, though the Court has never directly addressed what constitutional—as compared to statutory—requirements exist for such surveillance. *But see* Berger v. New York, 388 U.S. 41, 58–59 (1967) (identifying features of a New York state wiretapping statute that made it incompatible with the Fourth Amendment).

42. *Olmstead*, 277 U.S. at 465–67.

43. Federal Communications Act of 1934 § 705, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605).

44. *Id.* (emphasis added).

B. Problem Not Solved: The Failure of the FCA and the Enactment of Title III

By all appearances, the FCA should have resolved the electronic surveillance problem once and for all. Assuming, as this Note does, that Congress at the time supported the purist position, the ban on electronic surveillance would appear to be a total victory, particularly given the statute's unambiguous language. That language, prohibiting *all* wiretaps, prevented the Court from watering down the prohibition through interpretation.[45] So why did Congress abandon the FCA in 1968, exchanging a clear-cut ban for a complex—and arguably convoluted—system of regulation in Title III? What happened during the intervening thirty-four years to convince legislators that "the present state of the law is extremely unsatisfactory"?[46]

Two answers readily emerge. The first, somewhat surprisingly, is organized crime.[47] Though hardly a new problem in 1968,[48] legislators at the time increasingly worried about "highly organized, structured and formalized groups of criminal cartels, whose existence transcends the crime known yesterday, for which our criminal laws and procedures were primarily designed."[49] Spurred to action by the release of the President's Crime Commission Report, THE CHALLENGE OF CRIME IN A FREE SOCIETY, Congress concluded that traditional law enforcement techniques had failed to penetrate these "corporations of corruption."[50] New tools were needed, and wiretaps fit the bill.[51]

At the same time that law enforcement was clamoring for greater investigatory power, privacy advocates were questioning whether the FCA was truly the ban on wiretapping that Congress intended it to be.[52] Professor Susan Freiwald has investigated this

---

45. *See, e.g.*, Nardone v. United States, 302 U.S. 379, 382 (1937) (upholding the Act against a claim that the prohibition was not meant to apply to government agents).

46. S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.

47. *Id.* at 2157 ("The major purpose of Title III is to combat organized crime.").

48. Congress itself conceded this point. *See id.* ("We have always had forms of organized crime and corruption.").

49. *Id.*

50. *Id.*

51. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968 § 801(a), 42 U.S.C. § 3711 ("Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications . . . is an indispensible aid to law enforcement and the administration of justice.").

52. *See* S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 ("Both proponents and opponents of wiretapping and electronic surveillance agree that the present state

issue and concluded that government agents "conducted a significant number of wiretapping investigations, even when it was illegal to do so."[53] Law enforcement, in other words, "simply broke the law."[54] The Justice Department was aware of these developments, but between 1934 and 1968 did not prosecute a single government agent, state or federal, for violating the FCA. The agency thus signaled to law enforcement that their agents could flaunt the wiretap ban with impunity.[55] As Professor Freiwald noted, this disconnect between theory and application helps to explain the fact that many commentators actually viewed proposals to permit surveillance for the first time as "opportunities to crack down on illegal wiretapping."[56] By bringing the process out of the shadows, Congress could at least hope to control its excesses.

C. The Shape of Things: The Structure of Title III and the Birth of the Minimization Requirement

Having decided to relegalize police wiretaps, Congress faced the daunting question of how to control them.[57] The answer it came up with was Title III.[58] Because all subsequent surveillance laws in this country developed, in some form or another, from this act, it is worth pausing for a moment to explain its regulatory framework in some detail.

The constraints set out in Title III fall into two categories: (1) those that limit law enforcement's power to *initiate* a wiretap; and (2) those that limit the ways in which agents may *conduct* the wiretap.

The first category of restraint arises from Title III's onerous warrant requirement, which demands greater certainty and specificity

---

of the law in this area is extremely unsatisfactory and that Congress should act to clarify the resulting confusion.").

53. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 33 (2004).

54. *Id.*

55. *Id.*

56. *Id.*

57. It is clear from the legislative history that Congress intended for Title III to tightly constrain the use of police wiretaps. *See* S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 ("[T]itle III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers engaged in the investigation or prevention of specified types of serious crimes, and only after authorization of a court order obtained after a showing and finding of probable cause.").

58. Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2520).

than a traditional search warrant.[59] An agent applying for wiretap authorization must, for example, describe the place where the communication is to be intercepted;[60] describe the type(s) of communications to be intercepted;[61] establish probable cause to believe that the target is engaged in a specific, enumerated criminal offense;[62] and establish probable cause to believe that communications relating to that particular offense will be obtained through the surveillance.[63] Additionally, the agent must demonstrate that "normal investigative techniques have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[64] Put simply, Title III seeks to ensure that investigators know what they are looking for prior to starting the surveillance and are not just engaging in a fishing expedition.

Success in obtaining wiretap authorization does not mean the agent is then free to conduct surveillance in whatever manner he sees fit. The second category of Title III protections provides agents with specific instructions, laying down ground rules for how surveillance must proceed. In particular, it establishes the following:

> Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.[65]

Just like the category one restrictions, these requirements are meant to prevent government fishing expeditions. They force government agents to conduct their surveillance within strict time limits—ensuring that the surveillance will not become a new form of "general warrant"[66]—and command the agents to "minimize" all communications other than those they are authorized to intercept.[67]

---

59. § 2518.

60. § 2518(1)(b)(ii).

61. § 2518(1)(b)(iii).

62. § 2518(3)(a).

63. § 2518(3)(b).

64. § 2518(3)(c).

65. § 2518(5) (emphasis added).

66. Congress appeared to take to heart Justice Brandeis's concern that "[a]s a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping." Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

67. As noted in the introduction, the statute itself provides relatively little guidance on what "minimization" should entail. *See supra* notes 8–10 and accompanying text. Part II and III of this Note will take up this question at much greater length.

Finally, in support of these two categories, Title III establishes several forms of redress for victims of illegal government surveillance, including a right of civil action.[68] In some ways, this is the critical difference between Title III and the FCA. As Professor Freiwald has noted, the FCA had not clearly provided for civil claims, raising serious questions about what would stop law enforcement from just ignoring the statutory prohibition.[69] Title III, in contrast, explicitly provides for a damage remedy, complete with attorneys' fees and, where appropriate, punitive damages.[70] It also calls for suppression of illegally obtained communications in any subsequent criminal trial.[71]

By including such meaningful punitive provisions, Congress sought to ensure that law enforcement would take the new law seriously and would not simply return to the bad old days of strict-in-theory but lax-in-practice surveillance.[72]

The Supreme Court, however, had a different vision, at least as applied to minimization.

D. Scott v. United States *and the "Reasonableness" Requirement*

In light of the terse language of the minimization requirement[73] and the absence of any detailed legislative history, it was only a matter of time before the Court provided its own interpretation. Though law enforcement had to wait ten years for a final judicial pronouncement on Title III,[74] the Court finally took up

---

68. §§ 2515, 2520.

69. Freiwald, *supra* note 53, at 33.

70. § 2520(b)(2)–(3). The statute also provides specific instructions about how civil damages should be calculated, instructing courts to award the greater of (1) "the sum of actual damages suffered by the plaintiff and any profits made by the violator," or (2) "whichever is the greater of $100 a day for each day of violation or $10,000." § 2520(c)(2).

71. § 2515 ("Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court . . . .").

72. *See, e.g.*, Michael Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 44 (1983) ("Title III's sponsors clearly recognized that society's right to privacy would depend, in large part, upon this system of statutory controls and that these controls, in turn, were dependent upon proper judicial implementation.").

73. The only reference in Title III to minimization is the command that the wiretap "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." § 2518(5).

74. Several lower courts had addressed the minimization requirement prior to *Scott v. United States*, generally handling the requirement permissively. For an overview of these decisions, see Goldsmith, *supra* note 72, at 104.

the minimization question in 1978, when it decided *Scott v. United States*.[75]

The petitioners in *Scott* had been convicted of a conspiracy to import and sell drugs in the Washington, D.C. area, based largely on wiretap evidence.[76] Petitioners appealed these convictions on the ground that government agents had intercepted *all* of the phone conversations over a particular line, despite judicial orders requiring the agents to "minimize" nonpertinent calls.[77] Petitioners argued that such blatant disregard for personal privacy violated the minimization requirement and warranted suppression of the evidence.

But the Court disagreed. Writing for the majority, Justice Rehnquist rejected the idea of any bright-line minimization rule, adopting instead a balancing test that "will depend on the facts and circumstances of each case."[78] Taking this deference for law enforcement even further, the majority suggested that it would not necessarily matter whether the agents had *deliberately* ignored the statutory requirement, so long as their conduct was "objectively" reasonable.[79] And because the investigation in question concerned a "widespread conspiracy," the Court concluded that it was perfectly reasonable to conduct extensive surveillance—even to the point of listening to *all* conversations on the target phone line.[80] While this permissive view of minimization was not quite a kiss of death for the requirement, it did pave the way for a host of new exceptions from the lower federal courts.[81] As a result, subsequent commentators were not wrong in arguing, in light of *Scott* and its progeny, that "the 'minimization requirement' imposes little in the way of additional checks on the execution of an authorized wiretap."[82]

E. Best-Laid Plans: The Electronic Communications Privacy Act and Congress's Failure to Keep Up with Changing Technologies

As previously noted, Congress passed Title III in 1968, roughly a generation before the current "tech boom." As a result, the statute

75. 436 U.S. 128, 130–31 (1978).

76. *Id.* at 131.

77. *Id.* at 130–31.

78. *Id.* at 139–40.

79. *Id.* at 138 ("[T]he fact that the officer does not have the state of mind which is hypothecated by the reasons which provide the legal justification for the officer's action does not invalidate the action taken as long as the circumstances, viewed objectively, justify that action.").

80. *Id.* at 140–41.

81. *See infra* Part II.E.

82. Downes, *supra* note 20, at 260.

only governed interception of "wire communications"—defined by the statute as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception."[83] Congress similarly defined "intercept" as the "*aural* acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[84]

These narrow definitions became more and more problematic as technology advanced. Specifically, as law enforcement agencies began intercepting new forms of communication, courts were increasingly forced to determine whether such surveillance fell under the aegis of Title III. For example, in *United States v. Gregg* the Western District of Missouri faced the question of whether monitoring telex messages constituted an "interception."[85] Based on the narrow statutory definition, the court concluded that it did not and that Title III therefore provided no protection to the target.[86] Similarly, in *United States v. Rose*, the First Circuit concluded that Ham radio broadcasts were not entitled to statutory protection.[87] As cases like these became more frequent, Congress concluded it was time for a change: Title III would have to adapt to shifting technological realities if it was going to continue protecting individual privacy.[88]

To meet that challenge, Congress enacted the ECPA in 1986, the first significant amendment in the history of Title III.[89] The Act's most basic change was to the definition of "intercept," expanding the

---

83. Omnibus Crime Control and Safe Streets Act of 1968 § 802(1), Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510(1)). The phrase "any communication" has since been amended to read "any aural transfer." 18 U.S.C. § 2510(1) (2006).

84. § 2510(4) (emphasis added).

85. United States v. Gregg, 629 F. Supp. 958, 961 (W.D. Mo. 1986). Telex machines were precursors to modern fax machines.

86. *Id.* at 962 ("[T]his interception simply is not the type of 'aural acquisition' within the purview of Title III. If Congress had intended for Title III to encompass all communications in which the contents of the communications were intercepted, it would have said so.").

87. United States v. Rose, 669 F.2d 23, 25 (1st Cir. 1982). Ham radio was, admittedly, a well-established technology in 1968. However, it appears to have nonetheless been beyond the contemplation of Congress.

88. S. REP. NO. 99–541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 ("Title I of the Electronic Communications Privacy Act addresses the interception of wire, oral and electronic communications. It amends existing chapter 119 of title 18 to bring it in line with technological developments and changes in the structure of the telecommunications industry.").

89. *Id.* at 1, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555 ("This bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

term to cover electronic as well as wire communications.[90] If the ECPA had simply stopped there, it may have maintained a workable regulatory framework. But Congress went further, making small but important changes to how Title III would apply in the context of nonwire intercepts.[91] The two changes relevant to this Note were to the exclusionary remedy and the concept of minimization.

The first change—spelled out in ECPA § 101(e)—removed *statutory* exclusionary relief for illegally intercepted electronic communications.[92] The reasons for this change are not at all obvious and appear to undermine Congress's stated intent that the ECPA protect against "the unauthorized interception of electronic communications."[93] The only explanation the Senate Report provided was that the change was a result of "conversations with the Justice Department,"[94] suggesting that the arch-pragmatists in federal law enforcement had influenced the drafting process.

The second and more important change was to Congress's understanding of minimization itself.[95] Although the ECPA did not alter the basic language of Title III's minimization requirement, the Senate Report emphasized that minimization of electronic communications "would require a somewhat different procedure than that used to minimize a telephone call."[96] Expounding on this idea, the report noted:

> 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.[97]

Two critical points stand out from this statement. First is the assertion that, in the context of electronic intercepts, minimization

---

90. ECPA of 1986 § 101(a)(3), Pub. L. No. 99–508, 100 Stat. 1848 (amending 18 U.S.C. § 2510(4)).

91. §§ 101, 103; *see also* Freiwald, *supra* note 53, at 41–42 (providing a general overview of the changes that the ECPA made to Title III).

92. § 101(e). The Senate Report on this section emphasizes that "[i]n the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing Constitutional law with respect to the exclusionary rule." S. REP. NO. 99–541, at 23 (1986), *reported in* 1986 U.S.C.C.A.N. 3555, 3577. It is not immediately clear, however, exactly how the scope of Constitutional exclusion compares with that of Title III exclusion.

93. S. REP. NO. 99–541, at 1, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

94. *Id.* at 23, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

95. *Id.* at 1, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585.

96. *Id.*

97. *Id.* (emphasis added).

should involve at least one government agent reviewing *every* intercepted communication.[98] Second is the report's suggestion that appropriate minimization is defined, at least in part, by the technology available to law enforcement. In this respect, the Act's amorphous notions of wiretap regulation in general, and minimization requirements in particular, lend support to Professor Freiwald's conclusion that "the ECPA's complexity has weakened its ability to protect privacy."[99]

But *how* weak is it? *How much* less does it protect privacy compared to the original Title III? Parts III and IV focus on these questions, respectively.

III. PRYING EYES AND COMPLACENT COURTS: THE FEDERAL JUDICIARY'S UNWILLINGNESS TO ESTABLISH MEANINGFUL MINIMIZATION REQUIREMENTS

Having outlined the origins and current state of the minimization requirement, the next question is, does it work? Given Congress's goal of protecting privacy against modern, high-tech surveillance,[100] does minimization advance that goal in any meaningful way?

Unfortunately, the answer to that question is no. In light of the relevant case law and federal surveillance statistics,[101] it is clear that minimization provides no real privacy protection beyond that contained in Title III's heightened warrant requirement.[102]

The reasons for this failure are threefold. First, courts—following the Supreme Court's lead in *Scott*—are overly deferential to

98. *See id.* ("[M]inimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all nonrelevant materials and disseminate to other officials only that information which is relevant to the investigation.").

99. Freiwald, *supra* note 53, at 42.

100. *See supra* note 89 and accompanying text.

101. One of the most useful sections of Title III is its reporting requirement, spelled out at length in § 2519. That section requires:

> In June of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year.

18 U.S.C. § 2519(3) (2006). The federal judiciary makes these reports publicly available. At present, federal Wiretap Reports for the years 1997–2009 are available at *Wiretap Reports*, U.S. COURTS, http:/www.uscourts.gov/statistics/wiretapreports.aspx (last visited Mar. 28, 2011).

102. *See supra* notes 59–64 and accompanying text; *see also* Downes, *supra* note 20, at 260 (explaining the rather minimal effect of the minimization requirement).

law enforcement agencies. In practice, this often means that courts take law enforcement agents at their word when they assert that they have adequately minimized nonpertinent communications. Second, in cases of electronic interceptions,[103] courts interpret minimization so loosely as to make it effectively worthless. Third, for most forms of electronic communication, including text messages, government agents can sidestep minimization altogether by performing other types of surveillance that do not require "intercepting" the communications.[104]

A. Some Initial Clarification

Before diving into this analysis, a point of clarification is in order concerning the underlying subject of this Note: minimization *in the context of text-message interceptions*. By this point, skeptical or curious readers may be wondering about the value of such a narrow topic, particularly given the paucity of case law.[105] Why not address minimization more generally, or at least expand the scope to cover different forms of electronic communication?

The basic reason is that text messages are an interesting gray area in modern surveillance law. Traditional wiretaps have gone on for more than one hundred years[106] and have been subject to federal regulation for more than forty years. The minimization requirement in that context is well established and comparatively well defined. Cell phones, though technologically different from landlines, are still a form of oral communication, and therefore fit comfortably into the existing minimization framework. At the other extreme, e-mail is beyond the bounds of Title III and ECPA protection.[107] Law enforcement typically obtains e-mail *after* it arrives in the recipient's inbox, which does not meet the legal definition of "interception."[108]

---

103. For the purposes of this analysis, "electronic interceptions" is defined broadly to include the interception of all electronic forms of communication but does not include traditional wiretaps.

104. § 2518(5) (stating that law enforcement must minimize "the *interception* of communications not otherwise subject to *interception* under this chapter") (emphasis added).

105. To date, research has not revealed a single federal case that directly addresses the minimization of text messages.

106. *See supra* notes 24–25 and accompanying text.

107. *See, e.g.*, United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers. . . . They may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient.").

108. *Id.*; *see also* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994) ("[R]equirements applicable to the interception of electronic communications, such as those

Text messages, to borrow from Goldilocks, are in this respect neither "too hot" nor "too cold." They are "just right" for scholarly analysis because Title III applies to them, but in ways that are not entirely clear.

The other reason to focus on text-message minimization is that it makes for a useful test case. Since the ECPA does not cover e-mail, and cell-phone calls now fall under traditional Title III rules,[109] text messages are the one major sphere of electronic communication where minimization might still make a difference. In other words, if minimization does not protect privacy in text messages, then it probably has no value outside the traditional wiretap context.

B. Undue Deference: The Failure of Courts to Provide Meaningful Oversight

When an individual claims that government agents have violated the minimization requirement, the judicial response often unfolds as follows:

> Claimant: Your Honor, the government has failed to take reasonable steps to minimize nonpertinent communications. Therefore, under Title III, the evidence should be suppressed.[110]
>
> Judge: (To government) Is this true, counselor?
>
> Prosecutor: Not at all, your Honor. Look, the investigating agents drafted this minimization memo, specifically stating that nonpertinent communications should be minimized. And I think we can all safely assume that the agents followed their own procedures, can't we?
>
> Judge: Agreed. The defendant's motion to suppress is hereby denied.

While this hypothetical is obvious hyperbole, it reflects one of the basic problems of minimization, both for wire and electronic communications. Following the Supreme Court's decision in *Scott,*

---

governing minimization, duration, and the types of crimes that may be investigated, are not imposed when the communications at issue are not in the process of being transmitted at the moment of seizure, but instead are in electronic storage.").

109. § 2516(1) (noting that federal judges may issue an order authorizing "the interception of wire *or oral* communications") (emphasis added).

110. As noted in Part II, the ECPA does not provide for a suppression remedy for electronic surveillance. *See supra* note 92 and accompanying text. However, a constitutional suppression remedy may still be appropriate in some cases, and, even in a suit for damages, the same basic framework would apply.

judges tend to look at whether investigators developed minimization procedures without giving much attention to whether the agents actually *followed* them.

In *United States v. Rivera*, for example, drug traffickers appealed their convictions on the grounds that DEA agents failed to conduct reasonable minimization and indiscriminately labeled many nonpertinent cell-phone calls as pertinent.[111] In rejecting these claims, the Ninth Circuit emphasized that "all agents working on the case and all monitors were required to read [the supervising agent]'s affidavit, the court order for the wiretap, and the minimization memorandum."[112] The agents, of course, could easily have read and then blatantly ignored those documents, but the court refused to entertain that possibility.[113]

Similarly, in *United States v. Szpyt*, a district court found the government had met its initial burden of reasonable minimization by demonstrating that it had trained its agents to respect the privacy of privileged phone calls and had filed occasional reports regarding its minimization efforts.[114] As in *Rivera*, however, the judge placed greater emphasis on this plan than on its subsequent implementation.[115]

Moreover, federal agents *do* sometimes ignore internal guidelines. In *United States v. Renzi,* FBI agents obtained a wiretap order as part of their investigation into possible election law

111. 527 F.3d 891, 904 (9th Cir. 2008).

112. *Id.* A minimization memorandum is a document, often prepared by an Assistant U.S. Attorney, explaining to law enforcement personnel the rules and procedures they must follow in conducting electronic surveillance. *See, e.g., id.* at 905.

113. *Id.* at 904 ("It is apparent from the record that the DEA's monitoring procedures and its training of the monitors were adequate.").

114. United States v. Szpyt, Criminal No. 08–54–P–S, 2008 WL 4840896, at *21 (D. Me. Nov. 9, 2008) ("Van Alstyne averred that minimization standards would be strictly followed, that monitoring agents would be trained to implement such standards, including respect for the privacy of innocent and privileged phone calls, and that the government would supply periodic reports to the court touching, inter alia, on its minimization efforts. Similar procedures and training have been deemed adequate in other cases.").

115. *Id.* at *22 (shifting the burden of proof to defendants to show that government agents insufficiently or improperly minimized); *see also* United States v. Haque, 315 F. App'x 510, 519 (6th Cir. 2009) ("Special Agent Morgan testified that all persons involved in the instant surveillance read the original minimization order and attended a briefing where the minimization procedures were discussed. Additionally, two agents involved in the surveillance were charged with seeing that the procedures were followed."). *But see* United States v. Mancari, 663 F. Supp. 1343, 1359 (N.D. Ill. 1987) (ordering further factfinding on an alleged minimization violation and holding that government agents, despite their minimization memo, had failed to make a prima facie showing of reasonableness).

violations.[116] The supervising attorney drafted a memorandum prohibiting agents from listening to or recording *any* calls subject to attorney-client privilege.[117] But, as a magistrate judge later determined, agents occasionally ignored the memo and recorded most of the calls between the defendant and one of his attorneys—including a number of privileged communications.[118] As a consequence, the court excluded *all* of the government's wiretap evidence, concluding that the government "conducted an unreasonable wholesale interception of calls they knew to be attorney-client communications."[119] On the one hand, this case shows that government agents cannot always be trusted to police their own wiretaps. On the other hand, it suggests that at least some courts—unlike in *Rivera* and *Szpyt*—refuse to take law enforcement claims at face value.

So which approach is more common: the broad deference of *Rivera* and *Szpyt*, or the critical oversight of *Renzi*? In truth, it is hard to know. The cases above are anecdotal and may reflect nothing more than the proclivities of individual judges or districts. However, the Federal Wiretap Reports suggest that deference to law enforcement is the rule rather than the exception.[120] Though they present no specific data regarding minimization, these reports show a consistent, generalized pattern of deference to investigators at all stages of the surveillance process. In 2007, for example, federal courts granted two motions to suppress while denying ninety-eight.[121] In 2006, the ratio was one motion granted to thirty-one motions denied.[122]

This deference is even more pronounced at the front end of the regulatory process. Between 1998 and 2008, federal agents submitted 5,870 intercept applications for approval.[123] The courts approved 5,866 of them.[124] That means that for the ten-year period, federal judges rejected only .07% of all government surveillance requests.

---

116. United States v. Renzi, 722 F. Supp. 2d 1100, 1107 (D. Ariz. 2010).

117. *Id.*

118. *Id.* at 1107–08.

119. *Id.* at 1118.

120. *See supra* note 101.

121. ADMIN. OFFICE OF THE U.S. COURTS, 2008 WIRETAP REPORT 35 tbl.8 (2009) [hereinafter 2008 WIRETAP REPORT].

122. *Id.* at 34.

123. *Id.* at 32 tbl.7. Because of the organization of data in the table, it was not possible to calculate this figure with absolute precision. However, the number of applications was no greater than 5,870 nor less than 5,866.

124. *Id.*; *see also* Dempsey, *supra* note 6, at 76 (noting that between 1989 and 1995, no judge, state or federal, denied a government request for electronic surveillance).

The problem with affording such deference to investigators is that it can encourage bad behavior. Absent a serious threat of judicial rebuke, careless agents have less incentive to be careful and unscrupulous agents have less incentive to behave ethically. And while there is no evidence that the agents in *Rivera* or *Szpyt* were behaving dishonestly or trying to deceive the courts, other agents might. The minimization requirement, in this respect, provides little protection against investigators willing to blatantly violate Title III and their own minimization memos.

C. Defining Minimization Down: The ECPA and Electronic Communications

Judicial deference is a problem for all minimization, both in the wire and electronic contexts. But electronic communications present additional problems and additional opportunities for investigatory mischief. As the case law shows, minimization was simply not designed for electronic communications such as text messages, and attempts to expand minimization into the electronic realm have produced odd, inconsistent, and generally unhelpful rules.

Although courts have never addressed text-message minimization directly,[125] they have addressed minimization in some similar settings, such as (1) pager intercepts[126] and (2) facsimile intercepts.[127] It is clear from these cases that courts, in reviewing electronic intercepts, require investigators to observe the *forms* of minimization while largely giving them a pass on the *substance*.

Minimization, as originally conceived, existed in the context of *aural* interceptions—of government agents *listening to* target conversations.[128] Over time, courts came to understand minimization as a temporal restriction, governing when and for how long investigators could listen to phone calls.[129] As a result, courts

125. The closest research has come to unearthing a text-message intercept case is *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010). The case did involve police officers monitoring text messages but is only somewhat on point because it involved the retrieval of text messages from electronic storage, rather than actual "interception." *Id.* at 2630.

126. Brown v. Waddell, 50 F.3d 285, 287 (4th Cir. 1995); United States v. David, 940 F.2d 722, 728–29 (1st Cir. 1991); United States v. Meriwether, 917 F.2d 955, 958 (6th Cir. 1990).

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

128. *See supra* notes 83–84 and accompanying text.

129. *See, e.g.*, Scott v. United States, 436 U.S. 128, 140 (1978) ("[A]gents can hardly be expected to know that . . . [very short calls] are not pertinent prior to their termination.").

developed the "two-minute rule,"[130] which allows agents to listen to all phone calls for at least two minutes to determine whether they are relevant to the investigation.[131] This rule is now widely recognized and in many districts is the starting point for any minimization analysis.[132] It is completely useless, however, in the context of electronic communications.[133] As a result, courts have been forced to expand their definitions of minimization, usually without a clear precedent to guide them. The results, as noted previously, have preserved certain formal elements of minimization, but have rarely, if ever, upheld its spirit.

So what types of minimization systems have courts developed? The short answer is relatively few. One promising analogy is to pager intercepts, since the technology, particularly on recent models, is not so different from text messaging.[134] Fifteen to twenty years ago, courts were largely unwilling to extend Title III protection to pager transmissions on the theory that they revealed only numbers, rather than substantive communications.[135] But as pagers became more advanced, judges recognized that the devices *could*, in fact, send substantive messages.[136] As a consequence, several circuits now

130. *See* United States v. Segura, 318 F. App'x 706, 712 (10th Cir. 2009) ("Segura contends that the government's two-minute instruction violates the minimization requirement. We disagree."); United States v. Yarbrough, 527 F.3d 1092, 1098 (10th Cir. 2008) ("[C]onsistent with Supreme Court and Tenth Circuit precedent, in analyzing the reasonableness of the government's minimization efforts, we exclude calls under two minutes.").

131. *Scott*, 436 U.S. at 140.

132. *See* United States v. Olmedo, 552 F. Supp. 2d 1347, 1367 (S.D. Fla. 2008) ("Although there is no bright-line rule as to how long an agent can listen to a call to determine whether it is pertinent, many courts have approved two-minute and three-minute cutoffs as a reasonable guide."); United States v. Borrayo-Gutierrez, 119 F. Supp. 2d 1168, 1184 (D. Colo. 2000) (finding proper minimization when the supervising agent told monitors that "they could listen for approximately two minutes and should disconnect at that point if the call did not appear to be relevant to the investigation"); United States v. Wright, 121 F. Supp. 2d 1344, 1348 (D. Kan. 2000) ("[S]hort calls lasting less than two minutes are generally not scrutinized for minimization.").

133. *See* Downes, *supra* note 20 ("Minimization as it has been understood up until now can have no meaning in an increasingly digital world.").

134. *See* Brown v. Waddell, 50 F.3d 285, 287–88 (4th Cir. 1995) (explaining how a criminal defendant used alphanumeric codes sent via pager to communicate with drug dealers).

135. United States v. Meriwether, 917 F.2d 955, 958 (6th Cir. 1990) ("[A] digital display pager, by its very nature, is nothing more than a contemporary receptacle for telephone numbers."); *see also* United States v. Benjamin, 72 F. Supp. 2d 161, 190 (W.D.N.Y. 1999) ("Paging devices, insofar as they reveal only numeric messages, but not the content of the communication, are similar to pen registers permitted under 18 U.S.C. § 3127(3).").

136. *Brown*, 50 F.3d at 287–88; *see also* United States v. Reyes, 922 F. Supp. 818, 837 n.20 (S.D.N.Y. 1996) ("[N]umerical codes may be transmitted to a pager that impart messages to the recipient.").

explicitly hold that Title III protects pager communications.[137] They have not, however, provided much guidance on *how* Title III protects them, particularly in the minimization context.[138]

One of the few courts to take up this question—albeit tangentially—was the First Circuit in *United States v. David*.[139] Although it was primarily a case about minimizing foreign-language conversations,[140] *David* also addressed pager intercepts and promulgated general rules about minimization in nontraditional contexts.[141] The court's basic command was that minimization—no matter what the process—must "protect the suspect's privacy interests to approximately the same extent as would *contemporaneous* minimization, properly conducted."[142] In the context of foreign-language phone calls, the court interpreted this command as allowing the government to *record* all of the conversations, and for translators to then minimize them after the fact, transcribing only pertinent portions for English-speaking agents.[143] Although the court only addressed this process in the context of foreign-language calls, it implicitly suggested that such procedures might apply more broadly, noting that "[w]here intercepted conversations are in a foreign language *or code* and, despite the exercise of reasonable diligence, a translator is not available for on-the-spot minimization, a different rule obtains."[144]

Given the confusion that still exists concerning substantive communications via pager, a better model may be facsimile interception.[145] Research has revealed only one case addressing minimization in that context, but that case addresses it at some length

137. *Brown*, 50 F.3d at 294; United States v. David, 940 F.2d 722, 728–29 (1st Cir. 1991).

138. Part of the problem is that courts have long recognized a minimization exemption for "coded" transmissions. *See* United States v. Williams, 109 F.3d 502, 507 (8th Cir. 1997) ("The remaining calls challenged by Williams were ambiguous in nature and included language the agents reasonably could have believed was coded language referring to possible cocaine transactions. More extensive wiretapping is reasonable when the conversations are in the jargon of the drug trade."). This exemption would presumably apply to all substantive, numeric pager messages.

139. *David*, 940 F.2d at 728–29.

140. *Id.* at 729–30.

141. *Id.* at 727, 729.

142. *Id.* at 730 (emphasis added).

143. *Id.*

144. *Id.* (emphasis added).

145. With faxes, unlike with electronic pages, there is usually a substantive message and therefore no real question that Title III and the minimization requirement apply.

and provides the most plausible model for how investigators would actually minimize text-message communications.[146]

The defendants in *United States v. McGuire* were members of the Montana Freemen, a radical militia devoted to setting up its own government and financial system.[147] McGuire and other militia members printed and distributed thousands of fake checks, using them as part of a scheme to over-pay debts and to cash the resulting refunds.[148] Although these crimes were "white collar" in nature, the FBI concluded that the group was well armed and capable of violence, and therefore decided to investigate them surreptitiously via surveillance of phone and fax communications.[149]

In authorizing FBI monitoring, the supervising judge provided a detailed statement on how the agents were to minimize fax interceptions.[150] One investigator would be designated "monitoring agent" and he, along with the Assistant U.S. Attorney ("AUSA"), would review every fax, in its entirety, to determine whether it was "pertinent to the criminal offenses listed in the court's order."[151] If so, then the fax would be shared with the rest of the agents. If not, it would be placed in a locked drawer until the interception order expired, at which point it would be turned over to the authorizing judge.[152] Although this procedure allowed one FBI agent and one AUSA to view many nonpertinent communications, it did ensure that "other people—government agents, lawyers, and others—did not read the non-pertinent documents at all."[153]

The defendants argued that these procedures were inadequate, as they did not truly "mimic those used for oral . . . interceptions."[154] As a counterfactual, they suggested that the monitoring agent "should have looked at each fax transmission with a ruler in hand, reading [it] line by line."[155] Once it became apparent that the fax was

146. *See* United States v. McGuire, 307 F.3d 1192, 1200 (9th Cir. 2002) (explaining how investigators actually minimize fax transmissions).

147. *Id.* at 1195. For background information on the militia and its various criminal enterprises, see Tom Kenworthy & Serge F. Kovaleski, *'Freemen' Finally Taxed the Patience of Federal Government*, WASH. POST, Mar. 31, 1996, at A1.

148. *McGuire*, 307 F.3d at 1195.

149. *Id.*

150. *Id.* at 1200.

151. *Id.*

152. *Id.*

153. *Id.* at 1201.

154. *Id.* at 1202.

155. *Id.*

nonpertinent, the monitoring agent "should have skipped about thirty lines and then continued," line-by-line, as before.[156]

Faced with these two alternatives, the Ninth Circuit endorsed the government's approach.[157] Echoing *Scott*, it emphasized that minimization must be analyzed in light of the particular circumstances, and that courts must strike a balance between reducing "to a practical minimum the interception of conversations unrelated to the criminal . . . investigation" and "permitting the government to pursue legitimate investigations."[158] But did *McGuire* really get that balance right?

While it would certainly be inconvenient for an FBI agent, ruler in hand, to read every fax transmission line-by-line, the Ninth Circuit seems nonetheless to have misunderstood the true purpose of the minimization requirement. Commentators from Justice Brennan to the Senate Judiciary Committee have noted that the impetus behind minimization was privacy protection, *not* due process protection.[159] In light of that fact, the Ninth Circuit did not—and probably could not—explain why it would be meaningfully better for a person to have one or two government agents monitoring his private communications than it would be to have a team of half a dozen doing the same. The *McGuire* Court claimed that it sought to reduce the interception of nonpertinent communications to a "practical minimum."[160] But if its findings are indicative of how other courts approach electronic intercepts, then a "practical minimum" will prove to be no real minimum at all.

Not surprisingly, the Supreme Court favors this "in light of the circumstances" approach to electronic communications. While the Court has never taken an ECPA minimization case, it has recently addressed the broad issue of text-message privacy in *City of Ontario v. Quon*. There, a police department obtained transcripts of a SWAT

156. *Id.*

157. *Id.* ("We interpret Congress' 'common sense' idea of electronic minimization to mean that law enforcement in some circumstances may look at every communication.").

158. *Id.* at 1199–1200.

159. Scott v. United States, 436 U.S. 128, 143–44 (1978) (Brennan, J., dissenting) (noting that the minimization requirement is a congressionally established safeguard "designed to prevent Government electronic surveillance from becoming the abhorred general warrant which historically had destroyed the cherished expectation of privacy in the home"); S. REP. NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 ("The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance.").

160. *McGuire*, 307 F.3d at 1199–1200.

sergeant's text messages to determine whether he had been improperly using his office-issued pager.[161] An audit uncovered a number of sexually explicit messages, leading the department to launch a formal investigation into Quon's behavior.[162] Quon, in turn, sued the department under the Secured Communications Act and the Fourth Amendment for obtaining and reviewing his personal communications.[163]

Writing for the Court, Justice Kennedy assumed without deciding that Quon had a reasonable expectation of privacy in these text messages.[164] He further concluded, however, that the department's review was reasonable in both purpose and scope[165] and did not wrongfully intrude on Quon's privacy rights. This ruling is notable because the Ontario Police Department reviewed communications in much the same way as the FBI had in *McGuire*. One officer read *all* of the transcripts, redacted irrelevant information, and then passed the remaining records on to additional reviewers.[166] The Court ultimately found this approach to be reasonable because "it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use."[167]

While it is important to emphasize that *Quon*, unlike *McGuire*, dealt with an employee's privacy rights vis-à-vis his employer and was not at all concerned with minimization, the factual similarities are still striking. Based on this decision, together with the Court's deferential holding in *Scott*, it seems reasonable to conclude that the Court will endorse the Ninth Circuit's approach in *McGuire* if it ever takes a text-message minimization case.

D. When Even a Quantum of Protection Is Too Much: Investigatory Alternatives to Interception and Minimization

Having established that minimization provides no substantive protection to text message privacy, the question remains whether it

---

161. City of Ontario v. Quon, 130 S. Ct. 2619, 2626 (2010).

162. *Id.*

163. *Id.*

164. *Id.* at 2630 ("For present purposes we assume several propositions *arguendo:* First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City.").

165. *Id.*

166. *Id.* at 2626.

167. *Id.* at 2631.

provides any procedural protection. If government agents must observe the formalities of minimization then their desire to avoid procedural hassles might discourage them, at least at the margins, from intercepting text messages in the first place. Might that discouragement serve as a valuable privacy protection in its own right?

The answer, unfortunately, is a resounding no. If government agents want to avoid the hassles of minimization, trivial as they may be, then those agents can typically do so with ease. There are many ways for agents to obtain the contents of text messages without intercepting them, and without interception Title III does not apply at all.[168] In this respect, a critical failure of the minimization requirement is that law enforcement can sidestep it so easily.

One of the ways for government agents to get around the minimization requirement is by pulling text messages from electronic storage rather than intercepting them directly.[169] Federal courts analyzing this technique have held that Title III does not apply,[170] making it an attractive option for sidestepping the procedural restrictions of electronic surveillance. Agents would still need to obtain a warrant before demanding such records, but they would only have to meet the normal warrant requirements of the Federal Rules of Criminal Procedure, not the heightened requirements of Title III.[171] At least one circuit has explicitly stated that stored communications are entitled to less protection than intercepted communications.[172]

A second technique available to government agents is to search the memory of a cell phone as part of a search incident to arrest.[173] In a controversial 2007 decision, the Fifth Circuit ruled in *United States*

168. 18 U.S.C. § 2518(5) (2006) (stating that law enforcement must "minimize the *interception* of communications not otherwise subject to *interception* under this chapter") (emphasis added).

169. *See, e.g.*, *Quon*, 130 S. Ct. at 2626 (describing how investigators at a California police department contacted a wireless service provider to gain access to the contents of the text messages sent or received from one of the city-owned pagers).

170. *See* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (holding that the Wiretap Act covers only "real-time interception of electronic communication"); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) ("Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'").

171. Stored Communications Act of 1986 § 201, 18 U.S.C. § 2703(a) (2006).

172. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002) ("The level of protection provided stored communications under the [Stored Communications Act] is considerably less than that provided communications covered by the Wiretap Act.").

173. *See, e.g.*, United States v. Finley, 477 F.3d 250, 254–55 (5th Cir. 2007) (describing the warrantless seizure and search of a cell phone after suspect was arrested for methamphetamine possession).

v. Finley that cell phones are analogous to "containers"[174] and that police can therefore search them without separate warrants after arresting the owner.[175] In practice, that means that government agents can read the text messages of any arrestee without performing minimization, and can even arrest suspects *for the specific purpose* of obtaining their text messages.[176] Of course, the value of this technique may be limited, as it applies only when there has been a valid arrest,[177] and only reveals the contents of messages physically saved on the cell phone. However, to the extent law enforcement can find a pretext to arrest their desired subject, the search-incident doctrine can be a highly effective way to circumvent minimization.[178]

Finally, and perhaps most significantly, the minimization requirement provides no real protection to subjects of surveillance unless the government files charges against them.[179] In *United States v. Dorfman*, for example, the Seventh Circuit emphasized that the Fourth Amendment's exclusionary rule "does not extend to a person against whom no evidence is offered," and that nonparties therefore have no standing to challenge the admission into evidence of improperly minimized conversations.[180] This loophole makes it easy—at least in certain circumstances—for law enforcement to get around

174. *See* New York v. Belton, 453 U.S. 454, 460–61 (1981) (holding that police have authority to search containers—whether open or closed—that are within suspect's reach at the time he is arrested).

175. *Finley*, 477 F.3d at 260.

176. Police would still need probable cause before they could make an arrest. They could, however, arrest a suspect on the pretext of some minor felony in order to gain access to his cell phone during the search incident to arrest. *See* Whren v. United States, 517 U.S. 806, 813 (1996) (noting that the constitutional "reasonableness" of an arrest does not depend on the "actual motivations of the individual officers involved").

177. *Finley*, 477 F.3d at 259–60 (emphasizing that the search of suspect's text messages was valid because it was part of a search incident to arrest).

178. Another limitation is the fact that the *Finley* approach to text-message searches remains controversial and has been explicitly rejected in several jurisdictions. *See* United States v. Wall, No. 08–60016–CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) ("The Court declines to adopt the reasoning of *Finley* and extend law to provide an exception to the warrant requirement for searches of cell phones."); United States v. Park, No. CR 05–375 SI., 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) (distinguishing pagers from cell phones and finding that the contents of the latter are protected by the Fourth Amendment); State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009) ("We hold that the warrantless search of data within a cell phone seized incident to valid arrest is prohibited by the Fourth Amendment when the search is unnecessary for the safety of law-enforcement officers and there are no exigent circumstances.").

179. United States v. Dorfman, 690 F.2d 1217, 1220–21 (7th Cir. 1982).

180. *Id.*

the minimization requirement. All they have to do is intercept the communications of a non-suspect third party.[181]

Based on the availability of these three techniques, government agents can sidestep even the hollowed-out minimization requirements for electronic interceptions if and when they determine those requirements to be too much of a nuisance.

IV. GLIMMERS OF TRUE PROTECTION: WHY THE "TRADITIONAL" MINIMIZATION REQUIREMENT AFFORDS MORE PRIVACY PROTECTION THAN THE ECPA VERSION

Minimization has failed as a form of privacy protection; the question is, how badly? Has it failed only in the context of electronic intercepts, or is "traditional" minimization every bit as flawed? The question might seem academic, but it is, in fact, critical to the broader analysis. Fixing a problem, after all, requires some understanding of what is broken. Is it electronic minimization, or minimization generally?

Critics of the current system argue that minimization as a whole has simply fallen short.[182] Case law seems to support this claim, as exceptions to minimization have grown so large and so numerous that they have arguably swallowed up the rule. Courts have held, for example, that government agents possess broader intercept powers while investigating "a wide-ranging conspiracy with large numbers of participants."[183] They have similarly ruled that agents may lawfully listen in on private calls during the early stages of an investigation,[184] and when the calls are in coded or ambiguous language.[185] And, of course, these specific exceptions fall on top of the deferential holding

181. As an example, if the police were seeking to obtain evidence to use against a suspected drug dealer, they could obtain a surveillance warrant for his mother or girlfriend rather than the suspect himself. If the police then violated the minimization requirement, no one would have standing to suppress the improperly minimized messages.

Admittedly, Title III also establishes a civil remedy for victims of improper minimization. 18 U.S.C. § 2520 (2006). However, this section fully exempts federal agents and contains a broad "good faith" exception for state law enforcement. *Id.* §§ 2510(5)(a)(ii), 2520(a). In practice, this means that civil recovery is almost never possible. For a detailed analysis of the law enforcement exception, see Amati v. City of Woodstock, 176 F.3d 952, 955–56 (7th Cir. 1999).

182. *See* Dempsey, *supra* note 6, at 77 ("[T]he lower courts have read [the *Scott* decision] as effectively eliminating the requirement to minimize the recording of innocent conversations.").

183. United States v. Bennett, 219 F.3d 1117, 1124 (9th Cir. 2000).

184. United States v. Willis, 890 F.2d 1099, 1102 (10th Cir. 1989).

185. United States v. Williams, 109 F.3d 502, 507 (8th Cir. 1997).

from *Scott,* which requires only that minimization efforts be objectively "reasonable."[186]

Despite these loopholes and exceptions, traditional minimization still provides real privacy protection, at least in some circumstances.[187] Compared to electronic minimization, which courts have thoroughly gutted, wiretap minimization continues to affect the way in which law enforcement conducts surveillance. Its continued, if partial, vitality can be attributed to three underlying factors. First, the statute governing traditional minimization makes it easier for victims to seek redress. Second, courts have been more willing to grant motions to suppress in the wiretap context. Third, and perhaps most importantly, law enforcement agencies have internalized wiretap minimization standards in a way they simply have not done for ECPA minimization standards.

A. The Stronger the Statute, the Stronger the Protection

Although electronic and wiretap minimization are both governed by Title III, there are small but significant differences in the protections they provide.[188] The most important of these differences is that the original Title III established suppression as a remedy for inadequate minimization,[189] while the ECPA refused to extend the same protection to electronic communications.[190] The Fourth Amendment, of course, may provide its own suppression remedy, independent of any statute.[191] As a result, failure to minimize

186. Scott v. United States, 436 U.S. 128, 138–39 (1978).

187. Courts have traditionally been most concerned about privacy in the contexts of attorney-client and marital communications. *See, e.g.*, United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987) (suppressing twenty-two calls between an attorney and client and holding that the government failed to minimize); United States v. Mancari, 663 F. Supp. 1343, 1359 (N.D. Ill. 1987) ("[T]he court is concerned that interception between [the defendant] and his wife appears to have continued beyond the period of the first authorization order despite the government's failure to list her in the extension application.").

188. *See supra* notes 92–99 and accompanying text.

189. 18 U.S.C. § 2515 (2006) ("Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court . . . .").

190. ECPA of 1986 § 101(e), 18 U.S.C. § 2518(10)(c) (stating that civil damages and sanctions are "the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications").

191. *See* Mapp v. Ohio, 367 U.S. 643, 656 (1961) (holding the exclusion doctrine to be "constitutionally necessary"). Subsequent Supreme Court decisions have called the constitutional status of the exclusionary rule into question. *See generally* INS. v. Lopez-Mendoza, 468 U.S. 1032 (1984) (holding that the "exclusionary rule would not apply in civil deportation hearing to require

electronic communications may still be grounds for suppression.[192] The Senate recognized this possibility, noting in its report on the ECPA that "[i]n the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing [c]onstitutional law with respect to the exclusionary rule."[193] The reality, however, is that no court has ever construed a particular failure to minimize as a constitutional violation.[194] Assuming this trend continues, the ECPA minimization requirement contains no true enforcement mechanism. In contrast, the original Title III requirement continues to protect the contents of phone calls through its statutory suppression remedy.

B. Judges Do Sometimes Grant Motions to Suppress in the Traditional Wiretap Context

It is all well and good that Title III contains a suppression remedy, but questions remain as to how much protection that remedy provides. Critics of the current minimization system argue that the protection is illusory, as judges rarely, if ever, find government minimization efforts unreasonable.[195] And without a finding of violation, questions of remedy are simply irrelevant.

The fact remains, however, that courts have found minimization violations and have suppressed conversations as a result. In *United States v. Hoffman*, for example, the First Circuit suppressed twenty-two phone calls between a defendant and her attorney, noting that "the agents should have stopped listening to

---

that admission of illegal entry by alien after allegedly unlawful arrest be excluded from evidence."); United States v. Calandra, 414 U.S. 338 (1974) (refusing to extend the exclusionary rule to grand jury proceedings). To date, the Court has not definitively resolved this issue.

192. Professor Goldsmith, for example, has argued that the minimization requirement is itself constitutional, rather than statutory, in origin and that a failure to minimize should therefore be treated in the same basic way as any other due process violation—which in most circumstances means exclusion of unlawfully obtained evidence. Goldsmith, *supra* note 72, at 98.

193. S. REP. NO. 99–541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

194. Professor Freiwald investigated this issue in the particular context of e-mail interceptions, noting that a few cases "suggest in dicta that the Fourth Amendment protects the contents of e-mail, but none has granted a suppression remedy to a victim of an unauthorized e-mail interception." Freiwald, *supra* note 53, at 53. Admittedly, e-mail intercepts may not raise the exact same issues as text-message intercepts. *See supra* note 107 and accompanying text. Research, however, has not revealed any examples of courts extending any greater constitutional protection to the contents of text messages.

195. *See* Dempsey, *supra* note 6, at 77 ("Defendants' after-the-fact challenges to the authorization or conduct of surveillance are rarely sustained. Between 1985 and 1994, judges nationwide granted 138 suppression motions while denying 3,060, for a 4.3% suppression rate.").

each call as soon as the parties were identified."[196] More recently, in *United States v. Simels*, the Eastern District of New York suppressed all of the conversations obtained during a wiretap, as agents in that case had recorded conversations without contemporaneously minimizing them.[197] The government argued it had not violated the statute, as only one agent had listened to the unedited tapes. But the court flatly rejected that argument.[198] Delivering an unusually strong rebuke, it declared, "When the government deliberately intercepts nonpertinent communications, it is no comfort to those whose privacy has been invaded that only government actors not involved in a particular criminal investigation will be listening to them."[199] The *Simels* decision, in turn, influenced the District of Arizona's reasoning in *United States v. Renzi*, which excluded all of the government's wiretap evidence because of a failure to minimize properly.[200]

A few courts have even reprimanded government agents for failing to make a prima facie showing that their minimization was "reasonable."[201] For example, in *United States v. Mancari* the Northern District of Illinois rejected the government's claim that submission of status reports to a judge was sufficient proof of reasonableness.[202] In particular, the court emphasized its concern that agents may have violated their own minimization guidelines and that the status reports failed to address that concern.[203] As noted above, skeptical judicial review of minimization is more likely the exception than the rule. Occasional scrutiny, however, is better than consistent and predictable laxity.

Taken together, these cases demonstrate that the minimization requirement still has teeth in the wiretap context. Though it is difficult to determine how often suppression takes place,[204] judicial rebukes—even infrequent ones—may help deter law-enforcement misconduct. At the very least, they establish that government agents

196. United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987).

197. United States v. Simels, No. 08–CR–640 (JG), 2009 WL 1924746, at *15 (E.D.N.Y. July 2, 2009).

198. *Id.* at *11.

199. *Id.*

200. United States v. Renzi, 722 F. Supp. 2d 1100, 1128 (D. Ariz. 2010) (citing *Simels* for the proposition that agents do not properly minimize calls by recording all communications and then sorting them out later).

201. United States v. Mancari, 663 F. Supp. 1343, 1359 (N.D. Ill. 1987).

202. *Id.*

203. *Id.*

204. The yearly Wiretap Reports are of little help in answering this question, as they do not distinguish between different types of suppression motions.

cannot flaunt Title III with impunity. In contrast, the ECPA minimization requirement fails to provide even that basic level of protection.

C. Law Enforcement Agencies Have Partially Internalized the Traditional Minimization Requirement

Law enforcement agencies have been living with Title III for more than four decades and have largely accepted its underlying restrictions. They have adapted to the statute through training and internal policymaking, and have at times placed tighter restrictions on themselves than the statutory language places on them. In *United States v. Rivera*, for example, a DEA taskforce developed detailed internal regulations to help guide agents in their surveillance.[205] The regulations required that new monitors be paired with experienced monitors to ensure that they minimized properly, and that scheduled surveillance shifts overlap, so that outgoing monitors could share information on intercepted calls with the incoming monitors.[206] In light of the *Scott* decision, where the Supreme Court upheld as "reasonable" a wiretap in which the agents performed no minimization at all,[207] it does not appear that any of these policies were required by law.[208]

Similarly, in *United States v. David*, the DEA demonstrated how its agents had gone beyond their legal obligations in minimizing foreign-language communications.[209] The agents in that case had been monitoring Hebrew-language phone calls as part of an investigation into international drug smuggling.[210] Because the task force did not include, and could not immediately locate, any Hebrew-speaking agents, they recorded the conversations and then turned the tapes over to translators.[211] Critically, however, the DEA required the translators to treat the tapes like live communications and immediately stop listening once it became clear that a conversation

205. United States v. Rivera, 527 F.3d 891, 904 (9th Cir. 2008).

206. *Id.* at 905.

207. Scott v. United States, 436 U.S. 128, 130–31 (1978).

208. For a comparable example of a federal agency applying stringent internal minimization policies, see *United States v. Haque*, 315 F. App'x 510, 519 (6th Cir. 2009) (describing an FBI wiretap memo that required all monitoring agents to attend initial training, and for two senior agents to oversee the monitoring at all times).

209. United States v. David, 940 F.2d 722, 730 (1st Cir. 1991).

210. *Id.*

211. *Id.*

was beyond the scope of the investigation.[212] As a result, *no one* on the task force listened to the nonpertinent communications.

Evidence strongly suggests that the First Circuit in *David* would have approved a much lower level of minimization. In its analysis, the court approvingly cited *United States v. Gambino*, a case from the Southern District of New York involving similar facts.[213] In *Gambino*, however, the FBI conducted minimization differently, allowing Sicilian-speaking agents to listen to all recorded conversations and then to transcribe and pass along only those pertinent to the investigation.[214] Unlike the agents in *David*, the FBI allowed certain investigators to listen in on all of the private, nonpertinent conversations.[215] If the DEA had wanted to, it could probably have gotten away with a similar minimization scheme. But, because of the task force's internal policies, the agents protected the privacy of their surveillance target more than either the statute or court required.

The underlying point here is not that government agents are always concerned with the privacy rights of their surveillance targets. If anything, exceptions to minimization for which agencies have fought—and usually won—over the years establish just the opposite.[216] But what these cases show is that government agents have internalized certain basic requirements of minimization. For all of the exceptions that exist at the periphery, agents have largely accepted that there is a core of private, nonpertinent conversation that law enforcement simply may not access. In contrast, government agents do not appear to view electronic communications as warranting any true privacy protection.[217]

The differences between traditional and ECPA minimization show the latter to be truly broken, while the former is flawed but functional. The evidence shows that the current wiretap framework

---

212. *Id.*

213. *Id.* (citing United States v. Gambino, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990)).

214. *Gambino*, 734 F. Supp. at 1106.

215. As noted earlier, permitting a single monitoring agent—rather than multiple monitoring agents—to access an individual's private communications is, at best, a flimsy form of privacy protection. *See supra* notes 152–55 and accompanying text.

216. *See supra* notes 170–74 and accompanying text.

217. *See, e.g.*, United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (accepting government argument that there is no right to privacy in e-mails). Admittedly, the FBI demonstrated some limited interest in individual privacy rights in *United States v. McGuire*, 307 F.3d 1192, 1199–1200 (9th Cir. 2002). But, even in that case, the FBI permitted one of its agents—along with the assistant U.S. Attorney—to read through nonminimized fax transmissions in their entirety. *Id.* at 1200.

successfully protects some level of personal privacy, and therefore should not be discarded.[218] The ECPA minimization requirement, on the other hand, is worthless, providing no true privacy protection for electronic communications.

The question, then, is how do we fix it? Or, at a more basic level, is it even worth fixing?

V. A TEMPEST IN A TEXT MESSAGE: SHOULD WE CARE THAT MINIMIZATION DOES NOT PROTECT ELECTRONIC COMMUNICATIONS AND, IF SO, WHAT SHOULD WE DO ABOUT IT?

Minimization fails when applied—or not applied, as the case may be—to electronic communications. But why should that fact concern us? Why does minimization even matter, particularly if it requires us to limit the power of police to investigate major crimes?

Scholars and jurists have debated this question for more than eighty years, with some pushing for privacy purity and others arguing for a more pragmatic approach.[219] After careful analysis, it is clear that the pragmatists have the better argument.[220] Minimization arose from the world of telephone wiretaps, and attempts to extend it have proven useless at best, counterproductive at worst. Rather than struggle to modify minimization in some vain attempt to keep up with technology, we should simply concede that the experiment has failed and should end it.

---

218. I am sympathetic in particular to the argument that judges should put more weight on the percentage of calls improperly intercepted, and should suppress *all* conversations in cases where the government brazenly disregards the minimization requirement. *See, e.g.*, Ronni L. Mann, Note, *Minimization of Wire Interception: Presearch Guidelines and Postsearch Remedies*, 26 STAN. L. REV. 1411, 1437–38 (1974) (arguing that courts should suppress all conversations when the government's violation of the minimization requirement is "substantial").

219. *Compare* Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) (suggesting that allowing for electronic surveillance is like "placing a policeman in every home or office where it was shown that there was probable cause to believe that evidence of a crime would be obtained"), *with id.* at 72 (Black., J., dissenting) (focusing on the fact that "[c]riminals are shrewd and constantly seek, too often successfully, to conceal their tracks and their outlawry from law officers").

220. As explained in Part III, this Note does not advocate the wholesale abandonment of the minimization requirement, as it continues to provide useful—if limited—privacy protection in the context of wire surveillance.

A. The Purist Approach

Privacy purists believe that people have a basic right to be "let alone."[221] In 1928, in his famous *Olmstead* dissent, Justice Brandeis turned this belief into a personal *cri-de-coeur*, arguing that the Founders recognized "the significance of man's spiritual nature, of his feelings and of his intellect" and that they intended "to protect Americans in their beliefs, their thoughts, their emotions and their sensations."[222] In erecting this intellectual redoubt, which Justices Frankfurter, Douglas, and Brennan would later defend,[223] Brandeis emphasized that privacy is more than just a due process concern. While he and other purists recognized the due process implications of unrestrained government surveillance,[224] their concern was a deeper one.[225] As purists saw the world, individual freedom was impossible without a private sphere free from state oversight and intervention.[226] And as new technologies threatened to knock down those sanctum walls, purists saw an immediate need for courts to step in with supplemental legal protection.

Another defining feature of the purists is their general disinterest in the needs of law enforcement.[227] To the purist, privacy is a fundamental right, not something to balance against the ebb and

---

221. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

222. *Id.*

223. *See Berger*, 388 U.S. at 64 (Douglas, J., concurring) ("A discreet selective wiretap or electronic 'bugging' is of course not rummaging around, collecting everything in a particular time and space zone. But even though it is limited in time, it is the greatest of all invasions of privacy."); Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting) ("Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny."); On Lee v. United States, 343 U.S. 747, 758 (1952) (Frankfurter, J., dissenting) ("Loose talk about war against crime too easily infuses the administration of justice with the psychology and morals of war.").

224. *See, e.g.*, *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting) ("Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.").

225. *See Berger*, 388 U.S. at 66 (Douglas, J., concurring) ("Whether or not the evidence obtained is used at a trial for another crime, the privacy of the individual has been infringed by the interception of all of his conversation."); *Olmstead*, 277 U.S. at 479 (Brandeis, J., dissenting) ("The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.").

226. *See, e.g.*, *Lopez*, 373 U.S. at 452 (Brennan, J., dissenting) ("In a free society, people ought not to have to watch their every word so carefully.").

227. *See On Lee*, 343 U.S. at 758 (Frankfurter, J., dissenting) ("Of course criminal prosecution is more than a game. But in any event it should not be deemed to be a dirty game in which 'the dirty business' of criminals is outwitted by 'the dirty business' of law officers."); *Olmstead*, 277 U.S. at 479 (Brandeis, J., dissenting) ("And it is also immaterial that the intrusion was in aid of law enforcement.").

flow of governmental demands.[228] Those demands, after all, just grow larger and larger with time, leading to a steady erosion of personal privacy.[229] In his *Olmstead* dissent, Justice Brandeis suggested that well-intentioned privacy violations could actually threaten liberty more than malicious ones,[230] as individuals can spot and resist encroachments from "evil-minded rulers," but are highly vulnerable to "insidious encroachment[s]" in the name of the common good.[231] The public does not really care about the privacy rights of mobsters and drug-dealers. But once the public acquiesces to one privacy violation, it becomes easier for the government to engage in others.[232] For the purists, this long-term risk is simply unacceptable.

So what does this all mean in the context of electronic minimization? For purists like Brandeis and Brennan, the answer is simple. Text messages and e-mail exist within the same sphere of privacy as phone calls and should remain beyond the reach of law enforcement.[233] The minimization requirement, in other words, should expand to exempt *all* private electronic communications from surveillance.

Of course, in light of *Scott*'s reasonableness requirement, such dramatic change is unlikely. Modern scholars, however, have suggested several purist alternatives that would strengthen minimization without prohibiting electronic intercepts.[234] Professor

228. *See, e.g.*, Warden v. Hayden, 387 U.S. 294, 325 (1967) (Douglas, J., dissenting) ("That there is a zone that no police can enter—whether in 'hot pursuit' or armed with a meticulously proper warrant—has been emphasized by *Boyd* and by *Gouled*.").

229. *Cf. Lopez*, 373 U.S. at 466 (Brennan, J., dissenting) ("[T]he fact that the police traditionally engage in some rather disreputable practices of law enforcement is no argument for their extension.").

230. *Olmstead*, 277 U.S. at 479 (Brandeis, J., dissenting).

231. *Id.*

232. This phenomenon calls to mind the saying—often attributed to H.L. Mencken—that "the trouble with fighting for human freedom is that one spends most of one's time defending scoundrels. For it is against scoundrels that oppressive laws are first aimed, and oppression must be stopped at the beginning if it is to be stopped at all."

233. Of course, the main purist justices—Brandeis, Frankfurter, Brennan, and Douglas—were active prior to the modern tech boom, so any conclusions about their views on e-mail or text message privacy involves a degree of speculation. However, given their absolutist position against wiretaps, it is not too much of a leap to think that they would favor similar protections for these newer forms of communication. The arguments against wiretapping apply with equal force against electronic intercepts, particularly because an electronic intercept also "intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations." Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring).

234. As a practical matter, many of these minimization "fixes" could apply to both wiretaps and electronic intercepts. This is consistent with the purist view that phone calls, as well as e-mails and text-messages, should receive greater privacy protection than they currently do. *See,*

James Dempsey, for example, has proposed a technological solution, noting that it may become "relatively easy for the service provider to perform the minimization."[235] Courts could then require such minimization as part of their reasonableness analysis under *Scott*. Ronni Mann, in turn, has suggested that courts suppress all intercepted communications in cases where law enforcement inadequately minimizes more than some set percentage of messages.[236] And—though no purist has actually proposed this approach—courts could force the government to adopt the appellee's position in *United States v. McGuire*, printing out messages and performing minimization on a line-by-line basis.[237]

B. The Pragmatist Approach

If purists tremble at the prospect of the too-strong state, pragmatists fear the opposite: a state unable to defend its citizens. In 1967, for example, the Johnson Administration released its landmark report, THE CHALLENGE OF CRIME IN A FREE SOCIETY. Striking a pessimistic tone, the Presidential Commission conceded that "[s]ome have become distrustful of the Government's ability, or even desire, to protect them."[238] Turning specifically to the problem of organized crime, the Commission stated bluntly that attempts to control it "have not been successful."[239] These findings proved influential in Congress, leading legislators to agree that wiretapping had become "indispensable" for combating certain crimes.[240]

Justice Black voiced similar concerns in his *Berger* dissent. He noted that "this country is painfully realizing that evidence of crime is difficult for governments to secure. Criminals are shrewd and constantly seek, too often successfully, to conceal their tracks and their outlawry from law officers."[241] Even the Senate, which had

---

e.g., Goldsmith, *supra* note 72, at 106–07 (criticizing the *Scott* Court for failing to "rectify the consequences of its prior neglect").

235. Dempsey, *supra* note 6, at 87.

236. *See* Mann, *supra* note 218, at 1438 ("If, in the court's opinion, substantial compliance has not occurred, [then] the proper remedy is suppression of the entire wiretap.").

237. 307 F.3d 1192, 1202 (9th Cir. 2002).

238. PRESIDENT'S COMM'N ON LAW ENFORCEMENT & ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 1 (1967) [hereinafter CHALLENGE OF CRIME], *available at* http://www.ncjrs.gov/pdffiles1/nij/42.pdf.

239. *Id.* at 198.

240. S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2161 ("[A]uthorized wiretapping and electronic surveillance techniques by law enforcement officials are indispensable legal tools.").

241. Berger v. New York, 388 U.S. 41, 72 (1967) (Black, J., dissenting).

traditionally been more privacy-conscious than the Court, emphasized the country's growing crime problem in its report on Title III.[242] In particular, it noted that traditional police techniques had proven "notably unsuccessful" in combating the rise of criminal cartels.[243] Pragmatists, in this respect, view the purist position as well intentioned but misguided.[244] Government agents may violate one's privacy, but they are "assuredly not engaged in a more 'ignoble' or 'dirty business' than are bribers, thieves, burglars, robbers, rapists, kidnappers, and murderers."[245]

The crux of this pragmatist argument is that government endangers society's interests by providing *too much* privacy protection, rather than too little. Justice Rehnquist made this point in *Scott*, emphasizing that the public is ill served by "inflexible" restrictions on law enforcement.[246] Police, he reasoned, must have the freedom to adapt to changing circumstances, even when the consequence is more extensive surveillance.[247] Lower courts have largely embraced this understanding. For example, in 1971, seven years before the *Scott* decision, the Southern District of California declared that "the imposition of a rigid set of rules might in diverse situations serve to thwart the very purposes of the [minimization] statute."[248] In *United States v. Yarbrough*, the Court of Appeals for the Tenth Circuit similarly concluded that "[i]n light of the extensive nature of the criminal investigation . . . agents were entitled to more leeway in monitoring calls."[249] Pragmatists therefore reject the idea of bright-line privacy rules. When benefits are slight and costs to law enforcement are high, privacy protection must give way to the needs of law and order.[250]

---

242. S. REP NO. 90–1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2157–58.

243. *Id.* at 2157.

244. *Cf.* Leon Jaworski et al., *Additional Views of Individual Commission Members*, *in* CHALLENGE OF CRIME, *supra* note 238, at 678–79 ("We are passing through a phase in our history of understandable, yet unprecedented, concern with the rights of accused persons. . . . But the time has come for a like concern for the rights of citizens to be free from criminal molestation of their persons and property.").

245. *Berger*, 388 U.S. at 72–73 (Black, J., dissenting).

246. Scott v. United States, 436 U.S. 128, 139 (1978).

247. *Id.* at 140 ("In determining whether the agents properly minimized, it is also important to consider the circumstances of the wiretap.").

248. United States v. King, 335 F. Supp. 523, 538 (S.D. Cal. 1971), *aff'd in part, rev'd in part*, 478 F.2d 494 (9th Cir. 1973).

249. 527 F.3d 1092, 1098 (10th Cir. 2008).

250. *See, e.g.*, *Berger*, 388 U.S. at 72–73 (Black, J., dissenting) (noting that in dealing with criminals "eavesdroppers are not merely useful, they are frequently a necessity"); *see also* Jaworski et al., *supra* note 244, at 307 ("In many respects, the victims of crime have been the

Under this framework, statutory checks on police power are justifiable only when the clear, quantifiable benefit outweighs the loss in investigatory effectiveness; small or symbolic privacy protections are downplayed or discounted. Courts taking this approach have routinely held that minor failures to minimize are not true violations at all.[251] In *McGuire*, the Ninth Circuit concluded that the incremental privacy benefit of preventing all FBI agents from reading nonpertinent faxes—rather than allowing one agent to read them—did not justify burdening the investigators.[252] While pragmatists have not always come down on the side of law enforcement,[253] they have shown that they will generally defer to police interests unless substantial privacy rights are involved.

Given the utter failure of the ECPA minimization requirement, pragmatists favor discarding it. On the one hand, it provides no meaningful privacy protection,[254] while on the other hand, it burdens law enforcement.

C. Resolution: A Grudging Concession to Pragmatism

So who has the better of the arguments: purists or pragmatists? Purists certainly win the battle of words, framing the privacy debate as a twilight struggle between the forces of liberty and unwitting harbingers of tyranny.[255] But rhetoric is no substitute for evidence, and in the narrow context of electronic minimization, evidence is on the pragmatists' side. Though purists are right to worry

---

forgotten men of our society—inadequately protected, generally uncompensated, and the object of relatively little attention by the public at large.").

251. *See* United States v. Bennett, 219 F.3d 1117, 1124 (9th Cir. 2000) ("Even assuming the government improperly intercepted all 267 [of 7322] calls as the appellants assert, this was only 3.65% of the total number of calls intercepted. Such a percentage alone is not fatal."); United States v. Willis, 890 F.2d 1099, 1102 (10th Cir. 1989) (calculating that the police had minimized only seventy percent of nonpertinent calls, but concluding that there was "nothing which indicates that these statistics are anything short of reasonable").

252. United States v. McGuire, 307 F.3d 1192, 1199 (9th Cir. 2002) ("Minimization requires that the government adopt reasonable measures to reduce to a *practical* minimum the interception of conversations unrelated to the criminal activity under investigation while permitting the government to pursue legitimate investigation.") (emphasis added).

253. *Berger*, 388 U.S. at 63 (noting the government's claimed interest in crime prevention, but nonetheless concluding that "it is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded").

254. *See supra* Part II.

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

about government invasions of personal privacy, their arguments vis-à-vis minimization (1) overstate the slippery slope effect; (2) fail to situate electronic intercepts within the broader universe of police investigation; and (3) overlook the possibility that rules governing electronic minimization could actually undermine wiretap minimization. Congress should therefore amend Title III to abolish the electronic minimization requirement, recognizing that a flawed protection is sometimes worse than no protection at all.

1. Numbers Matter

From the dissenting opinions of purist justices, it is clear that the bogeyman haunting their dreams was the all-seeing government agent.[256] More than eighty years after Brandeis's *Olmstead* dissent, those omniscient agents have still not appeared. We know, for instance, that law enforcement performs very few electronic intercepts under Title III—no more than thirty-six in 2009 and forty-three in 2008.[257] The number of traditional wiretaps, though larger, is still relatively modest—1,720 for 2009 and 1,757 for 2008.[258] With a national population during those years of roughly 307,000,000,[259] that means that in 2009, government agents conducted Title III wire surveillance against roughly one American in every 174,829.[260]

On the other side of the balance, data strongly suggest that these surveillance operations lead to actual arrests, generally for serious crimes such as drug trafficking.[261] In 2008, for example, 1,809

256. *See, e.g.*, *Berger*, 388 U.S. at 65 (Douglas, J., concurring) (likening electronic surveillance to placing "an invisible policeman in the home"); Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) ("The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding.").

257. ADMIN. OFFICE OF THE U.S. COURTS, 2009 WIRETAP REPORT 28 tbl.6 (2010) [hereinafter 2009 WIRETAP REPORT]; 2008 WIRETAP REPORT, *supra* note 121, at 28 tbl.6. These figures are the sum of "electronic" and "combination" intercepts performed during the relevant year.

258. 2009 WIRETAP REPORT, *supra* note 257, at 28 tbl.6; 2008 WIRETAP REPORT, *supra* note 121, at 28 tbl.6.

259. Based on the 2009 U.S. Census Bureau estimate of 307,006,550. *See* U.S. CENSUS BUREAU, POPULATION ESTIMATES, 2000–2009, *available at* http://www.census.gov/popest/states/NST-ann-est.html.

260. This number is the result of dividing the rounded U.S. population by the total number of wire, electronic, and combined wiretaps performed in 2009. It is worth noting, however, that this figure does not reflect surveillance performed under the Foreign Intelligence Surveillance Act ("FISA") or any other domestic security program, as such surveillance is governed by different laws and is beyond the scope of this analysis.

261. In 2008, for example, 1,593 of 1,891 total authorized wiretaps—a little more than eighty-four percent—were for narcotics offenses. 2008 WIRETAP REPORT, *supra* note 121, at 18 tbl.3.

total surveillance operations resulted in 4,133 arrests.[262] And based on past statistics, roughly forty percent to fifty-five percent of those arrested will ultimately be convicted.[263]

The critical point here is that the choice of whether to adopt the purists' bright-line test or the pragmatists' balancing test requires a balancing test of its own. A bright-line rule might be appropriate if the actual threat to liberty were fundamental and imminent. But, as the data show, we are not living in a nightmarish panopticon now,[264] and do not seem to be headed for one anytime soon. In 1967, Justice Douglas warned that allowing electronic surveillance would be the equivalent of putting an invisible police officer into every home.[265] That, indeed, would be a terrifying result. The reality, however, is that electronic surveillance has put an invisible police officer into only a tiny fraction of U.S. homes—usually those where serious crimes are taking place.[266] Under the circumstances, it is reasonable for citizens to make limited privacy concessions for the sake of police effectiveness. And because electronic minimization has been unsuccessful as a privacy protection, the concession turns out to be a small one.

2. Minimization Law Contains Too Many Loopholes

The second strike against the purist position is that even a strengthened minimization requirement would not meaningfully protect individual privacy. There are, quite simply, too many ways for law enforcement to circumvent it, foregoing Title III surveillance altogether in favor of other investigative techniques.[267]

At first glance, this outcome might appear satisfactory. If government agents can get the evidence they need and private citizens can avoid becoming targets of electronic surveillance, then where is

---

262. 2008 WIRETAP REPORT, *supra* note 121, at 26 tbl.6.

263. 2008 WIRETAP REPORT, *supra* note 121, at 38 tbl.9.

264. The term "Panopticon" was first used by Jeremy Bentham to describe a model prison in which prisoners would come to believe that they were under constant surveillance and would, over time, alter their behavior in response. This idea, in turn, became the basis for Michel Foucault's concept of Panopticism—a system of societal control that induces individuals to internalize particular behaviors through constant observation and correction. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–228 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).

265. Berger v. New York, 388 U.S. 41, 64–65 (1967) (Douglas, J., concurring).

266. One explanation for why electronic surveillance has remained a relatively uncommon law-enforcement tool is its high monetary cost. In 2008, the average cost per intercept order was $47,624. 2008 WIRETAP REPORT, *supra* note 121, at 25 tbl.5.

267. *See supra* notes 168–81 and accompanying text.

the downside? The logic behind this argument is seductive, but it ultimately wilts under scrutiny. The critical question is what procedures would take surveillance's place. Would they be more or less likely to intrude on personal privacy?

As noted in Part III.D, the alternatives to electronic surveillance are just as bad at protecting privacy—perhaps even worse.[268] If a heightened minimization requirement encourages police to take a person's electronic communications from a third-party server,[269] or to begin making dubious arrests as a pretext to search the contents of cell phones,[270] then the end result might, perversely, be an overall decrease in individual liberty. The risk of enhanced minimization becoming a Pyrrhic victory for privacy does not appear to be a risk worth taking.

Given how fast technology changes, critics may counter that police in the near future will not have access to the same alternatives to electronic surveillance they do today. They may not, for example, be able to retrieve text messages after the fact from cellular providers.[271] There is already one service—TigerText—that allows its users to create self-deleting text messages.[272] These messages are not just deleted from the recipient's phone, but from the provider network, putting them beyond the reach of any subsequent investigation.[273] While the technology appears to have been created primarily for adulterous spouses,[274] the criminal applications are readily apparent. As a result, law enforcement may find itself relying more and more heavily on real-time interceptions in the years ahead.

---

268. *See supra* notes 168–81 and accompanying text.

269. *See supra* notes 169–72 and accompanying text.

270. *See supra* notes 173–78 and accompanying text.

271. *See supra* notes 169–70 and accompanying text (describing the process of retrieving text-messages from storage).

272. Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, July 25, 2010, at MM 30 ("An app called TigerText allows text-message senders to set a time limit from one minute to 30 days after which the text disappears from the company's servers on which it is stored and therefore from the senders' and recipients' phones.").

273. Press Release, TigerText, TigerText Introduces New Mobile Privacy Network (Nov. 28, 2010), *available at* http://www.tigertextapp.com/tigertext-introduces-new-mobile-privacy-network/ ("The new texting technology enables sender to select the message lifespan (from 1 minute up to 30 days), and once the duration is over, the message will not be available even on server.").

274. *See, e.g.*, Daniel Vasquez, *Tigertext: The iPhone App that Protects Cheaters, Thwarts Snooping Lovers*, SUN-SENTINEL (Ft. Lauderdale, Fla.), Mar. 3, 2010, http://articles.sun-sentinel.com/2010-03-03/business/sfl-tigertext-iphone-app-link-030310_1_iphone-people-text-cheaters (describing the service as protecting cheaters "by removing or hiding sexy texts").

However, even if technological changes force investigators to intercept text messages more regularly, those investigators can still sidestep the minimization requirement by intercepting messages from non-suspects.[275] As Part IV noted, a person has no standing to challenge improper minimization unless the government criminally charges *that person*. For example, if the government intercepts all of *A*'s text messages, without performing any minimization, and uses that information to indict *B*, then *A* will have no meaningful recourse. Therefore, even with the aid of new technologies, the minimization requirement will not meaningfully protect text message privacy.

3. Maintaining the Minimization Rule in this Context Risks Watering Down the "Traditional" Minimization Rule

The analysis so far has mostly addressed the arguments against enhancing minimization in the electronic-surveillance context. Accepting those arguments, why not just leave the requirement as it is? Why, if there is a chance of it ever protecting someone's privacy, should we discard it?

The answer is that electronic minimization is worse than useless. Its existence actually *undermines* the traditional minimization requirement and chips away at Title III's uniform approach to phone conversations. To see how, one need only look at the language of the ECPA.

In 1968, the original Title III required law enforcement to "minimize the interception of communications not otherwise subject to interception under this chapter."[276] Although Congress did not define what it meant by minimization, the requirement was at least short and straightforward. In 1986, however, the ECPA added a curious caveat. It stated that "[i]n the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available . . . minimization may be accomplished as soon as practicable after such interception."[277] The Senate Judiciary Committee clarified that "it is contemplated that the translator or decoder will listen to the tapes of an interception and make available to the investigators the minimized portions . . . ."[278] For the first time since passing Title III, Congress *explicitly* endorsed

275. *See supra* notes 179–81 and accompanying text.

276. Omnibus Crime Control and Safe Streets Act of 1968 § 802(5), Pub. L. No. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2518(5)).

277. ECPA of 1986 § 106(c)(2), 18 U.S.C. § 2518(5) (2006).

278. S. REP. NO. 99–541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3584.

a minimization scheme that allowed one or more agents to listen to all intercepted conversations.[279]

Where did this new language come from? Why did Congress decide to add it? The legislative history does not say, though it is notable that this "foreign/coded language" exception appeared at the same time as, and bore a close resemblance to, the Senate recommendations on how to minimize electronic intercepts.[280] Critically, both provisions called for one or more agents to read or listen to *all* communications, minimize them after the fact, and then pass the minimized transcripts along to other investigators on the team.[281] Congress, in expanding the minimization requirement, tore apart the unitary framework that had once governed phone calls.[282] In its place, Congress left a bifurcated system, in which certain phone calls are treated the same as electronic communications, at least for minimization purposes. From the standpoint of privacy protection, this development was a significant step backward.

A closely related problem is law enforcement confusion. How should government agents determine which minimization standard to use when? The Eastern District of New York highlighted this problem recently in *United States v. Semels*, where it criticized Congress for needlessly muddying the waters.[283] In granting a defendant's motion to suppress, the court emphasized that federal agents had applied the wrong standard, minimizing conversations after the fact that they should have minimized contemporaneously.[284] The court, however, blamed Congress for this mistake as much as it blamed the investigators. As Judge Gleeson noted, the problem "no doubt derive[d] from Congress's use of the word 'minimize' in consecutive

279. For an example of a court analyzing minimization under this standard, see United States v. Gambino, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990).

280. S. REP. NO. 99–541, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585 ("[I]t is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete non-relevant materials and disseminate to other officials only that information which is relevant to the investigation.").

281. *Id.* at 3584–85.

282. The federal courts, admittedly, had been carving out exceptions to this unitary framework for almost two decades. *See, e.g.*, Scott v. United States, 436 U.S. 128, 140 (1978) ("Many of the nonpertinent calls may have been very short. Others may have been one-time only calls. Still other calls may have been ambiguous in nature or apparently involved guarded or coded language. In all these circumstances agents can hardly be expected to know that the calls are not pertinent prior to their termination."). The ECPA is still important, however, as it marked the first time that Congress explicitly approved such an approach.

283. United States v. Simels, No. 08–CR–640 (JG), 2009 WL 1924746, at *3 (E.D.N.Y. July 2, 2009) ("The terminology used by Congress in the 1986 amendment is unfortunate.").

284. *Id.*

sentences in § 2518(5) to mean two different things."[285] Given this confusing language, federal agents ended up applying the wrong standard to their wiretap and intercepting nonpertinent communications. The ECPA's minimization language helped no one and hurt everyone. It led federal agents to violate a suspect's privacy, while also destroying the government's case against that suspect.

The ECPA minimization requirement is beyond worthless; it is detrimental to both privacy and law enforcement interests. Congress, following the implicit advice of the pragmatists, should therefore do away with it.

VI. CONCLUSION

In 1934, Congress faced a serious problem: how to regulate increasingly intrusive but important wire surveillance. It responded with the Federal Communications Act, effectively "minimizing" *all* private conversations by banning wiretaps outright.[286] However, poor drafting and lax enforcement ruined this framework, allowing government agents to violate the ban with impunity.[287]

History repeated in 1968, when Congress again tried to reign in rampant personal privacy violations. The result that time was Title III and the birth of statutory minimization.[288] The tragedy in that case was that Title III actually presented a workable solution and could potentially have struck an enduring compromise between the competing interests of law enforcement and privacy advocates, permitting electronic surveillance but subjecting it to demanding judicial oversight. The courts, however, unraveled that plan, interpreting minimization down into a "reasonableness" requirement rather than a hard and fast rule.[289]

Tragedy turned to farce in 1986. Looking to update Title III and keep pace with technological development, Congress had a perfect opportunity to strengthen the privacy protections that courts had progressively watered down. Instead, it passed the ECPA. While ostensibly affirming and expanding the sphere of personal privacy, the statute provided no meaningful protections for electronic communications and actually undermined existing protections for oral communication. Congress, in other words, lost sight of its original

285. *Id.* at *4.

286. *See supra* notes 42–44 and accompanying text.

287. *See supra* notes 52–56 and accompanying text.

288. *See supra* notes 65–67 and accompanying text.

289. *See supra* notes 78–82 and accompanying text.

goal, insisting on the outward formalities of minimization while acquiescing in the very privacy violations minimization was designed to prevent.

The flaws of modern surveillance law run deeper than the ECPA minimization requirement, and overturning that provision would not serve as a panacea. It would, however, be a welcome first step toward restoring the spirit—rather than the empty formalism—of Title III and true privacy protection.

Seth M. Hyatt[*]

* J.D. Candidate, May 2011, Vanderbilt University Law School. I would like to thank the editors and staff of the VANDERBILT LAW REVIEW for all of the feedback and advice they have given me during the writing process. I would also like to thank Assistant U.S. Attorney Joe Pinjuh of the Northern District of Ohio for suggesting this topic. And always, I thank my family for their continuing support.

***