Fordham Law Review

Volume 84
Issue 3 *Volume 84, Issue 3*

Article 11

2015

Behind Enemy Phone Lines: Insider Trading, Parallel Enforcement, and Sharing the Fruits of Wiretaps

Alexandra N. Mogul
Fordham University School of Law

BEHIND ENEMY PHONE LINES: INSIDER TRADING, PARALLEL ENFORCEMENT, AND SHARING THE FRUITS OF WIRETAPS

*Alexandra N. Mogul**

Two key trends were present in the successful prosecution of Raj Rajaratnam and his coconspirators in one of the largest insider-trading conspiracies in history: the use of wiretaps to investigate and prosecute insider trading and a joint effort between the Department of Justice (DOJ) and the Securities & Exchange Commission (SEC) to conduct the investigation. Despite the close working relationship between the DOJ and the SEC, the DOJ never disclosed the fruits of the wiretaps to the SEC, presumably due to its belief that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended, the "Wiretap Act")—the comprehensive framework that authorizes the government to conduct wiretaps in certain circumstances—prohibited it from doing so.

Though the Second Circuit in SEC v. Rajaratnam *ultimately held that the SEC could obtain wiretap materials from the criminal defendants as part of civil discovery, the question of whether direct disclosure of the wiretap materials from the DOJ to the SEC is prohibited has been raised but not yet addressed. This Note analyzes previous cases addressing the construction of the Wiretap Act's disclosure provisions and concludes that direct disclosure from the DOJ to the SEC is not prohibited by the Act. It further proposes a process by which civil enforcement agencies, such as the SEC, can request disclosure of wiretap materials through the DOJ in such a way that balances the benefits of disclosure against the privacy interests of the parties whose conversations were intercepted.*

* J.D. Candidate, 2016, Fordham University School of Law; B.A., 2010, University of Maryland. I would like to thank my family and friends for their unwavering support.

INTRODUCTION

Throughout American history, criminal organizations—from prohibition-era bootleggers and the mid-century mafia to drug-dealing street gangs and present-day Cosa Nostra—all have used secret, coded communications to conduct their operations.[1] And today, white-collar criminals are the newest players in the world of organized crime. Insider-trading conspirators have resorted to tactics similar to those used in organized crime, such as holding secret meetings, using burner phones,[2] establishing secret codes, and providing cash kickbacks to those willing to assist the Wall Street mob.[3]

1. *See* ANTHONY A. ALBERTI, WIRETAPS: A COMPLETE GUIDE FOR THE LAW AND CRIMINAL JUSTICE PROFESSIONAL 5 (1999).

2. This is a term used to describe cell phones that are disposed of frequently so as to throw off investigators. *See* Matthew DeVoy Jones, *The "Orwellian Consequence" of Smartphone Tracking: Why a Warrant Under the Fourth Amendment Is Required Prior to Collection of GPS Data from Smartphones*, 62 CLEV. ST. L. REV. 211, 211–12 (2014).

3. *SEC Charges 14 in Wall Street Insider Trading Case*, REUTERS (Mar. 1, 2007, 5:03 PM), http://uk.reuters.com/article/2007/03/01/sec-insidertrading-idUKN01350020070301

As Wall Street criminals mimic mob techniques, the government has begun treating them accordingly. Indeed, Preet Bharara, the United States Attorney for the Southern District of New York, has stated that the government is now "targeting white-collar insider trading rings with the same powerful investigative tools that have worked so successfully against the mob and drug cartels"—that is, wiretaps.[4]

This novel use of wiretaps came to light in the recent prosecution of Raj Rajaratnam, his hedge fund Galleon Group, and his coconspirators for their involvement in a massive insider-trading scheme.[5] Over the course of three years, the Department of Justice[6] (DOJ) and the Securities and Exchange Commission[7] (SEC) targeted Rajaratnam, his associates, and his hedge fund for allegedly engaging in a network of shared inside information, enabling the participants in this network to reap millions of dollars on illicit trades.[8] After finding that traditional investigative methods were inadequate to establish sufficient evidence of such insider-trading conspiracies, the government resorted to the use of wiretaps.[9] As a result of the substantial evidence of criminal activity uncovered by the wiretaps, the United States Attorney's Office[10] (USAO) for the Southern District of New York charged and successfully prosecuted numerous people for securities fraud.[11] In addition to criminal charges, the SEC successfully brought civil

---

[http://perma.cc/V6XN-6J2P]; Shane Miller, Note, *Drawing the Line: The Legality of Using Wiretaps to Investigate Insider Trading*, 13 U. PITT. J. TECH. L. & POL'Y 1, 6 (2013).

4. Jordan Maglich, *Once Reserved for Drug Crimes, Wiretapping Takes Center Stage in White Collar Prosecutions*, FORBES (May 21, 2013, 11:32 AM), http://www.forbes.com/sites/jordanmaglich/2013/05/21/once-reserved-for-drug-crimes-wiretapping-takes-center-stage-in-white-collar-prosecutions ("However, it was authorities' decision to employ wiretaps in an insider-trading case that would mark the beginning of an unparalleled and aggressive entrance of wiretaps into white-collar crime jurisprudence.") [http://perma.cc/59JY-R24F]. "Wiretapping" is defined as "[e]lectronic or mechanical eavesdropping, [usually] done by law-enforcement officers under court order, to listen to private conversations." *Wiretapping*, BLACK'S LAW DICTIONARY (10th ed. 2014).

5. *See* United States v. Rajaratnam, 719 F.3d 139 (2d Cir. 2013); Peter Lattman, *Galleon Chief Sentenced to 11-Year Term in Insider Case*, N.Y. TIMES (Oct. 13, 2011, 11:18 AM), http://dealbook.nytimes.com/2011/10/13/rajaratnam-is-sentenced-to-11-years/?_r=0 [http://perma.cc/HT6Z-VMYC]; Maglich, *supra* note 4. *See generally* J. Scott Colesanti, *Wall Street As Yossarian: The Other Effects of the Rajaratnam Insider Trading Conviction*, 40 HOFSTRA L. REV. 411 (2011) (discussing the effects of the Rajaratnam conviction on the "government's ongoing crusade against insider trading").

6. The mission of the DOJ is

> [t]o enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.

About, U.S. DEP'T JUST. http://www.justice.gov/about (last visited Nov. 27, 2015) [http://perma.cc/GWH3-G2JS].

7. *See* Colesanti, *supra* note 5, at 416.

8. *See* Lattman, *supra* note 5.

9. Miller, *supra* note 3, at 6.

10. The USAO is the prosecutorial agency of the DOJ, responsible for bringing criminal cases on behalf of the federal government. *Agencies*, U.S. DEP'T JUST. http://www.justice.gov/agencies (last visited Nov. 27, 2015) [http://perma.cc/G57M-662C].

11. *See* Lattman, *supra* note 5.

enforcement actions against Rajaratnam, Galleon Group, and other coconspirators, recovering tens of millions of dollars in civil penalties.[12]

The Rajaratnam cases[13] represent a coalescence of two trends in the investigation and prosecution of insider trading. First, the DOJ and the SEC engaged in a joint or parallel investigation into the insider-trading activities of the conspirators.[14] Criminal investigators have increasingly engaged the help and expertise of administrative agencies, such as the SEC, charged with the civil enforcement of shared statutory provisions and related regulations.[15] These investigations may involve joint interviews, depositions, and status conferences, and they occasionally involve such an open flow of information between the two agencies that they trigger additional *Brady*[16] requirements.[17] Second, the criminal case against Rajaratnam was the first time that wiretaps were used as evidence in an insider-trading prosecution, and it has opened the door to the use of wiretap information in future insider-trading investigations.[18]

But what happens when these two trends converge? Can the DOJ share the fruits of wiretaps with administrative agencies as part of the increasingly open discourse between the two entities, in light of Title III of the Omnibus Crime Control and Safe Streets Act[19] ("Title III" or "the

12. *See* Press Release, SEC, SEC Obtains Record $92.8 Million Penalty Against Raj Rajaratnam (Nov. 8, 2011), https://www.sec.gov/news/press/2011/2011-233.htm [http://perma.cc/BKK3-ESNL].

13. I use the term "cases" to refer to the fact that not all of the coconspirators were charged under the same docket and that the criminal cases brought by the USAO are separate from the enforcement actions brought by the SEC.

14. *See* Colesanti, *supra* note 5, at 416.

15. Mary Jo White, Chairwoman, SEC, All-Encompassing Enforcement: The Robust Use of Civil and Criminal Actions to Police the Markets (Mar. 31, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370541342996#.VAp5t7xdW50 (noting that the number of criminal cases related to SEC proceedings has doubled since 1993, and the number of times where the SEC grants other law enforcement authorities access to its files—"a rough proxy for the number of cases where [there are] parallel investigations—has also more than doubled") [http://perma.cc/2ANL-8R62]; *see also, e.g.*, Richard A. Goodman et al., *Forensic Epidemiology: Law at the Intersection of Public Health and Criminal Investigations*, 31 J.L. MED. & ETHICS 684, 684 (2003) (discussing parallel investigations between public health agencies and law enforcement authorities); Mark D. Hunter, *SEC/DOJ Parallel Proceedings: Contemplating the Propriety of Recent Judicial Trends*, 68 MO. L. REV. 149 (2003) (discussing parallel investigations between the SEC and the DOJ); *infra* Part I.B.1 (discussing the shared law enforcement authority between the DOJ and the SEC).

16. Brady v. Maryland, 373 U.S. 83 (1963) (requiring the government to disclose any exculpatory evidence in its possession to the defendant).

17. *See, e.g.*, United States v. Martoma, 990 F. Supp. 2d 458 (S.D.N.Y. 2014) (holding that in a parallel investigation between the USAO and the SEC, materials in the sole possession of the SEC are subject to disclosure to the defense in accordance with *Brady* requirements); United States v. Gupta, 848 F. Supp. 2d 491 (S.D.N.Y. 2012) (same).

18. *See* United States v. Rajaratnam, 719 F.3d 139 (2d Cir. 2013); *see also* Kenneth M. Breen & Sean T. Haran, *The Rise of Wiretaps and Government Eavesdropping in Securities Fraud Cases*, 35 CHAMPION 43, 45 (2011) ("The government's victory in *Rajaratnam* will likely embolden its efforts to use wiretaps to investigate insider trading, and the Second Circuit's views on Raj Rajaratnam's appeals on the wiretap suppression issues will be followed closely by the defense bar."); Maglich, *supra* note 4.

19. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2522 (2006)).

Wiretap Act")—the statutory framework authorizing the government to conduct wiretaps?[20]

This question remains unresolved by the circuit courts that have been presented with it,[21] and it has yet to reach the Supreme Court.[22] However, with the increased prosecution of insider trading,[23] the anticipated increase in the use of wiretaps to investigate and prosecute these crimes,[24] and the continuing use of parallel investigations to investigate securities fraud,[25] it is only a matter of time before the question will need to be resolved.

Drawing on traditional tools of statutory interpretation, this Note examines whether the Wiretap Act permits the DOJ to directly disclose the fruits of lawfully intercepted wiretaps to the SEC. Further, this Note examines whether policy dictates that they *should* be able to do so. Part I of this Note provides an overview of the key tools of statutory interpretation relevant to the different readings of the Wiretap Act, the special relationship between the DOJ and the SEC with respect to the enforcement of the securities laws, and the history and relevant provisions of the Wiretap Act. Part II begins with an examination of the different ways that circuit courts have interpreted the disclosure provisions of Title III with respect to civil enforcement agencies. It then addresses the policy issues surrounding the normative question of whether the DOJ *should* be allowed to share the fruits of wiretaps with the SEC during a parallel or joint investigation. Part III argues that, based on the common application of traditional tools of statutory interpretation, the Wiretap Act does not prohibit the DOJ from sharing the fruits of wiretaps with civil enforcement agencies such as the SEC. This Note concludes with a proposed process by which civil enforcement agencies, such as the SEC, can request disclosure of wiretap materials in a way that balances the dual goals of the Wiretap Act.

---

20. *See infra* Part I.C (discussing relevant provisions of Title III, the comprehensive statutory framework governing the government's use of wiretaps to investigate certain crimes).

21. *See infra* Part II.A; *see, e.g.*, SEC v. Rajaratnam, 622 F.3d 159, 174 (2d Cir. 2010) (refusing to address whether the USAO could provide wiretap conversations to the SEC without any law enforcement purpose and solely to assist the SEC in a civil case); Resha v. United States, 767 F.2d 285, 287–88 (6th Cir. 1985) (finding it unnecessary to address the question on the limits of the disclosure provisions of Title III); Fleming v. United States, 547 F.2d 872, 873 (5th Cir. 1977) ("The statute provides no ready answer to the important issue of the extent to which information developed through wiretaps as part of criminal investigations can be disclosed to the Internal Revenue Service for use in civil tax proceedings. We decline to resolve the statutory ambiguities, for we find that whatever the exact scope of the statutory provisions, the evidence was properly admitted under the circumstances here.").

22. *See* Andrew P. Atkins, *New Methods of Financial White-Collar Criminal Investigation and Prosecution: The Spillover of Wiretaps to Civil Enforcement Proceedings*, 33 PACE L. REV. 716, 729 (2013).

23. *See, e.g.*, Patrick Craine & Lashon Kell, *Prosecuting Insider Trading: Recent Developments and Novel Approaches*, 59 ADVOCATE (TEXAS) 45, 47 (2012); Maglich, *supra* note 4 ("The SEC has filed more insider trading cases in the past three years than any three-year period in history, and criminal authorities have obtained more than seventy convictions. Authorities have seized on this momentum, and many more cases are expected.").

24. *See, e.g.*, Atkins, *supra* note 22, at 744–45; Craine & Kell, *supra* note 23, at 47–48.

25. *See* White, *supra* note 15.

I. UNDERSTANDING THE LANDSCAPE: PARALLEL INVESTIGATIONS AND THE DUAL MISSION OF THE WIRETAP ACT

Title III of the Omnibus Crime Control and Safe Streets Act outlines a detailed framework for both the interception of wire communications and the disclosure of the materials intercepted. However, circuit courts have interpreted these provisions differently, leading to varying outcomes. To assist in the analysis of whether Title III permits the DOJ to share the fruits of wiretaps with the SEC, Part I.A provides an overview of some tools of statutory interpretation, including the key tools used in various courts' constructions of Title III. Part I.B then discusses the relationship between the DOJ and the SEC—the two key agencies responsible for the enforcement of the securities laws—and how this relationship lends itself to parallel investigations. Finally, Part I.C discusses the background leading up to the enactment of Title III, as well as the provisions of Title III most relevant to this Note's analysis.

A. Tools of Statutory Interpretation

The question of whether the Wiretap Act permits the DOJ to share the fruits of wiretaps with the SEC in the course of a parallel investigation boils down to a question of statutory interpretation. As such, an understanding of the tools and methods used by courts to interpret statutes is necessary.

Courts have long and consistently held that statutory interpretation begins with the text of the statute itself.[26] As such, courts should ascribe the words of a statute with their ordinary meaning.[27] If the language of the actual text is unclear or ambiguous, then courts may employ additional tools of interpretation, known as "the canons of construction," to derive meaning from the text.[28]

---

26. *See, e.g.*, Barnhart v. Sigmon Coal Co., 534 U.S. 438, 450 (2002) ("As in all statutory construction cases, we begin with the language of the statute."); Victoria F. Nourse, *A Decision Theory of Statutory Interpretation: Legislative History by the Rules*, 122 YALE L.J. 70, 89–90 (2012) (noting that all statutory theories start with the text when engaging in statutory interpretation); *see also* Abbe R. Gluck, *The States As Laboratories of Statutory Interpretation: Methodological Consensus and the New Modified Textualism*, 119 YALE L.J. 1750, 1761 (2010) (discussing how courts may differ in the emphasis placed on the various tools of statutory interpretation).

27. Lawson v. FMR LLC, 134 S. Ct. 1158, 1165 (2014) ("In determining the meaning of a statutory provision, 'we look first to its language, giving the words used their ordinary meaning.'" (quoting Moskal v. United States, 498 U.S. 103, 108 (1990))); *In re* New York Times Co. to Unseal Wiretap & Search Warrant Materials, 577 F.3d 401, 406 (2d Cir. 2009) (interpreting provisions of the Wiretap Act "in light of their ordinary meaning and their contextual setting"). However, different schools of interpretation may differ in the tools used to establish ordinary meaning. *Compare* Gluck, *supra* note 26 (suggesting that not all courts would first examine a term's dictionary definition), *with* Paul J. Larkin, Jr., *Public Choice Theory and Overcriminalization*, 36 HARV. J.L. & PUB. POL'Y 715, 771 (2013) ("[A] court always must start with the text of a statute and give its terms their ordinary, dictionary meaning." (citing Pasquantino v. United States, 544 U.S. 349, 355–56 (2005))).

28. United States v. Magassouba, 544 F.3d 387, 404 (2d Cir. 2008) ("Only if we conclude that statutory language is ambiguous 'do we resort . . . to canons of construction and, if the meaning remains ambiguous, to legislative history.'" (alteration in original) (quoting United States v. Boccagna, 450 F.3d 107, 114 (2d Cir. 2006))); Nourse, *supra* note

Canons of construction are judge-made maxims designed to assist with statutory interpretation by promoting consistency among judicial decision makers.[29] Though the canons of construction are not without their critics (and a considerable amount of academia has focused on rebutting or refining the canons),[30] courts continue to employ them.[31] One canon in particular has been instrumental in some circuits' interpretation of Title III's disclosure provisions: *expressio unius est exclusio alterius* or, simply, *expressio unius*.[32]

Expressio unius means the "inclusion of one thing indicates exclusion of the other."[33] Take, for example the following hypothetical statute, stating: "Grocery stores may sell beer and wine." A strict *expressio unius* reading of this statute would find that grocery stores may sell *only* beer and wine and are prohibited from selling anything else, because the statute does not explicitly say that the grocery store can sell other products.[34] But surely the legislature did not intend to forbid grocery stores from selling other products, such as food and nonalcoholic beverages.[35] Accordingly, the Supreme Court has long held "that the *expressio unius* canon does not apply 'unless it is fair to suppose that Congress considered the unnamed

26, at 137 ("If a court does not use legislative history, it uses something else to resolve ambiguity, whether canons of interpretation, prior precedent, or other statutes . . . .").

29. *See, e.g.*, CBS Inc. v. PrimeTime 24 Joint Venture, 245 F.3d 1217, 1225 (11th Cir. 2001) ("Canons of construction are essentially tools which help [the court] determine whether the meaning of a statutory provision is sufficiently plain, in light of the text of the statute as a whole, to avoid the need to consider extrinsic evidence of Congress' intent."); *see also* Andrew C. Spiropoulos, *Making Laws Moral: A Defense of Substantive Canons of Construction*, 2001 UTAH L. REV. 915, 918 (proposing that judges can "resolve hard cases of statutory interpretation and maintain their legitimacy by developing substantive canons of construction").

30. For further reading on these criticisms, see KARL N. LLEWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS (1960) (arguing that canons are not necessarily determinative of any outcome because every canon can be countered by an equal and opposite counter-canon); Cass R. Sunstein, *Interpreting Statutes in the Regulatory State*, 103 HARV. L. REV. 405, 462–505 (1989) (proposing "interpretive principles" to determine which canon should be applied in a given situation). *See also* Bradford C. Mank, *Textualism's Selective Canons of Statutory Construction: Reinvigorating Individual Liberties, Legislative Authority, and Deference to Executive Agencies*, 86 KY. L.J. 527, 603–08 (1998) (examining Professor Sunstein's interpretive principles).

31. *See, e.g.*, Utility Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2441 (2014) (discussing the canon that "words of a statute must be read in their context and with a view to their place in the overall statutory scheme"); Marx v. Gen. Revenue Corp., 133 S. Ct. 1166, 1175–76 (2013) (applying the canon *expressio unius est exclusio alterius*); RadLAX Gateway Hotel, LLC v. Amalgamated Bank, 132 S. Ct. 2065, 2071 (2012) (discussing the general/specific canon); Clark v. Martinez, 543 U.S. 371, 380–82 (2005) (applying the canon of constitutional avoidance).

32. *See infra* Part II.A.2–3.

33. WILLIAM N. ESKRIDGE, JR., PHILIP P. FRICKEY & ELIZABETH GARRETT, CASES AND MATERIALS ON LEGISLATION: STATUTES AND THE CREATION OF PUBLIC POLICY 824 (3d ed. 2001).

34. *See id.*

35. Indeed, the canon of construction called the "absurdity doctrine" permits judges to deviate from even the most unambiguous statutory text if such a direct interpretation would lead to "absurd results." John F. Manning, *The Absurdity Doctrine*, 116 HARV. L. REV. 2387, 2388–90 (2003). It would certainly be absurd to prohibit a grocery store from selling nonalcoholic beverages.

possibility and meant to say no to it.'"[36] Given the unlikelihood that Congress considered the sale of nonalcoholic beverages and intended to prohibit it, *expressio unius* should not be used to interpret the statute. Additionally, *expressio unius* should not be applied where "Congress has 'an obvious reason for selecting the [examples] that are addressed' in the statute[] and omitting others."[37] Because "beer and wine" are alcoholic beverages, the sale of which tends to be highly regulated, it is obvious why there was a need to expressly authorize grocery stores to sell beer and wine. As such, *expressio unius* should not be used to interpret the statute.

B. The Special Relationship Between the DOJ and the SEC

The DOJ and the SEC enjoy a particularly unique relationship as law enforcement agencies tasked with enforcing the same securities laws, though in different capacities. This part of the Note discusses how the structure of the securities laws creates an attractive environment for the use of parallel or joint investigations between the two agencies. It then discusses the benefits of joint investigations and how they are increasingly used between the DOJ and the SEC.

1. Shared Law Enforcement Authority of Section 10(b)

Section 10(b) of the Securities Exchange Act of 1934[38] ("the Exchange Act") governs securities fraud. It makes it "*unlawful* for any person . . . [t]o use any manipulative or deceptive device or contrivance . . . in connection with the purchase or sale of any security" in violation of an SEC regulation.[39] The section also authorizes the SEC to promulgate rules and regulations that are "necessary or appropriate in the public interest or for the protection of investors."[40] Thus, the criminal and civil enforcement of securities fraud is inherently intertwined, given that a criminal violation of section 10(b) requires a violation of an SEC rule.[41]

Pursuant to section 10(b)'s authorization, the SEC promulgated SEC Rule 10b-5 to address securities fraud[42] and 10b5-1 to more specifically address insider trading.[43] Rule 10b-5 makes it unlawful for any person,

---

36. *Marx*, 133 S. Ct. at 1175 (quoting Barnhart v. Peabody Coal Co., 537 U.S. 149, 168 (2003)).

37. Figueroa v. Sec'y of Health and Human Servs., 715 F.3d 1314, 1323 (Fed. Cir. 2013) (quoting Setser v. United States, 132 S. Ct. 1463, 1469 (2012)).

38. Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j(b) (2012).

39. *Id.* (emphasis added).

40. *Id.* Section 10(b) covers cases of insider trading. *See* Chiarella v. United States, 445 U.S. 222, 230 (1980) (finding that where there is "a duty to disclose arising from a relationship of trust and confidence between parties to a transaction," "silence in connection with the purchase or sale of securities" may constitute fraud under section 10(b)).

41. *See* 15 U.S.C. § 78j(b); Steve Thel, *Taking Section 10(b) Seriously: Criminal Enforcement of SEC Rules*, 2014 COLUM. BUS. L. REV. 1, 4–5 ("[A]bsent a[n SEC] rule, section 10(b) does not prohibit anything. Even when there is a rule, it is the rule that prohibits conduct—section 10(b) does not come into play unless some conduct violates a rule.").

42. 17 C.F.R. § 240.10b-5 (2015).

43. *Id.* § 240.10b5-1.

directly or indirectly, to engage in fraudulent activity in connection with the purchase or sale of any security.[44] Rule 10b5-1 further provides guidance as to what constitutes certain elements of the crime of insider trading.[45]

But being two separate entities with two distinct charters—one a law enforcement agency with the authorization to imprison convicted criminals and the other a civil enforcement agency with the ability to bring civil actions on behalf of the public—the DOJ and the SEC can avail themselves of very different tools when conducting their investigations. The DOJ has the ability to execute search warrants, conduct undercover operations, and—pursuant to the Wiretap Act—execute wiretaps.[46] As a civil enforcement agency, however, the SEC has the ability to issue formal orders of investigation[47] and subpoenas;[48] but unlike the DOJ, the SEC does not have authority to conduct wiretaps.[49] Initially, the SEC's primary means of enforcement was its authority to obtain injunctive relief; however, the SEC's enforcement authority was expanded greatly by a 1990 amendment to the Exchange Act, which authorized the SEC to seek civil money penalties in administrative enforcement actions against regulated entities and people associated with those entities.[50] The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("the Dodd-Frank Act") further expanded this authority by permitting the SEC to seek civil penalties against all persons in administrative enforcement proceedings, not just those associated with regulated entities.[51]

Though the SEC does not have the authority to bring criminal actions, the SEC can facilitate criminal investigations by referring its cases to the

---

44. *Id.* § 240.10b-5. Fraudulent activities include "employ[ing] any device, scheme, or artifice to defraud," "mak[ing] any untrue statement of a material fact or [] omit[ting] to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading," or "engag[ing] in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person." *Id.*

45. *See id.* § 240.10b5-1.

46. *See infra* Part I.C.2.a.

47. *See* SEC DIV. OF ENF'T, ENFORCEMENT MANUAL 17 (2015), http://www.sec.gov/divisions/enforce/enforcementmanual.pdf [http://perma.cc/D4UT-R7BL].

48. *See id.* at 40; *see also* Zachary A. Goldfarb, *SEC Enforcement Division Granted Permanent Subpoena Powers*, WASH. POST (Aug. 12, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/11/AR2010081106274.html [http://perma.cc/A39P-4MCG].

49. *See* White, *supra* note 15.

50. Securities Enforcement Remedies and Penny Stock Reform Act of 1990, Pub. L. No. 101-429, § 201, 104 Stat. 931, 935 (codified at 15 U.S.C. § 78u(d)(3) (2012)); *see also* Thel, *supra* note 41, at 10; GIBSON DUNN, THE DODD-FRANK ACT REINFORCES AND EXPANDS SEC ENFORCEMENT POWERS (2010), http://www.gibsondunn.com/publications/pages/Dodd-FrankActReinforcesAndExpandsSECEnforcementPowers.aspx [http://perma.cc/9CGD-XX2J]. Prior to 1990, the SEC could only obtain civil money penalties in a proceeding before a district judge, rather than in a civil enforcement proceeding. ALAN J. BRUDNER, HOWARD M. PRIVETTE & ADAM D. SCHNEIR, PAUL HASTINGS LLP, STAY CURRENT: A CLIENT ALERT FROM PAUL HASTINGS: FINANCIAL REFORM EXPANDS SEC ENFORCEMENT AUTHORITY 1 (2010), http://www.paulhastings.com/assets/publications/1684.pdf [http://perma.cc/48KB-U4NS].

51. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 § 929P, 15 U.S.C. § 77t (2012); *see also* GIBSON DUNN, *supra* note 50.

appropriate criminal enforcement authorities.[52] Indeed, when the SEC subpoenas a witness to testify before the SEC, the SEC routinely provides the witness with a form, "Form 1662," expressly notifying the recipient that the SEC "often makes its files available to other governmental agencies, particularly the United States Attorneys and state prosecutors [and t]here is a likelihood that information supplied by [the testifying witness] will be made available to such agencies where appropriate."[53] Thus, it is clear that despite the differing authorities of the DOJ and the SEC, their activities and investigations are often interrelated.

2. Benefits and Trends of Parallel Proceedings

Given the joint jurisdiction between the DOJ and the SEC to prosecute securities fraud criminally and civilly, respectively, the two agencies often engage in parallel investigations and proceedings. Parallel proceedings have been defined as "simultaneous, adjudicative proceedings that (1) arise out of a single set of transactions, and (2) are directed against the same defendant or defendants."[54] In recent years, parallel proceedings have been formally established through task forces created by Presidents George W. Bush and Barack Obama to combat financial crime.[55] Informally, many

52. 15 U.S.C. § 77t(b); *id.* § 78u(d)(1); *see* United States v. Stringer, 535 F.3d 929, 933 (9th Cir. 2008) ("Federal securities laws authorize the SEC to transmit evidence it has gathered to the USAO to facilitate a criminal investigation by the USAO."); Anish Vashista, David R. Johnson & Muhtashem S. Choudhury, *Securities Fraud*, 42 AM. CRIM. L. REV. 877, 932–37 (2005) (discussing referrals from the SEC to the DOJ as well as parallel and subsequent proceedings).

53. *See Stringer*, 535 F.3d at 934 (noting that Form 1662 is a routine form provided to witnesses subpoenaed by the SEC).

54. Hunter, *supra* note 15, at 149. Recently, some courts have found that some parallel investigations have become so intertwined as to warrant classification as "joint investigations" and as such have extended the application of *Brady* disclosure requirements to materials held in the sole possession of the administrative agency. *See*, *e.g.*, United States v. Martoma, No. 12 Cr. 973(PGG), 2014 WL 31704, at *1 (S.D.N.Y. Jan. 6, 2014); United States v. Gupta, 848 F. Supp. 2d 491, 493 (S.D.N.Y. 2012) ("Where the USAO conducts a 'joint investigation' with another state or federal agency, courts in this Circuit have held that the prosecutor's duty extends to reviewing the materials in the possession of that other agency for *Brady* evidence."); United States v. Upton, 856 F. Supp. 727, 749 (E.D.N.Y. 1994). For the purposes of this Note, however, the distinction between "joint" and "parallel" proceedings is irrelevant.

55. President George W. Bush established the Corporate Fraud Task Force in 2002 as a joint effort by the DOJ, SEC, Commodity Futures Trade Commission (CFTC), and other agencies to combat financial crime. *See* Miheer Mhatre, Note, *Parallel or Paralyzed?* Sklena, *Rule 804(B)(1), and the Costly Implications for Interagency Law Enforcement Efforts*, 2013 COLUM. BUS. L. REV. 546, 557–59. President Obama established the Financial Fraud Enforcement Task Force (FFETF) to reinvigorate the preceding Bush Administration's task force and to hold accountable those responsible for the financial crisis. *Id.* at 558–59. The FFETF is an interagency coalition of multiple federal departments, agencies and offices, including the DOJ and the SEC. *See About the Task Force: Task Force Members*, FIN. FRAUD ENFORCEMENT TASK FORCE, www.stopfraud.gov/members.html (last visited Nov. 27, 2015) [http://perma.cc/A744-C4AZ]. The FFETF is further broken down into multiple working groups, one of which is the Securities and Commodities Fraud Working Group, cochaired by a U.S. Attorney, an Assistant Attorney General for the Criminal Division of the DOJ, the Director of Enforcement for the CFTC, and the Director of Enforcement for the SEC. *See About the Task Force: Task Force Leadership*, FIN. FRAUD

parallel investigations arise out of the shared statutory authority of the SEC and the DOJ to investigate and enforce the federal securities laws—in particular the laws and rules pursuant to section 10(b).[56]

Courts, including the Supreme Court, have consistently upheld the constitutionality of parallel investigations between criminal investigative agencies and civil enforcement agencies, as long as the agencies do not act in bad faith.[57] Courts, however, have noted that agencies act in bad faith where an agency makes affirmative misrepresentations or uses the civil investigation as a subterfuge to obtain information solely for the purpose of the criminal investigation.[58]

Traditionally, criminal investigations into insider trading stemmed from referrals from the SEC or other self-regulatory organizations, such as when SEC systems identify suspicious trading patterns.[59] Insider-trading cases have historically been based on—and convictions have been obtained through—circumstantial evidence, such as trading records and call logs.[60] Prosecutors would present a timeline of suspicious activity (for example, the tipper comes out of a board meeting at 12 p.m., then makes a phone call to the alleged tippee at 12:02 p.m.), supplemented by trading records of the tippee's transactions on the alleged inside information, followed by information of a substantial gain or loss avoidance on behalf of the tippee.[61] However, as the case against Rajaratnam shows, the government is now willing to undertake more aggressive investigative tactics to obtain more direct evidence of insider trading—tactics like wiretaps.[62]

ENFORCEMENT TASK FORCE, www.stopfraud.gov/leadership.html (last visited Nov. 27, 2015) [http://perma.cc/JWV9-BX3Z].

56. *See* Thel, *supra* note 41; Mhatre, *supra* note 55, at 560–61; *supra* Part I.B.1 (discussing the shared enforcement authority between the DOJ and the SEC).

57. *See, e.g.*, United States v. Kordel, 397 U.S. 1, 11 (1970); SEC v. Dresser Indus. Inc., 628 F.2d 1368, 1376–77 (D.C. Cir. 1980) (en banc) ("Effective enforcement of the securities laws requires that the SEC and [DOJ] be able to investigate possible violations simultaneously."); *see also Panel: The SEC's Perspective*, 2013 COLUM. BUS. L. REV. 519, 525–26 [hereinafter *Panel I*] ("That means that as long as [the SEC is] making decisions for [itself]—independent of the criminal interest—and [the SEC and the DOJ] do not use one another's investigative powers and processes to advantage the other's interest, then [the SEC's actions] are okay.").

58. *See, e.g.*, *Stringer*, 535 F.3d at 937; United States v. Carriles, 486 F. Supp. 2d 599, 615, 619 (W.D. Tex. 2007); United States v. Rand, 308 F. Supp. 1231, 1233, 1237 (N.D. Ohio 1970).

59. *See* Kenneth Herzinger & Mark Mermelstein, *On Tap: The Government's Use of Wiretaps in Insider Trading Prosecutions Shows a Willingness to Use Nontraditional Methods of Investigation*, L.A. LAW., April 2012, at 30, 32.

60. *See id.*; *Panel: A View from the Front Lines*, 2013 COLUM. BUS. L. REV. 463, 471–72 [hereinafter *Panel II*].

61. *See Panel II*, *supra* note 60, at 472. A tipper is the party providing the inside information; a tippee is the party receiving the inside information.

62. *See generally* United States v. Rajaratnam, 719 F.3d 139 (2d Cir. 2013) (upholding the government's use of wiretaps to investigate the defendant's participation in an insider-trading scheme).

C. The Wiretap Act: A Balancing Act

The Communications Act of 1934 first addressed the interception of wire communications.[63] Section 605 of this act "outlawed the interception [of wire communications] without authorization" as well as "the divulging or publishing of the contents of wiretaps."[64] However, after the Supreme Court's rulings in *Berger v. New York*[65] and *Katz v. United States*,[66] both proponents and opponents of wiretapping and electronic surveillance "agree[d] that the present state of law in this area [was] extremely unsatisfactory" and that Congress needed "to clarify the resulting confusion."[67] Thus, the Wiretap Act was born. This section begins with the history of the Wiretap Act, including the problems that it was intended to solve and its legislative history. It then summarizes the relevant provisions of the Wiretap Act.

1. Balancing Individual Privacy with Investigative Value

Originally passed by Congress as Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[68] the Wiretap Act was enacted with a "dual purpose" to (1) protect against violations of individuals' Fourth Amendment rights, and (2) provide the government with the authority to intercept wire communications in the course of certain criminal investigations.[69] In 1986, the Electronic Communications Privacy Act (ECPA) amended Title III to address the interception of electronic communications in addition to wire communications.[70]

---

63. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended at 47 U.S.C. §§ 151–622 (2012)); *see* Weiss v. United States, 308 U.S. 321 (1939) (holding that section 605 of the Communications Act prohibited the interception and divulgence of both interstate and intrastate telephone calls); *see also* S. REP. NO. 90-1097, at 67 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.

64. Berger v. New York, 388 U.S. 41, 46 (1967) (discussing The Communications Act of 1934). *See generally Weiss*, 308 U.S. 321. Title III amended the language of section 605 of the Communications Act and narrowed its application by excluding "a law enforcement officer acting in the normal course of his duties" from the definition of "any person," to which the section applies. S. REP. NO. 90-1097, at 108, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2197; *see also* 47 U.S.C. § 605 ("No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.").

65. 388 U.S. 41 (1967) (finding a New York statute authorizing wiretaps in violation of the Fourth Amendment, and delineating the constitutional criteria that electronic surveillance legislation should contain).

66. 389 U.S. 347 (1967) (extending the protections of the Fourth Amendment to all areas where a person has a reasonable expectation of privacy).

67. S. REP. NO. 90-1097, at 67, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 (noting that the present status of wiretapping and electronic surveillance law is "intolerable").

68. Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522).

69. S. REP. NO. 90-1097, at 66, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

70. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). The ECPA also included provisions known as the Stored Communications Act (SCA), which outlined the processes and procedures by which the government may access electronic communications in stored

The drafters of the Wiretap Act were concerned that technological developments had led to the widespread use and abuse of electronic surveillance, due to the newfound ease of intercepting communications.[71] They feared that this had upset commercial soundness by increasing commercial espionage and making it difficult to conduct business meetings in private.[72] They also expressed concern that the intrusions did not stop at the commercial level, but also broke the barrier into individuals' private lives by generally enabling "every spoken word relating to each man's personal, marital, religious, political, or commercial concerns [to] be intercepted by an unseen auditor and turned against the speaker."[73]

At the same time, however, the drafters recognized that the structured, regulated use of wiretaps held significant value in one particular aspect of the criminal justice system: organized crime.[74] The framers of the act recognized that the structure of the criminal justice system was incompatible with the development of organized crime.[75] Though laws existed to penalize such behavior, authorities found it difficult to meaningfully enforce them due to problems with gathering sufficient evidence.[76] Investigations were unlikely to yield any willing witnesses, as "[i]nsiders are kept quiet by an ideology of silence underwritten by a fear, quite realistic, that death comes to him who talks."[77] And even when the authorities had found someone willing to talk in exchange for payment, the resulting information was often unreliable.[78] Furthermore, traditional investigative tools, such as search warrants and subpoenas, proved ineffective because "organized crime groups do not keep books and records available for law enforcement inspection."[79]

The framers of the act recognized organized crime's heightened reliance on in-person and phone communications to avoid "the possibility of loss or

---

mediums such as emails, voice messages, and secondary information about communications like pen registers. *Id.*

71. S. REP. NO. 90-1097, at 67, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.

72. *Id.*

73. *Id.* The Supreme Court has interpreted the intentions of the framers of Title III with an emphasis toward the protection of privacy: "[A]lthough Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern." Gelbard v. United States, 408 U.S. 41, 48 (1972).

74. S. REP. NO. 90-1097, at 70, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2157.

75. *Id.* ("In our formative years, offenses usually occurred between neighbors. . . . Ignored entirely in the development of our system of justice, therefore, was the possibility of the growth of a phenomenon such as modern organized crime with its attendant corruption [of] our political and law enforcement processes.").

76. *Id.* at 73, *reprinted in* 1968 U.S.C.C.A.N. at 2160 ("The prohibitions of the criminal law are, in short, not self-executing."). Indeed, a 1967 report by the President's Commission on Law Enforcement and Administration of Justice ("the Presidential Commission") found that organized crime was "continu[ing] to grow because of defects in the evidence gathering process." *Id. See also generally* THE PRESIDENT'S COMM'N ON LAW ENF'T AND ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY (1967) https://www.ncjrs.gov/pdffiles1/nij/42.pdf [http://perma.cc/34LA-BT8N].

77. S. REP. NO. 90-1097, at 73, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2160.

78. *Id.* at 72, *reprinted in* 1968 U.S.C.C.A.N. at 2159.

79. *Id.* at 73, *reprinted in* 1968 U.S.C.C.A.N. at 2160.

seizure of an incriminating document."[80] But there was one tool that proved particularly successful in prosecuting these crimes: wiretaps.[81] Former New York County District Attorney Frank Hogan testified before the Senate about the indispensability of wiretapping as a "weapon in the fight against organized crime,"[82] noting its contribution to successful prosecutions of criminal enterprises in New York in prior years.[83] Consequently, Congress recognized the value that wiretaps possessed in the combat of organized crime[84] and enacted the Wiretap Act on June 19, 1968.[85]

2. The Act in Action

The Wiretap Act outlines a broad regulatory framework for the interception and disclosure of wire, electronic, and oral communications, imposing greater limitations on the use of wiretaps than on other investigative tools due to the substantial privacy interests at stake. Part I.B.2 of this Note discusses the procedural requirements to obtain court authorization to conduct wiretaps, the relevant provisions addressing the disclosure of wiretapped communications, and the use of such intercepted communications as evidence during trial.

a. Procedural Requirements

In recognition of the privacy interests at stake, Title III permits wiretaps only in the course of investigations for certain serious offenses known as "predicate offenses," which are outlined in 18 U.S.C. § 2516.[86] Included in this list are offenses historically prevalent in organized crime, including mail fraud, wire fraud, money laundering, bank fraud, and computer fraud.[87] Notably absent from this enumeration of fraud-related crimes is securities fraud.[88] However, if evidence of a nonpredicate offense is

80. *Id.* at 71, *reprinted in* 1968 U.S.C.C.A.N. at 2159.

81. *Id.* at 72, *reprinted in* 1968 U.S.C.C.A.N. at 2159.

82. *Id.*

83. *Id.* at 72–73, *reprinted in* 1968 U.S.C.C.A.N. at 2159–63.

84. *Id.* at 72–76, *reprinted in* 1968 U.S.C.C.A.N. at 2159–63. *But see* Berger v. New York, 388 U.S. 41, 60 (1967) (noting that despite the Presidential Commission's report, the court had found no empirical statistics on the use of electronic devices in the fight against organized crime).

85. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)).

86. *See* 18 U.S.C. § 2516. Title III also allows for the investigations of certain state crimes to utilize wiretaps, so long as the state separately authorizes its use by statute. *Id.* § 2516(2); *see also* Kyle G. Grimm, *The Expanded Use of Wiretap Evidence in White-Collar Prosecutions: Rebalancing Privacy Through More Vigorous Enforcement of the Predicate Offense Requirement and the Suppression Provisions of Title III*, 33 PACE L. REV. 1146, 1166 (2013).

87. 18 U.S.C. § 2516; *see* S. REP. NO. 90-1097, at 97, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2186 ("Each offense has been chosen either because it is intrinsically serious or because it is characteristic of the operations of organized crime."); Grimm, *supra* note 86, at 1166.

88. *See* 18 U.S.C. § 2516.

revealed during the course of a lawful wiretap, the wiretap evidence of that second crime may still be admitted.[89] This "plain-view exception" is codified in Title III and states that such information may be disclosed or used pursuant to the "law enforcement use"[90] and "law enforcement disclosure"[91] provisions, but disclosures pursuant to the "testimonial disclosure"[92] provision are permitted only after a judge of competent jurisdiction rules that "the contents were otherwise intercepted in accordance with" Title III.[93]

Section 2518, entitled "Procedure for interception of wire, oral, or electronic communications," outlines, inter alia, the application requirements, the conditions that must be met before a judge grants such authorization, the required contents of the order, the amount of time the applicant has to conduct the wiretaps, and the post-interception procedural requirements.[94] Applications must include, inter alia, the identity of the party making the request, a statement of facts justifying the applicant's belief that a wiretap order should be issued, details regarding the particular offense being investigated, a description of the communications sought, and the identity, if known, of the party whose communications are sought.[95] The Wiretap Act then permits a judge to enter an ex parte order authorizing a wiretap, subject to some additional limitations, if the judge determines that, based on the facts included in the application, "there is probable cause for belief that an individual is committing, has committed, or is about to commit" a predicate offense, "there is probable cause for belief that particular communications concerning that offense will be obtained through such interception," and 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."[96]

---

89. *Id.* § 2517(5); *see* United States v. Rajaratnam, No. 09 Cr. 1184(RJH), 2010 WL 4867402, at *1 (S.D.N.Y. Nov. 24, 2010) (finding that the government was permitted to use wiretaps to investigate fraudulent insider-trading activity using interstate wires because wire fraud is a permitted predicate offense subject to wiretaps).

90. *See infra* notes 109–12 and accompanying text.

91. *See infra* notes 106–09 and accompanying text.

92. *See infra* notes 114–18 and accompanying text.

93. 18 U.S.C. § 2517(5); *see id.* § 2517(1)–(2). Critics of the plain-view exception argue that it has the potential for abuse, in that a purported investigation into a predicate offense may be used as a subterfuge to use wiretaps to investigate nonpredicate offenses. *See* Miller, *supra* note 3, at 9–10. Indeed, Raj Rajaratnam raised this issue in his criminal case, arguing that because the initial wiretap application stated the predicate offense of wire fraud and he was never charged with wire fraud, the evidence derived from the wiretaps should not be admitted in a prosecution for securities fraud. *Rajaratnam*, 2010 WL 4867402, at *1. However, the court held that because "Title III authorizes the government to use wiretaps to investigate wire fraud, the government was authorized to use wiretaps to investigate a fraudulent insider trading scheme using interstate wires even though Title III does not specifically authorize wiretaps to investigate insider trading alone." *Id.* Thus, the government's failure to charge the defendants with wire fraud does not necessarily preclude the use of the plain-view exception. *See id.*; *see also* 18 U.S.C. § 2517(5).

94. 18 U.S.C. § 2518; *see also* Mike Lewis, *Electronic Surveillance*, 77 GEO. L.J. 594, 598–611 (1988).

95. 18 U.S.C. § 2517(5).

96. *Id.* § 2518(3).

Upon expiration of a wiretap order, the intercepted recordings must be made available to the judge who issued the order and filed under seal,[97] though the government is permitted to maintain duplicate recordings of the wiretaps for use or disclosure in accordance with the provisions of § 2517(1)–(2).[98] The section also requires that applications for and orders granting the government authority to conduct wiretaps be sealed by the judge and that they "shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction."[99]

b. Disclosures Expressly Prohibited—§ 2511

Section 2511 explicitly prohibits the disclosure or use of wiretaps in two instances: (1) with the knowledge that said wiretaps were obtained unlawfully,[100] and (2) for the purpose of impeding a criminal investigation, with knowledge that said wiretaps were intercepted in connection with a criminal investigation.[101]

Notably, though the Senate Report accompanying Title III states that § 2511 prohibits the disclosure of all intercepted communications except for those explicitly permitted,[102] the language of § 2511 itself does not

97. *Id.* §§ 2518(5), (8)(a); U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 27 (2005), http://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf [hereinafter DOJ MANUAL] ("The purpose of the sealing requirement is to preserve the integrity of the electronic surveillance evidence.") [http://perma.cc/CW3V-2JPS].

98. 18 U.S.C. § 2518(8)(a); *see id.* § 2517(1)–(2); *infra* notes 106–13 and accompanying text.

99. 18 U.S.C. § 2518(8)(b). The DOJ has taken the position that the legislative history of this subsection implies that the subsection also governs the disclosure of wiretap materials themselves, not just the applications and orders. *See* DOJ MANUAL, *supra* note 97 ("Although section 2518(8)(b) provides for the disclosure of Title III 'applications and orders,' the legislative history reflects that it was also intended to apply to the disclosure of the Title III recordings themselves, as well as any related documentation."). The DOJ recommends that "when in doubt about whether the disclosure or use of electronic surveillance evidence is permitted, [attorneys should] obtain a court order pursuant to 18 U.S.C. § 2518(8)(b) authorizing the disclosure and use for 'good cause.'" *Id.* However, this seems to overlook the fact that some courts have defined "good cause" similar to "aggrieved person," and thus it is unlikely that the government will succeed. *See* 18 U.S.C. § 2510(11) (defining "aggrieved person" as "a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed"); *In re* New York Times Co. to Unseal Wiretap & Search Warrant Materials, 577 F.3d 401, 408 (2d Cir. 2009).

100. 18 U.S.C. § 2511(1)(c)–(d); *see also* United States v. Dorfman, 690 F.2d 1230, 1232 (7th Cir. 1982) ("Title III makes it a crime to disclose wiretap evidence (transcripts, logs, summaries, etc.) only if the evidence was obtained in violation of Title III and the disclosure is willful.").

101. 18 U.S.C. § 2511(1)(e). The statute does not specifically say *who* would be doing the disclosing, but presumably addresses disclosure or use by anyone in lawful possession of the wiretap materials. *See id.*

102. S. REP. NO. 90-1097, at 91 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2180 ("Section 2511 of the new chapter prohibits, except as otherwise specifically provided in the chapter itself, the interception and disclosure of all wire or oral communications.").

explicitly say this.[103] This inconsistency has led circuit courts to interpret Title III differently.[104]

c. Disclosures Expressly Permitted—§ 2517

But § 2511 is not the only section of Title III causing trouble among circuit courts. Section 2517, which outlines specific instances in which the disclosure of wiretaps or evidence derived therefrom is expressly *permitted*, also feeds into the question of whether the DOJ can disclose the fruits of wiretaps to civil enforcement agencies.[105]

First, investigative or law enforcement officers[106] are permitted to *disclose* the contents of wiretaps, or evidence derived therefrom, to another investigative or law enforcement officer "to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."[107] This will be referred to as the "law enforcement disclosure" provision. Disclosures under this provision may be made at any time and are not required to be postponed until after the surveillance is completed.[108] The purpose of this provision is to facilitate the exchange of information among law enforcement personnel, particularly between state and federal officers.[109]

Second, investigative or law enforcement officers may *use* the contents of wiretaps "to the extent such use is appropriate to the proper performance of [the investigative or law enforcement officer's] official duties."[110] This will be referred to as the "law enforcement use" provision. In framing this

---

103. *See* 18 U.S.C. § 2511. A canon of construction, "the title and heading canon," provides that in certain circumstances, courts may use titles or headings as interpretive aids. Jacob Scott, *Codified Canons and the Common Law of Interpretation*, 98 GEO. L.J. 341, 367 (2010). Two states' codified canons of construction lend support to giving a section header some weight when interpreting a statute; however, twenty-two states have codified an affirmative rejection of this canon. *Id.* at 368.

104. *See infra* Part II.A.

105. 18 U.S.C. § 2517; *see also Dorfman*, 690 F.2d at 1232 ("[B]y permitting disclosure of lawfully obtained wiretap evidence only under the specific circumstances listed in 18 U.S.C. § 2517, Title III implies that what is not permitted is forbidden."); *infra* Part II.A. The three discussed permitted disclosures under § 2517 appear to "assume that disclosure may be made without a determination as to the legality of the interception, except as to disclosure through testimony about offenses not listed in the order." Atkins, *supra* note 22, at 740.

106. An "investigative or law enforcement officer" is "any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter[] and any attorney authorized by law to prosecute or participate in the prosecution of such offenses." 18 U.S.C. § 2510(7).

107. *Id.* § 2517(1).

108. 2 HON. JAMES G. CARR & PATRICIA L. BELLIA, LAW OF ELECTRONIC SURVEILLANCE § 7:34 (2015).

109. *Id.*

110. 18 U.S.C. § 2517(2); *see* Fleming v. United States, 547 F.2d 872, 874 (5th Cir. 1977) ("The disclosure by an investigative or law enforcement officer of the contents of an intercepted communication to IRS revenue agents may constitute 'use' of such contents that is 'appropriate to the proper performance of his official duties.'" (quoting 18 U.S.C. § 2517(2))); *infra* Part II.A.

section, the Senate had in mind that it would authorize uses such as establishing probable cause for arrest, establishing probable cause to search, or refreshing the recollection of witnesses.[111] Additional lawful disclosures under § 2517(2) include the disclosure to third parties in order to have them identify speakers' voices[112] and to secretaries for administrative assistance.[113]

Third, any person[114] who has lawfully received any information from a wiretap may *disclose* that information "while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof."[115] This will be referred to as the "testimonial disclosure" provision. Prior to 1970,[116] however, § 2517(3) permitted testimonial disclosures "in any *criminal* proceeding."[117] However, pursuant to the Racketeer Influenced and Corrupt Organizations Act, § 2517(3) was amended to remove the word "criminal," thus potentially broadening the applicability of the provision to permit testimonial disclosures of wiretap materials in civil proceedings as well as criminal proceedings.[118]

Section 2518(8)(b) addresses the disclosure of the applications made and orders granted under Title III.[119] The DOJ, however, has suggested that this section should be interpreted as addressing requests for disclosures of wiretap materials themselves.[120]

---

111. S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2188.

112. United States v. Rabstein, 554 F.2d 190, 193 (5th Cir. 1977).

113. *See, e.g.*, United States v. O'Connell, 841 F.2d 1408, 1417 (8th Cir. 1988); *Rabstein*, 554 F.2d at 193; 2 CARR & BELLIA, *supra* note 108, § 7:36.

114. "Any person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6). *Compare id.*, *with supra* note 106 and accompanying text.

115. 18 U.S.C. § 2517(3).

116. In 1970, the Racketeer Influenced and Corrupt Organizations Act (RICO) was enacted, which established a civil cause of action for activities undertaken by criminal organizations and amended 18 U.S.C. § 2517(3). Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 902(b), 84 Stat. 922, 947.

117. *Id.* at 944 (emphasis added).

118. *See In re* Motion to Unseal Elec. Surveillance Evidence, 965 F.2d 637, 639 (8th Cir. 1992) ("The words 'any proceeding' [in § 2517(3)] are clearly sufficient to include private civil action such as the one in this case."), *rev'd en banc*, 990 F.2d 1015, 1018–19 (8th Cir. 1993) (rejecting the contention that the 1970 amendment's removal of the word "criminal" from § 2517(3) permits pretrial disclosure of wiretap materials to a nongovernmental party); Jesse G. Kreier, *Electronic Surveillance*, 74 GEO. L.J. 559, 568 n.517 (1986) (suggesting that wiretaps may be used in civil proceedings to which the government is a party). *But see* Nat'l Broadcasting Co. v. U.S. Dep't of Justice, 735 F.2d 51, 54 (2d Cir. 1984) ("[T]urning Title III into a general civil discovery mechanism would simply ignore the privacy rights of those whose conversations are overheard.").

119. 18 U.S.C. § 2518(8)(b).

120. DOJ MANUAL, *supra* note 97, § 9-7.000.

d. Use As Evidence and Grounds for Suppression

Sections 2515 and 2518 address whether wiretap materials may be introduced into evidence, as well as the grounds for suppression.[121] Section 2515 prohibits the introduction into evidence of wiretaps or evidence derived therefrom "if the disclosure of [such materials] would be in violation of" the Wiretap Act.[122] This subsection has been interpreted as prohibiting wiretap materials *intercepted* in violation of the Wiretap Act from being introduced into evidence, not wiretap materials that were *disclosed* in violation of the act.[123] For example, wire communications obtained without a warrant would be prohibited from being introduced into evidence because they were *intercepted* in violation of the Wiretap Act; however, lawfully intercepted wire communications that have subsequently been *disclosed* to another party in violation of the act are not necessarily prohibited from being introduced into evidence.[124]

Section 2518(10)(a) outlines the provisions regarding the suppression of wiretaps.[125] It states, in relevant part:

> Any aggrieved person in any . . . proceeding in or before any court . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—
>
> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.[126]

Notably absent from the list of grounds for suppression is an unlawful disclosure.[127] Indeed, courts have interpreted this provision as providing a remedy of suppression for *unlawfully intercepted* communications, not for *unlawfully disclosed* communications.[128]

121. *See* 18 U.S.C. §§ 2515, 2518.
122. 18 U.S.C. § 2515.
123. *See* Fleming v. United States, 547 F.2d 872, 874 (5th Cir. 1977).
124. *See id.*
125. *See* 18 U.S.C. § 2518(10)(a).
126. *Id.*
127. *See id.*
128. *See* Resha v. United States, 767 F.2d 285, 289 (6th Cir. 1985); *Fleming*, 547 F.2d at 874; *see also* Memorandum in Support of Defendants' Joint Motion for a Protective Order to Prohibit the Unlawful Disclosure of Wiretap Evidence, United States v. Rajaratnam, 2010 WL 2131194 (S.D.N.Y. Nov. 24, 2010) (No. 09 Cr. 1184) [hereinafter Memorandum] (arguing that *Fleming* should not be interpreted as permitting disclosure of wiretaps to a civil enforcement agency, because it held only that such disclosed evidence could not be suppressed).

II. DIFFERENT STROKES FOR DIFFERENT FOLKS: CONFLICTING INTERPRETATIONS AND CONSIDERATIONS OF TITLE III

With an understanding of the statutory framework governing court-authorized wiretaps, the tools of statutory construction, and the importance of resolving the circuit split, this part discusses the cases and arguments pertaining to whether the DOJ can share the fruits of wiretaps with the SEC in a parallel or joint investigation. Part II.A begins with the descriptive question of statutory interpretation—that is, whether the Wiretap Act *permits* the DOJ to share the fruits of wiretaps with civil enforcement agencies. It discusses the different constructions of the Wiretap Act and the cases that support such constructions. Part II.B then addresses the normative question of whether the DOJ *should* be allowed to share the fruits of wiretaps with the SEC during a parallel or joint investigation in light of the privacy interests at stake.

A. The Descriptive Question: Three Views on Sharing Wiretaps with Civil Enforcement Agencies

Though some courts have been presented with the opportunity to address the issue of direct disclosure of the fruits of wiretaps from the DOJ to a civil enforcement agency, they have declined to do so.[129] Many courts have, however, addressed the limits of the disclosure provisions of the Wiretap Act and have come out in different ways. It is these assessments of the disclosure provisions that may support or weaken the case for the direct disclosure of wiretaps from the DOJ to the SEC.

1. The Wiretap Act Explicitly Permits Such Disclosures

Some have argued that the Wiretap Act expressly permits direct disclosures of wiretap materials from the DOJ to the SEC under the law enforcement disclosure and law enforcement use provisions.[130] However, the law enforcement disclosure provision requires both the disclosing party and the recipient to be "investigative or law enforcement officer[s]."[131] This is unlikely to happen, however, because only those officials who are authorized to investigate or prosecute predicate offenses qualify as an investigative or law enforcement officer, and securities fraud is not a predicate offense.[132] However, the SEC could argue that because it often investigates wire fraud as part of its investigations into insider trading and

129. *See, e.g.*, SEC v. Rajaratnam, 622 F.3d 159, 174 (2d Cir. 2010) (declining to confirm whether the USAO's position that it is permitted to disclose wiretap materials directly to the SEC is correct); *Resha*, 767 F.2d at 287–88 (finding it unnecessary to decide whether the disclosure of wiretap materials from the DOJ to the IRS was permissible, because even if it were unlawful, unlawful disclosure is not grounds for suppression).

130. Atkins, *supra* note 22, at 737; DOJ MANUAL, *supra* note 97 (noting that the legislative history and case law indicate that "disclosure of Title III information for any legitimate investigative purpose associated with the development of a criminal case" is permitted under § 2517); *see supra* Part I.C.2.b.

131. *See supra* notes 106–09 and accompanying text.

132. Atkins, *supra* note 22, at 737–38.

shares that information with the DOJ, such SEC officials qualify as law enforcement or investigative officers under § 2517(1).[133] Additionally, the SEC could argue that by participating in a formal joint task force such as the Financial Fraud Enforcement Task Force,[134] its agents qualify as a law enforcement or investigative officer because of their direct involvement in the government's criminal investigations into wire fraud, which is a predicate offense.[135]

Disclosures under § 2517(2) may be more likely to withstand scrutiny, because this subsection does not limit disclosures to investigative or law enforcement officers.[136] Indeed, the Fifth Circuit has suggested that "disclosure by an investigative or law enforcement officer of [wiretap materials] to IRS revenue agents *may* constitute 'use' of such contents that is 'appropriate to the proper performance of his official duties'"[137] in accordance with the permitted disclosures under § 2517(2).[138]

In *Fleming v. United States*,[139] the court addressed the question of whether lawfully intercepted wiretap materials that were disclosed from the DOJ to IRS revenue agents could be introduced into evidence in a subsequent civil case.[140] The petitioner argued that Title III prohibited the wiretaps from being admitted into evidence in the civil case because § 2515 mandates the exclusion of evidence that has been improperly disclosed, and § 2517 is the sole authority for permitted disclosures.[141] Therefore, the petitioner argued, because § 2517 does not expressly permit disclosure from the FBI to the civil tax authorities, the disclosure was unlawful and thus should not have been admitted into evidence in accordance with § 2515.[142]

---

133. *Id.*

134. *See supra* Part I.B.2.

135. *See supra* Part I.C.2.a.

136. *See* Atkins, *supra* note 22, at 738; *supra* Part I.C.2.c (discussing expressly permitted disclosures).

137. Fleming v. United States, 547 F.2d 872, 874 (5th Cir. 1977) (emphasis added) (quoting 18 U.S.C. § 2517(2)(2012)); *see also* Griffin v. United States, 588 F.2d 521, 526 (5th Cir. 1979) (refusing to overrule the holding in *Fleming*). Both *Griffin* and *Fleming* stemmed from the same incident, but the cases involved different claims against the IRS; the IRS counterclaimed in each case and relied on the wiretaps from the criminal investigation as part of its counterclaims. *Griffin*, 588 F.2d at 521–22; *Fleming*, 547 F.2d at 873.

138. IRS revenue agents are responsible for auditing tax returns; IRS special agents are responsible for the criminal investigation of tax offenses. *See* Caroline D. Ciraolo, *Criminal Tax Cases: A Primer*, *in* STRATEGIES FOR CRIMINAL TAX CASES: LEADING LAWYERS ON NAVIGATING TAX LAW, UNDERSTANDING DISCLOSURE GUIDELINES, AND RESPONDING TO GOVERNMENT INVESTIGATIONS 75, 80–82 (Aspatore 2011).

139. 547 F.2d 872 (5th Cir. 1977).

140. *Id.* at 873. The defense conceded that the interception of the wiretaps conducted by the FBI comported with all statutory requirements. *Id.*

141. *See id.* at 873; *see also supra* Part I.C.2.c.

142. The court's opinion did not discuss the government's opposing arguments, if any. *Fleming*, 547 F.2d at 873 ("[T]he government agents were not free to disclose the information they had obtained to IRS revenue agents."). The petitioner further argued that Title III does not permit the use of wiretaps to investigate civil tax offenses. *Id.*

Though the court ultimately resolved the question of admissibility based on other grounds,[143] it proceeded to hypothetically analyze the question of whether the materials were lawfully disclosed.[144] The court found that, even if the Wiretap Act prohibited the introduction of evidence that was unlawfully disclosed (as opposed to unlawfully intercepted), "[t]he disclosure by an investigative or law enforcement officer of the contents of an intercepted communication to IRS revenue agents may constitute 'use' of such contents that is 'appropriate to the proper performance of his official duties'" under the law enforcement use[145] provision.[146] The court additionally found that, given that the disclosure of wiretap materials when testifying in court is permitted pursuant to the testimonial disclosure[147] provision, it would be reasonable to permit disclosure of the contents of testimony to the IRS revenue agents in preparation for the trial.[148]

To fit direct disclosure into the reach of § 2517(2), the SEC and similar civil enforcement agencies could "condition aid in USAO criminal investigations on forthright cooperation by the USAO, including disclosure of wiretap recordings."[149] By doing so, disclosure or use of the wiretaps in this manner would be made in furtherance of the USAO's official duties of criminal investigation and prosecution.[150]

2. *Expressio Unius* Prohibits Such Disclosure

When presented with questions regarding disclosures of wiretaps, some circuits have applied *expressio unius* to interpret Title III as prohibiting all

143. The court permitted the introduction of the wiretaps into evidence based on its interpretation of § 2515—that § 2515 prohibited unlawfully intercepted wiretap materials from being introduced into evidence, not unlawfully *disclosed* wiretap materials. *Id.* at 874.

144. *Id.*

145. *See supra* notes 110–13 and accompanying text.

146. *Fleming*, 547 F.2d at 874 (quoting 18 U.S.C. § 2515 (2012)).

147. *See supra* notes 115–18 and accompanying text.

148. *Fleming*, 547 F.2d at 875.

149. Atkins, *supra* note 22, at 745.

150. *Id.*; *see* 18 U.S.C. § 2517(1)–(2); DOJ MANUAL, *supra* note 97, at 33 ("[I]t is clear from the legislative history and the case law . . . that section 2517 allows the disclosure of Title III information for any legitimate investigative purpose associated with the development of a criminal case . . . .").

disclosures except those expressly permitted by § 2517.[151] Many academics and professionals construe the disclosure provisions similarly.[152]

The Seventh Circuit is one circuit that has followed this approach.[153] In *United States v. Dorfman*,[154] news media (who were not parties to the case) submitted a motion to the district court to unseal sealed exhibits in an ongoing criminal proceeding that contained wiretap materials, so that the media could inspect and copy them.[155] The district judge ruled that most of the sealed exhibits could be unsealed, though the unsealing of some would have to wait until the jury was empaneled.[156] The defendants to the criminal case, whose conversations were intercepted by the wiretaps, appealed the district court's order to the Seventh Circuit on the basis that the unsealing of the exhibits before they were admitted into evidence at trial[157] would violate Title III and the defendants' constitutional right to a fair trial.[158]

In ruling on the appeal, the Seventh Circuit made clear that it was adopting an *expressio unius* approach to interpret the disclosure provisions

151. *See, e.g.*, *In re* Grand Jury, 111 F.3d 1066, 1078 (3d Cir. 1997) ("The statutory structure makes it clear that any interceptions of communications and invasions of individual privacy are prohibited unless expressly authorized in Title III."); *In re* Motion to Unseal Elec. Surveillance Evidence, 990 F.2d 1015, 1018 (8th Cir. 1993) (en banc) (rehearing en banc overruling the 8th Circuit's prior decision that previously undisclosed wiretap evidence could be made available to private civil RICO litigants in some situations and stating that "[w]hen addressing disclosure of the contents of a wiretap, the question is whether Title III specifically *authorizes* such disclosure, not whether Title III specifically prohibits the disclosure, for Title III prohibits all disclosures not authorized therein"); United States v. Underhill, 813 F.2d 105, 107 (6th Cir. 1987) ("Unless there is a specific section of the statute which excepts a particular interception, all willful interceptions of wire and oral communications are prohibited by the [Wiretap] Act."); United States v. Dorfman, 690 F.2d 1230, 1232–33 (7th Cir. 1982).

152. *See* 2 CARR & BELLIA, *supra* note 108, § 7:51; Title III Electronic Surveillance Material and the Intelligence Community, 24 Op. O.L.C. 261, 263 (2000), http://www.justice.gov/sites/default/files/olc/opinions/2000/10/31/op-olc-v024-p0261.pdf [hereinafter OLC Opinion] [http://perma.cc/4RWN-FHCQ].

153. *See Dorfman*, 690 F.2d at 1231. It is noteworthy, however, that the party requesting access was neither a civil enforcement agency nor a party to the case. *See id.*

154. 690 F.2d 1230 (7th Cir. 1982).

155. *Id.* The government had engaged in comprehensive wiretapping of suspects in a scheme to defraud a union's pension fund, and as a result of evidence obtained through these wiretaps, five defendants were ultimately charged with various federal criminal offenses, including bribery of a U.S. Senator. *Id.* The defendants in the case included "senior officers of labor unions and alleged captains of 'organized crime.'" *Id.* The defendants in the criminal case challenged the legality of the government's use of wiretaps to investigate the crimes allegedly committed by the defendants and moved to suppress such evidence in accordance with 18 U.S.C. § 2518(10)(a). *Id.* During an evidentiary hearing on the defendants' motion, the government submitted approximately 200 exhibits containing wiretap materials. *Id.* The district court ultimately found that the government's use of wiretaps to investigate certain crimes was lawful, and the judge ordered the exhibits to be sealed. *Id.*

156. *Id.*

157. In a parenthetical insertion, the Seventh Circuit noted that most of the wiretap exhibits would not be put into evidence at trial. *Id.*

158. *Id.*; *see* U.S. CONST. amend. VI; *supra* Part I.C.2.a (discussing the procedures regarding sealing wiretaps and related materials).

of Title III.[159] The court reasoned that by criminalizing the disclosure of wiretaps in the specific instances outlined in § 2511, yet also expressly permitting certain disclosures in § 2517, "Title III implies that what is not permitted is forbidden . . . though not necessarily under pain of criminal punishment."[160] The court also looked to the legislative history of Title III, namely the "emphasis the draftsmen put on the importance of protecting privacy to the extent compatible with the law enforcement objectives of Title III," and found that given the legislative interest in protecting privacy, Title III should be construed narrowly.[161]

Judge James G. Carr and Professor Patricia L. Bellia adopted the use of *expressio unius* to interpret the disclosure provisions of Title III in their treatise on the law of electronic surveillance.[162] They state, "A prosecutor has no discretion to disregard the restrictions in these provisions or to request or obtain authorization for release that is not within the statutory limitations."[163] However, "[o]nce public disclosure has occurred at a trial, disclosure can be made in other proceedings without regard to the strictures of § 2517."[164] This is because any privacy interests at stake pretrial are eliminated when the information is made public via disclosure during trial, which is generally open to the public.

The DOJ's Office of Legal Counsel (OLC)—the office responsible for providing legal advice to the executive branch of the government—similarly adopted the *expressio unius* approach in a published opinion letter providing guidance on the interpretation of Title III's disclosure provisions.[165] In this letter, the OLC stated that "Title III prohibits every disclosure that it does not explicitly authorize."[166] Likewise, the Criminal Resource Manual published by the DOJ provides that Assistant United States Attorneys should use wiretap materials in accordance with the disclosure requirements of § 2517, including "obtaining all appropriate court orders[] and advising the court of the full scope of the proposed disclosure."[167]

Thus, when determining whether direct disclosures of wiretap materials from the DOJ to the SEC are permitted, a court may construe Title III in accordance with *expressio unius*, as did the Seventh Circuit in *Dorfman* and

159. *Dorfman*, 690 F.2d at 1232; *see also supra* Part I.A.

160. *Dorfman*, 690 F.2d at 1232.

161. *Id.* (citing Gelbard v. United States, 408 U.S. 41, 47–51 (1972)); *see* S. REP. NO. 90-1097, at 66–67 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153–54.

162. 2 CARR & BELLIA, *supra* note 108, § 7:51.

163. *Id.* § 7:33.

164. *Id.*

165. OLC Opinion, *supra* note 152.

166. *Id.* at 272.

167. U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL: CRIMINAL RESOURCE MANUAL § 34, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00034.htm#34 [http://perma.cc/63B2-T5B9]. Recently, however, the DOJ has appeared to recognize the increased debate over Title III's interpretation, as in its Electronic Surveillance Manual, the DOJ notes that "the release of [wiretap materials] for [purposes other than the development of a criminal case] is the subject of dispute." DOJ MANUAL, *supra* note 97.

the OLC in its opinion letter.[168] In such a case, direct disclosure of wiretaps from the DOJ to the SEC would only be permitted if it qualified under the law enforcement disclosure or law enforcement use provisions of § 2517.[169]

3. The Adoption of a Balancing Test

Though the particular question of direct disclosure from the USAO to civil enforcement agencies like the SEC has not been resolved by any court, the Second Circuit has, on numerous occasions, addressed the disclosure provisions with respect to third-party access to wiretapped conversations or their related documents.[170] In addressing these cases, the Second Circuit has consistently rejected the application of *expressio unius* to the disclosure provisions of Title III and has instead held that a failure to explicitly permit something does not necessarily mean that the obverse is true.[171] Indeed, in *In re Application of Newsday, Inc.*,[172] the Second Circuit adopted a two-part balancing test to determine whether disclosure of wiretap materials may be disclosed to a particular third party.[173]

The balancing test first requires the court to consider whether the requesting party would generally have a right of access to the materials, notwithstanding the fact that they may contain wiretaps (or evidence derived therefrom) lawfully obtained pursuant to Title III.[174] The Supreme Court has recognized a general common law "right to inspect and copy public records and documents, including judicial records and documents,"[175] and also recognized that search warrants and affidavits submitted in their support qualify as public documents that are required to be filed with the clerk of the issuing court under Rule 41 of the Federal

168. *See* United States v. Dorfman, 690 F.2d 1230, 1232 (7th Cir. 1982); *see also supra* notes 162–67 and accompanying text.

169. *See Dorfman*, 690 F.2d at 1232; *see also supra* Part II.A.1.

170. *See, e.g.*, *In re* Application of Newsday, Inc., 895 F.2d 74, 76 (2d Cir. 1990) (noting that Title III does not "address the issue of public access to intercepted communications when those communications become part of a public document after having been used by the government in the course of its law enforcement activities"); Nat'l Broadcasting Co. v. U.S. Dep't of Justice, 735 F.2d 51, 53–55 (2d Cir. 1984) (finding that the testimonial disclosure provision does not turn "Title III into a general civil discovery mechanism").

171. *See, e.g.*, SEC v. Rajaratnam, 622 F.3d 159, 173 (2d Cir. 2010) ("[W]e reiterate today that Title III does not prohibit whatever disclosures of lawfully seized communications it does not expressly permit."); *Newsday*, 895 F.2d at 77 (rejecting the contention that § 2517's failure to create a right of public access evidences Congress's intent "to forbid public access by any other means on any other occasion"). *Contra Dorfman*, 690 F.2d at 1232 ("Title III implies that what is not permitted is forbidden."). Rejecting *expressio unius* thus shifts the analysis from whether Title III expressly *permits* a disclosure, to whether Title III expressly *prohibits* a disclosure. *See Rajaratnam*, 622 F.3d at 180 (finding that because the appellants "failed to point [the court] to any case law establishing that Title III prohibits the disclosure of wiretap materials in a situation such as this one," the court should proceed with the *Newsday* balancing test).

172. 895 F.2d 74 (2d Cir. 1990).

173. *See id.* at 79. Though not a direct party to the case, the government took "the position that Title III does not forbid disclosure and that the district court's order should be affirmed." *Id.* at 76.

174. *Id.* at 79.

175. *Id.* at 78 (quoting Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597–98 (1978)).

Rules of Criminal Procedure.[176] The Second Circuit further stated, "The presence of material derived from intercepted communications in the warrant application [did] not change its status as a public document subject to a common law right of access," though its presence may require close review by the judge before the materials are unsealed.[177] The court held that "there is a common law right to inspect what is commanded thus to be filed" where "the warrant has been executed, a plea-bargain agreement has been reached, the government admits that its need for secrecy is over, and the time has arrived for filing the application with the clerk."[178]

The second part of the test requires the court to balance the right of access identified in part one of the test against the privacy interests of the parties whose communications were intercepted, because "the common law right of access is qualified by recognition of the privacy rights of the persons whose intimate relations may thereby be disclosed."[179] In conducting this balancing, courts should consider "whose privacy interests might be infringed, how they would be infringed, what portions of the tapes might infringe them, and what portion of the evidence consisted of the tapes."[180] Additionally, courts should give extra weight to the privacy interests of innocent third parties that may be implicated or harmed by disclosure.[181] In *Newsday*, the Second Circuit found that the district court satisfactorily balanced the privacy interests, given the legitimate public interest in the case, the defendants' guilty pleas, the "mundane business nature" of the wiretaps, and the redactions made to protect the identities of innocent third parties.[182] The Second Circuit was also satisfied that the defendant in the criminal case was provided with a copy of the intercepted communications and found that the defendant had sufficient time to develop objections to the disclosure.[183] As such, the materials could be disclosed without harming any privacy interests.

176. *Id.* at 77; *see* FED. R. CRIM. P. 41(d)(2)(C) ("Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit."); *see also Newsday*, 895 F.2d at 77–79 (comparing the materials sought in the present case to those sought in *Dorfman*, 690 F.2d at 1231—sealed exhibits containing wiretap materials which are not public documents required to be filed in the court's records—and *Times Mirror Co. v. United States*, 873 F.2d 1210, 1219 (9th Cir. 1989)—grand jury records, to which no general right of access have ever been recognized).

177. *Newsday*, 895 F.2d at 79. The court did not address the argument that the press has a constitutional right of access to documents contained in search warrant applications, because the canon of constitutional avoidance requires that courts avoid deciding constitutional issues if judgments can be rendered on some other basis. *Id.* at 75, 78.

178. *Id.* at 79.

179. *Id.*

180. *Id.* (quoting *In re* New York Times Co., 828 F.2d 110, 116 (2d Cir. 1987)).

181. *Id.*

182. *Id.* at 76, 80.

183. *Id.* at 80.

In 2009, the SEC brought a civil action against Raj Rajaratnam,[184] the CEO of Galleon Group whose criminal prosecution marked the first time that wiretaps were used to prosecute securities fraud.[185] As part of its criminal investigation, the DOJ conducted court-authorized wiretaps of phone calls between the various defendants and other parties, the fruits of which were subsequently provided to the defense as part of criminal discovery.[186] After the criminal suit was brought, but before any ruling was made on the legality of the wiretaps, the SEC sought access to the wiretap recordings from the defense as part of discovery in its civil case.[187] The district court approved the request and ordered the defense to produce the materials to the SEC under a protective order that "prohibit[ed] the disclosure of the wiretap recordings to any non-party until, at a minimum, a court of competent jurisdiction had ruled on the [defendants'] suppression motion."[188] The defense appealed.[189]

On appeal, the Second Circuit reiterated *Newsday*'s rejection of *expressio unius* as a means of interpreting the disclosure provisions of Title III.[190] The court likened the present case to *Newsday* because the SEC requested disclosure of Title III materials "incident to, or after," their use under § 2517, which *Newsday* recognized as not addressed by Title III and thus not necessarily prohibited.[191] The Second Circuit then proceeded to conduct the *Newsday* two-part balancing test.[192]

First, the court found that the SEC had an independent right of access to the wiretap materials in the defendants' possession "based on the civil discovery principle of equal information."[193] The court found that failure to permit the SEC to obtain materials in the possession of the defendants would create an "informational imbalance" between the civil litigants, because the defendants would have the benefit of knowing the contents of the wiretaps while the SEC would not.[194] The court found that this "informational imbalance" prejudiced the SEC's preparation for the civil trial and thus "clearly" established the SEC's interest in accessing the materials.[195]

184. Press Release, SEC, SEC Charges Billionaire Hedge Fund Manager Raj Rajaratnam with Insider Trading (Oct. 16, 2009), https://www.sec.gov/news/press/2009/2009-221.htm [http://perma.cc/5H8D-X4C5].

185. SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010).

186. *Id.* at 165.

187. *Id.*

188. *Id.* at 166.

189. *Id.*

190. *Id.* at 176–77.

191. *Id.* at 177 (quoting *In re* Application of Newsday, 895 F.2d 74, 78 (2d Cir. 1990)).

192. *See id.* at 177–78; *see also supra* notes 174–83 and accompanying text (discussing *Newsday*'s two-part balancing test).

193. *Rajaratnam*, 622 F.3d at 180 ("Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation." (quoting Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 540 n.25 (1987))).

194. *Id.* at 175.

195. *Id.* at 184.

However, the Second Circuit found that the district court did not properly balance the SEC's right to the materials against the relevant privacy interests at stake, because the legality of the wiretaps in the criminal case had not been determined.[196] The Second Circuit found that even though Title III does not address disclosures of intercepted calls by defendants to other parties, "[i]t absolutely prohibits . . . the intentional disclosure of the fruits of *unlawful* wiretapping."[197] Thus, if the criminal court were to subsequently determine that the wiretaps were obtained unlawfully, the second prong of the *Newsday* test would be drastically affected because the privacy rights of the individuals involved would have already been found to be "grievously infringed, and further dissemination of conversations that had been illegally intercepted would only compound the injury."[198] The court thus concluded that "[t]he privacy interests at stake prior to a ruling on the legality of interceptions clearly outweigh the SEC's interest in discovery."[199] The Second Circuit also found that the privacy interests of innocent third parties whose communications were intercepted must be addressed before a ruling on disclosure could be made.[200] Because the district court failed to limit the disclosure of the wiretaps to relevant conversations, it erroneously balanced the privacy interests at stake.[201]

B. The Normative Question: Should the DOJ Share Wiretap Materials with the SEC?

The legislature was aware that creating a framework for government-authorized wiretaps could potentially have serious implications for an individual's privacy interests.[202] Thus, when evaluating the scope of Title III, it is important not to lose sight of the first of the dual purposes of its enactment: the protection of individuals' privacy rights.[203] Part II.B begins with a discussion of the benefits of allowing the DOJ to directly disclose the fruits of wiretaps with the SEC. It then discusses the policy issues regarding whether the DOJ *should* be able to directly disclose the fruits of wiretaps with the SEC in light of the privacy interests at stake at various points throughout the course of an investigation.

196. *Id.* at 167–68.
197. *Id.* at 185.
198. *Id.*
199. *Id.* at 187. It has been suggested that it may be unnecessary to wait until the criminal court has ruled on the legality of the interception of the wiretaps, as long as the civil judge in the case makes the determination herself. Atkins, *supra* note 22, at 745.
200. *Rajaratnam*, 622 F.3d at 187.
201. *Id.*
202. *See* S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.
203. *See supra* Part I.C.1 (discussing the legislative history and dual-purpose of Title III).

1. Benefits of Comprehensive Information Sharing Between the DOJ and the SEC

Courts recognize the efficiency of parallel investigations, especially with respect to requests for information.[204] Mary Jo White, current Chairwoman of the SEC, has noted that "the SEC's expertise and extensive cooperation and partnership with the criminal authorities is essential to all-encompassing enforcement of the federal securities laws."[205] She argues that a "robust combination of criminal and regulatory enforcement of the securities laws is not only appropriate, but also critical to deterring securities violators, punishing misconduct, and protecting investors."[206]

But as previously discussed, the strategies used by conspirators of insider trading have increasingly made the crime more difficult to investigate using traditional methods of investigation.[207] For example, the SEC had initially been unable to establish a sufficient case in *SEC v. Rajaratnam*[208] through traditional methods of investigation and thus referred the case to the criminal authorities who could investigate the case using more aggressive techniques.[209]

As the agencies work so closely together—often conducting joint interviews and depositions and sharing notes and strategies—"[i]t is certainly anomalous that the SEC can't get the [wiretap materials] from the Department of Justice, its ally."[210] Professor Dan Richman has said, "It would be extremely odd [to] have an adjudication of the civil case without evidence that could emerge in a subsequent criminal case."[211]

2. Concerns Regarding Increased Sharing Among Agencies

One of the cases leading up to the enactment of Title III emphasized the seriousness of the implications that wiretaps have on individuals' privacy interests: "Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[212] When personal communications are intercepted via wiretaps, privacy interests of innocent third parties are often

204. *See Panel I*, *supra* note 57 (discussing the reasoning behind the legality of parallel investigations).

205. White, *supra* note 15.

206. *Id.*

207. *See* Herzinger & Mermelstein, *supra* note 59, at 32.

208. 622 F.3d 159 (2d Cir. 2010).

209. *See* Herzinger & Mermelstein, *supra* note 59, at 32 ("With traditional tactics, he escaped prosecution. With wiretaps, he was convicted, fined $10 million, ordered to forfeit $53.8 million, and sentenced to 11 years in federal prison. Rajaratnam was also ordered to pay a $92.8 million civil penalty to the SEC, the largest ever in an insider trading case."). *But see Panel II*, *supra* note 60 (suggesting that the criminal case against Rajaratnam might have been successful even without the wiretapped conversations).

210. Jonathan Stempel, *ANALYSIS—Galleon Wiretaps Big for White-Collar Crime Cases*, REUTERS (Jan. 27, 2010, 9:12 PM), http://in.reuters.com/article/2010/01/27/idINIndia-45739920100127 [http://perma.cc/3MR5-MK8K].

211. *Id.*

212. Berger v. New York, 388 U.S. 41, 63 (1967).

implicated.[213] Every year, the personal communications of hundreds of thousands of people are intercepted by the government, and approximately 80 percent are deemed "not incriminating."[214] Phone lines authorized for interception by the government may be used for lawful, intimate conversations with loved ones, or calls involving other deeply personal information. This section first discusses the varying levels of privacy interests at stake at different stages of investigations and then turns to the tools available to courts to protect privacy.

a. The Varying Privacy Implications over the Course of an Investigation

In *Bartnicki v. Vopper*,[215] the Supreme Court stated, "[T]he disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself."[216] Similarly, the Second Circuit has found that once the wiretaps have been disclosed and listened to by another party, the privacy rights of the parties to the recorded conversations "will forever have been harmed by the very act of exposure."[217] Essentially, once a disclosure has been made and the privacy rights have been violated, there is no going back.[218] However, the privacy interests implicated by disclosure of wiretaps vary depending on the stage of the criminal investigation or prosecution.[219] For example, once wiretap materials have been made public in court, any remaining privacy interests in such materials are weak because information that is public is no longer private.[220] Indeed, in *Fleming*, the Fifth Circuit found that privacy interests were weak because the intercepted communications had already been introduced in open court during prior criminal proceedings.[221] Additionally, in *Newsday*, the Second Circuit found that where the "warrant [had] been executed, a plea-bargain

213. *See generally* Brief for Electronic Privacy Information Center (EPIC) as Amicus Curiae Supporting Appellants at 9, SEC v. Rajaratnam, 622 F.3d 159 (2d Cir. 2010) (Nos. 10-462-cv(L), 10-464-cv(CON)), 2010 WL 2584231 [hereinafter EPIC Brief].

214. *Id.* at 6–8.

215. 532 U.S. 514 (2001).

216. *Id.* at 533.

217. *Rajaratnam*, 622 F.3d at 170; *see* Mark B. Sheppard & Erin C. Dougherty, *"Tapping" into Wall Street*, 26 CRIM. JUST. 20, 22 (2012).

218. *See Rajaratnam*, 622 F.3d at 170.

219. *See, e.g.*, *id.* at 171 (discussing the issues regarding timing of the parallel proceedings, including the fact that the legality of the wiretaps was not yet adjudicated in the criminal case parallel to the SEC proceeding); *In re* Application of Newsday, 895 F.2d 74, 78 (2d Cir. 1990) (discussing cases in the Ninth, Eighth, and Fourth Circuits addressing varying rights of access to materials at differing stages of an investigation or prosecution).

220. *See* Fleming v. United States, 547 F.2d 872, 874 (5th Cir. 1977); *supra* note 164 and accompanying text.

221. *Fleming*, 547 F.2d at 874. In *Griffin v. United States*, the petitioners argued that they retained a privacy interest in the wiretap materials disclosed to the IRS prior to the admission of wiretap evidence in the criminal trial, but the Fifth Circuit rejected the argument. 588 F.2d 521, 525 (5th Cir. 1979). Instead, the court found that because the underlying facts of the case were identical to those in *Fleming*, "[t]he privacy interests implicated in *Fleming* and those in the present case do not differ in any significant respect," and the statute must thus be construed as it was in *Fleming*. *Id.*

agreement [had] been reached, the government admit[ted] that its need for secrecy is over, and the time [had] arrived for filing the application with the clerk," the privacy interests at stake in a search warrant affidavit containing evidence derived from wiretap materials no longer weighed in favor of nondisclosure.[222]

However, in cases at the opposite end of the spectrum—where not only have the wiretap materials not been introduced into evidence, but the government has not even indicted targeted individuals—the privacy interests of the individuals' conversations are likely to be very strong.[223] *Times Mirror Co. v. United States*[224] found that the privacy interests of individuals named in the materials sought—warrants and their supporting affidavits—would be seriously compromised "if the public had access to warrant materials before indictments [were] returned."[225] The court expressed concern that disclosing the identities of investigative targets before an indictment has been returned would suggest to the public that such individuals may be guilty of a crime; but until such individuals are actually indicted, they would lack access to the appropriate forum to challenge such accusations.[226]

Similarly, disclosures of wiretap materials prior to their lawful introduction during a public proceeding may have serious privacy implications in the event that the wiretaps are subsequently found to have been intercepted unlawfully.[227] This issue arose in the *Rajaratnam* cases. In the criminal case, Rajaratnam and his codefendant sought to suppress the wiretaps and evidence derived therefrom on the basis that they were unlawfully intercepted.[228] However, before any ruling was made on the legality of the interceptions, the SEC sought access to the wiretaps from the defendants as part of discovery in the SEC's civil case.[229] In addition to objecting to the SEC's turnover request, the defense also motioned for the court hearing the criminal case to issue a protective order to prevent the USAO from sharing the fruits of wiretaps with the SEC.[230] The defense argued that disclosure of the wiretaps before the court ruled on their legality would "irreparably compromis[e] their personal privacy rights, their statutorily protected privacy rights under Title III as 'aggrieved persons,' and their constitutional rights under the Fourth, Fifth, and Sixth Amendments."[231] Like the targets of investigations in the pre-indictment stages, innocent third parties whose conversations have been intercepted as

222. *Newsday*, 895 F.2d at 79.
223. *See id.* (discussing Times Mirror Co. v. United States, 873 F.2d 1210 (9th Cir. 1989)).
224. 873 F.2d 1210 (9th Cir. 1989).
225. *Id.* at 1218. Note that the materials sought in *Times Mirror Co.* were not wiretap materials, but sealed affidavits in support of an application for a search warrant. *Id.*
226. *Id.* at 1216.
227. *See* SEC v. Rajaratnam, 622 F.3d 159, 185–87 (2d Cir. 2010).
228. *Id.*
229. *Id.* at 166–67; *see also* Memorandum, *supra* note 128, at 2.
230. *See generally* Memorandum, *supra* note 128.
231. *Id.* at 6.

part of the wiretaps of the targets also cannot meaningfully advocate for the preservation of their privacy, regardless of the stage of the investigation.[232]

b. Other Factors Weighing in the Balance

The procedural requirements of Title III arguably help to assuage issues regarding privacy.[233] When applying for authorization to conduct wiretaps, the government must explain whether traditional methods of investigation have been attempted, or why they likely would be unsuccessful.[234] Patrick Carroll, an FBI Agent responsible for investigations into securities fraud and white collar crime, has acknowledged the "tremendous" intrusions into privacy posed by the use of wiretaps.[235] As such, Agent Carroll has said that his team uses wiretapping "when [they] have exhausted all other techniques and . . . believe it is the right thing to do to disrupt and dismantle an organization."[236] The requirement for minimization of conversations irrelevant to the investigation also serves to protect the privacy interests of innocent third parties whose conversations are intercepted in the course of an investigation.[237]

Additional tools are available to the courts to ensure that privacy interests are protected.[238] Courts may grant protective orders to eliminate privacy concerns and prohibit further disclosure of wiretap materials to any additional parties—a precaution the Southern District of New York took when it first addressed the SEC's request for the wiretap materials as part of civil discovery.[239] As noted in an amicus brief in support of Rajaratnam's appeal of the civil discovery order, "the principles of search minimization and relevance, as well as the Fourth Amendment, limit the state's use of and access to these recordings."[240]

Furthermore, there is a key distinction between many of the cases that have addressed the interpretation of the disclosure provisions and the present question regarding direct disclosure: the former cases often involved public disclosure of wiretap materials, whereas disclosure in the present hypothetical would be to a few professionally interested

232. *See* EPIC Brief, *supra* note 213, at 3–4.

233. *See supra* Part I.C.2.a (discussing the application and minimization requirements for wiretaps).

234. *See supra* Part I.C.2.a (discussing the application and minimization requirements for wiretaps).

235. Ailsa Chang, *Wall Street Wiretaps: Investigators Use Insiders' Own Words to Convict Them*, NPR (Dec. 26, 2012, 3:25 AM), http://www.npr.org/2012/12/26/168021457/wall-street-wiretaps-investigators-use-insiders-own-words-to-convict-them [http://perma.cc/5PBW-AWR6].

236. *Id.*

237. *See supra* Part I.C.2.a.

238. *See* SEC v. Rajaratnam, 622 F.3d 159, 166 (2d Cir. 2010) (noting that the district court had entered a protective order prohibiting the disclosure of wiretap recordings to any nonparty).

239. *See* SEC v. Galleon Mgmt., 683 F. Supp. 2d 316, 319 (S.D.N.Y. 2010), *vacated*, *Rajaratnam*, 622 F.3d 159 (granting the SEC's motion for disclosure of the wiretap materials in part).

240. EPIC Brief, *supra* note 213, at 9.

government parties.[241] Indeed, the court in *Dorfman* acknowledged that privacy interests are substantially implicated when wiretap materials are disclosed "to the world at large," as opposed to when a handful of law enforcement officers and a district judge know the contents of wiretapped conversations.[242]

III. SHARING IS CARING, IT COULD BE FUN

If there is one clear conclusion that comes out of the above cases, it is that there is serious disagreement about the proper way to interpret the disclosure provisions of Title III.[243] But what principles can be gleaned from these cases and applied to the question of whether direct disclosure of wiretaps from the USAO to the SEC is permissible? Part III.A argues that the proper way to interpret Title III is through an approach that incorporates aspects and principles of both the Seventh Circuit's holding in *Dorfman* and the Second Circuit's holdings in *Rajaratnam* and *Newsday*. Part III.B then outlines a recommended procedure that Congress should enact to achieve the dual purposes of Title III.

A. A Blended Approach to Interpreting Title III

First, it is clear that the disclosure of materials from the USAO to the SEC is neither explicitly prohibited nor explicitly permitted by Title III.[244] However, an analysis of the structure of Title III as a whole shows that such a blanket prohibition of disclosures does exist, though not necessarily under pain of criminal law. Second, notwithstanding the fact that permitted disclosures are not required to be found within the boundaries of Title III, the SEC officers may have a strong case either to be considered "law enforcement officers" within the definition of the Wiretap Act, given the use of formal task forces targeting financial crime, or for the DOJ's disclosure of wiretap materials to fall within the boundaries of a permitted disclosure under § 2517(2)'s law enforcement use provision.

Section 2511—the provision outlining the expressly prohibited disclosures—does not explicitly prohibit *all* disclosures of wiretaps, though the legislative history indicates that perhaps it was intended to do so.[245] Rather, the specifically enumerated disclosures in § 2511 are those that are subject to criminal penalties of fines and/or imprisonment of up to five years.[246] Furthermore, nowhere does Title III state that § 2511 outlines the

241. *See, e.g.*, *In re* Application of Newsday, Inc., 895 F.2d 74 (2d Cir. 1990) (addressing disclosure to the news media); United States v. Dorfman, 690 F.2d 1230, 1234 (7th Cir. 1982) (same).

242. *Dorfman*, 690 F.2d at 1234.

243. *See supra* Part II.A (outlining the conflicting interpretations of Title III's disclosure provisions).

244. *See supra* Part I.C.2.b (discussing the explicitly prohibited disclosures); *see also supra* Part II.A.3.

245. *See supra* notes 102–04 and accompanying text.

246. *See supra* Part I.C.2.b.

only prohibited disclosures, nor that § 2517 outlines the *only* permitted disclosures.[247]

In *Dorfman*, the Seventh Circuit held that § 2511 is not the sole source of prohibitions of interceptions and disclosures, but rather that the enumeration of certain permitted activities in § 2517 creates a negative implication that those disclosures that are not expressly permitted are thus prohibited.[248] Though the court was correct in emphasizing that § 2511 is the sole source of Title III's criminalizing authority, not the exclusive source of prohibited disclosures, its use of *expressio unius* to establish the universe of permitted interceptions and disclosures was incorrect.[249] The structure and legislative history of Title III does not support the application of *expressio unius*, and thus the implication that additional restrictions stem from the enumeration of certain permitted disclosures in § 2517 is erroneous.[250] As discussed earlier, the Supreme Court has held that the *expressio unius* canon only applies if "it is fair to suppose that Congress considered the unnamed possibility and meant to say no to it."[251] This question can be addressed in two ways: narrowly, by asking whether Congress considered the specific disclosure in question—from the USAO to the SEC—and meant to say no to it; or broadly, by asking whether Congress considered other types of disclosures—i.e., disclosures of wiretap materials as part of civil discovery or pursuant to a First Amendment right of access—and meant to say no to them.[252] Given that Title III was enacted to assist in the investigation of organized crime, it is unlikely that in 1968 Congress considered this particular type of disclosure from the USAO to the SEC.[253]

When applying the canon of constitutional avoidance, however, it becomes easier to assume that Congress did not intend Title III to be construed using *expressio unius*.[254] As the district court noted in *Newsday*, a strict *expressio unius* interpretation may have unconstitutional implications in the event that the media is found to have a First Amendment right to access wiretap materials.[255] Thus, in accordance with the canon of

247. *See supra* Part I.C.2.b–c (discussing the expressly prohibited and expressly permitted disclosures).

248. *See supra* Part II.A.2 (suggesting that additional interceptions and disclosures may be forbidden, "though not necessarily under pain of criminal punishment").

249. *See supra* Part II.A.2.

250. *See supra* Parts I.C.1, II.A.2.

251. *See supra* note 36 and accompanying text.

252. *See supra* notes 177–78 and accompanying text.

253. *See supra* Part I.C.1. Though section 10(b) of the Exchange Act and Rule 10b-5 existed before the enactment of the Wiretap Act in 1968, insider trading did not achieve "wide-spread notoriety [until] the 1980s." Thomas C. Newkirk, Assoc. Dir., SEC Div. of Enf't, Insider Trading—A U.S. Perspective: Speech by SEC Staff at the 16th International Symposium on Economic Crime (Sept. 19, 1998), https://www.sec.gov/news/speech/speecharchive/1998/spch221.htm#FOOTNOTE_25 [http://perma.cc/9KSJ-XANR].

254. *See supra* Part I.A (discussing the canons of construction).

255. *See supra* note 177 (noting that the district court held that the media may have a qualified constitutional right of access to the court documents). The Second Circuit decided the case based on a potential common law right of access, in accordance with the canon of constitutional avoidance. *See supra* note 177.

constitutional avoidance, Title III should not be construed in a manner that would raise constitutional questions, and courts should reject *expressio unius* in favor of a more flexible approach, such as the Second Circuit's two-part balancing test.[256]

B. A Balanced Proposal

The per curiam opinion in *Fleming* accurately described Title III—that it "is not a model of clarity."[257] To address this lack of clarity and to ensure that both of the dual purposes of Title III are well supported, Congress should amend the Wiretap Act to create an explicit ex parte or in camera process through which the DOJ can request court approval to share the fruits of wiretaps with civil enforcement agencies.

First, such a request for disclosure should come from the DOJ rather than the civil enforcement agency itself because the DOJ is in a better position to say whether the wiretaps contain useful information, being the party that presumably lawfully intercepted them. The DOJ should be required to submit an application to the court similar to the application it submits when requesting the initial authorization to conduct wiretaps.[258] In this application, the DOJ would need to identify the civil enforcement agency to which disclosure would be made, provide details regarding the particular regulatory violations believed to be evidenced by the wiretaps, describe the intercepted conversations that are believed to evidence such violations, and explain how such disclosure request came about (e.g., the SEC approached the DOJ after the SEC read an unsealed indictment suggesting that wiretaps were used to uncover evidence of securities fraud; the DOJ came across evidence of substantial regulatory violations and, on its own volition, would like to assist the SEC with an enforcement action). The purpose of this last requirement is to assist the court in determining whether the DOJ's wiretaps were merely a subterfuge for the civil enforcement action.

Disclosures should be limited in scope to conversations relevant to any potential agency investigation. Additionally, Congress may want to consider prohibiting the DOJ from disclosing actual copies of the wiretaps and instead limit permissible disclosure to transcripts of the relevant recordings or additional evidence derived therefrom. Furthermore, all disclosures should be made under a protective order that limits the receiving agency's ability to use or disclose the wiretap materials.

The disclosure framework should also include a recordkeeping component to keep track of all evidence that the agency derives from the wiretap materials. Then, if a court later finds that the wiretaps were unlawfully intercepted, this recordkeeping component would enable the SEC to easily identify what evidence may have been derived from unlawful wiretaps and would thus likely be inadmissible.

256. *See supra* notes 174–83 and accompanying text.
257. Fleming v. United States, 547 F.2d 872, 873 (5th Cir. 1977).
258. *See supra* notes 94–96 and accompanying text.

Defendants and other aggrieved parties should be afforded the same rights to suppress such evidence if it is ever introduced during a court proceeding.

CONCLUSION

Given the increase of insider-trading prosecutions, the recognition of wiretaps as useful tools in investigating insider trading, and the increase in parallel investigations to combat such crimes, the unanswered question of whether the DOJ can share the fruits of wiretaps with the SEC is sure to arise again. The circuit courts employing *expressio unius* have applied the tool incorrectly, because it is not necessarily "fair to suppose that Congress considered the unnamed possibility and meant to say no to it."[259] The balancing test adopted by other circuits balances the dual purposes of the Wiretap Act in a more efficient way, by ensuring that both the law enforcement and privacy protection objectives are fulfilled. Still, the uncertainty of the most appropriate interpretation lingers, and it will do so until either the Supreme Court or Congress does something about it.

Efficiency in investigation and prosecution calls for the DOJ to be able to share the fruits of wiretaps with their civil enforcement counterparts in the SEC. Though this may be accomplished relatively easily by amending the definition of "investigative or law enforcement officer" to include SEC officers and attorneys,[260] the lack of clarification and need to protect privacy interests may warrant additional changes, such as those outlined in this Note.

259. *See supra* note 36 and accompanying text.
260. *See supra* notes 106–09 and accompanying text.