

# 10-462-cv(L)

## 10-464-cv(CON)

---

---

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT



SECURITIES and EXCHANGE COMMISSION,

*Plaintiff-Appellee,*

*v.*

RAJ RAJARATNAM and DANIELLE CHIESI,

*Defendants-Appellants,*

*(Additional Caption on Reverse)*

---

*On Appeal from the United States District Court  
for the Southern District of New York*

---

**BRIEF FOR DEFENDANTS-APPELLANTS  
RAJ RAJARATNAM AND DANIELLE CHIESI**

---

Robert H. Hotz, Jr.  
Samidh Guha

AKIN GUMP STRAUSS HAUER  
& FELD LLP  
One Bryant Park  
New York, New York 10022  
212-872-1028

John M. Dowd  
Patricia A. Millett  
Terence J. Lynam  
William E. White  
Kevin R. Amer  
Issaac J. Lidsky  
Anne J. Lee

AKIN GUMP STRAUSS HAUER & FELD LLP  
1333 New Hampshire Avenue, NW  
Washington, DC 20036  
202-887-4000

*Attorneys for Defendant-Appellant  
Raj Rajaratnam*

---

---

*(Additional Counsel on Reverse)*

---

---

and

GALLEON MANAGEMENT, LP, RAJIV GOEL, ANIL KUMAR,  
MARK KURLAND, ROBERT MOFFAT, NEW CASTLE FUNDS LLC,  
ROOMY KHAN, DEEP SHAH, ALI T. FAR, CHOO-BENG LEE,  
FAR & LEE LLC, SPHERIX CAPITAL LLC, ALI HARIRI, ZVI GOFFER,  
DAVID PLATE, GAUTHAM SHANKAR,  
SCHOTTENFELD GROUP LLC, STEVEN FORTUNA,  
S2 CAPITAL MANAGEMENT, LP,

*Defendants.*

---

---

Alan R. Kaufman  
James M. Keanelly  
Thomas B. Kinzler

KELLEY DRYE & WARREN, LLP  
101 Park Avenue  
New York, New York 10178  
212-808-7800

*Attorneys for Defendant-Appellant  
Danielle Chiesi*

## TABLE OF CONTENTS

TABLE OF CONTENTS .....	i
TABLE OF AUTHORITIES .....	iii
JURISDICTIONAL STATEMENT .....	x
STATEMENT OF THE ISSUES PRESENTED FOR REVIEW .....	xii
STATEMENT OF THE CASE.....	1
STATEMENT OF LEGAL AND FACTUAL BACKGROUND.....	2
A.    Constitutional And Statutory Framework .....	2
B.    Factual and Procedural Background .....	8
SUMMARY OF ARGUMENT.....	13
ARGUMENT .....	17
I. THIS COURT HAS JURISDICTION UNDER THE COLLATERAL ORDER DOCTRINE.....	17
A.    Standard of Review .....	17
B.    The <i>Gerena</i> Decision Correctly Establishes Jurisdiction.....	17
C. <i>Gerena</i> Is Consistent with <i>Mohawk</i> .....	25
II. TITLE III AND THE CONSTITUTION FORBID THE MASS DISCLOSURE OF UNTESTED WIRETAP INTERCEPTS IN CIVIL DISCOVERY .....	27
A.    Standard of Review .....	27
B.    Title III’s Strict Textual Limitations Protecting Privacy And Strong Presumption Against Disclosure Foreclose The Compelled Civil Discovery Of Wiretap Materials From Criminal Defendants .....	28
1. <i>The Order Is Presumptively Invalid</i> .....	29
2. <i>Title III’s Text Forecloses Compelled Discovery</i> .....	31
3. <i>The Disclosure Order Lacks Support in Precedent and                 Logic</i> .....	39
a.    The cases cited by the SEC are inapt.....	39
b.    There is no relevant informational imbalance .....	41
4. <i>Release of the Wiretaps Would Significantly Harm the                 Defendants’ Privacy and Fair Trial Rights</i> .....	46
III. IN THE ALTERNATIVE, A WRIT OF MANDAMUS SHOULD BE GRANTED.....	49
A.    The Order Was A Clear Abuse Of Discretion That Cannot Otherwise Be Remedied.....	49

B.    Supervisory Mandamus Is Warranted .....	52
CONCLUSION .....	55
ADDENDUM	
U.S. Constitution, amendment IV .....	1a
18 U.S.C. §§ 2510-2522 .....	2a
Federal Rule of Civil Procedure 26 .....	25a

## TABLE OF AUTHORITIES

### CASES

<i>American Friends Serv. Comm. v. Webster</i> , 720 F.2d 29 (D.C. Cir. 1983) .....	6
<i>Anthony v. United States</i> , 667 F.2d 870 (10th Cir. 1981).....	25
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001).....	<i>passim</i>
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	<i>passim</i>
<i>Berry v. Funk</i> , 146 F.3d 1003 (D.C. Cir. 1998) .....	35
<i>Boothe v. Hammock</i> , 605 F.2d 661 (2d Cir. 1979).....	27
<i>Certain Interested Individuals v. Pulitzer Publ’g Co.</i> , 895 F.2d 460 (8th Cir. 1990).....	35
<i>Chandler v. United States Army</i> , 125 F.3d 1296 (9th Cir. 1997).....	35
<i>Chase Manhattan Bank, N.A. v. Turner &amp; Newell, PLC</i> , 964 F.2d 159 (2d Cir. 1992).....	54
<i>Cheney v. U.S. District Court</i> , 542 U.S. 367 (2004).....	44, 49
<i>Cohen v. Beneficial Industrial Loan Corp.</i> , 337 U.S. 541 (1949).....	<i>passim</i>
<i>Dalia v. United States</i> , 441 U.S. 238 (1979).....	2

<i>Doe v. Chao</i> , 540 U.S. 614 (2004).....	38
<i>Douglas Oil Co. of California v. Petrol Stops Nw.</i> , 441 U.S. 211 (1979).....	44
<i>European Cmty. v. RJR Nabisco, Inc.</i> , 424 F.3d 175 (2d Cir. 2005) (Sotomayor, J.).....	27
<i>Forsyth v. Barr</i> , 19 F.3d 1527 (5th Cir. 1994).....	35
<i>Fultz v. Gilliam</i> , 942 F.2d 396 (6th Cir. 1991).....	22, 29, 30
<i>Gelbard v. United States</i> , 408 U.S. 41 (1972).....	3, 4,
<i>In re Agent Orange Prod. Liability Litig.</i> , 517 F.3d 76 (2d Cir. 2008).....	27
<i>In re Application of NBC</i> , 735 F.2d 51 (2d Cir. 1984).....	<i>passim</i>
<i>In re Application of the New York Times Co. to Unseal Wiretap &amp; Search Warrant Materials</i> , 577 F.3d 401 (2d Cir. 2009).....	<i>passim</i>
<i>In re Application of Newsday, Inc.</i> , 895 F.2d 74 (2d Cir. 1990).....	39, 40
<i>In re Fitch, Inc.</i> , 330 F.3d 104 (2d Cir. 2003) (per curiam).....	28
<i>In re Globe Newspaper Company</i> , 729 F.2d 47 (1st Cir. 1984).....	23
<i>In re Grand Jury</i> , 111 F.3d 1066 (3d Cir. 1997).....	30

<i>In re High Fructose Corn Syrup Antitrust Litigation</i> , 216 F.3d 621 (7th Cir. 2000).....	41
<i>In re New York Times Co.</i> , 828 F.2d 110 (2d Cir. 1987), <i>cert. denied</i> , 485 U.S. 977 (1988).....	17, 20, 24
<i>In re Sims</i> , 534 F.3d 117 (2d Cir. 2008).....	53
<i>In re von Bulow</i> , 828 F.2d 94 (2d Cir. 1987).....	<i>passim</i>
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	<i>passim</i>
<i>Koon v. United States</i> , 518 U.S. 81 (1996).....	28
<i>Lam Lek Chong v. Drug Enforcement Admin.</i> , 929 F.2d 729 (D.C. Cir. 1991) .....	30
<i>Melzer v. Bd. of Educ.</i> , 336 F.3d 185 (2d Cir. 2003).....	28
<i>Mohawk Industries, Inc. v. Carpenter</i> , 130 S. Ct. 599 (2009).....	<i>passim</i>
<i>Morrison v. Olson</i> , 487 U.S. 654 (1988).....	37
<i>New York State Nat’l Org. for Women v. Terry</i> , 886 F.2d 1339 (2d Cir. 1989).....	50
<i>Nix v. O’Malley</i> , 160 F.3d 343 (6th Cir. 1998).....	29
<i>Orange County Water Dist. v. Unocal Corp.</i> , 584 F.3d 43 (2d Cir. 2009).....	54

<i>OSRecovery, Inc. v. One Groupe Int’l, Inc.</i> , 462 F.3d 87 (2d Cir. 2006).....	51
<i>Providence Journal Co. v. FBI</i> , 602 F.2d 1010 (1st Cir. 1979).....	48
<i>Richardson-Merrell, Inc. v. Koller</i> , 472 U.S. 424, 430-431 (1985).....	17
<i>San Filippo v. United States Trust Co.</i> , 737 F.2d 246 (2d Cir. 1984), <i>cert. denied</i> , 470 U.S. 1035 (1985).....	19
<i>Schlagenhauf v. Holder</i> , 379 U.S. 104, 110-111 (1964).....	51
<i>SEC v. Cutillo et. al</i> , No. 1:09-cv-9208 (Sullivan, J.) .....	9
<i>S.E.C. v. Galleon Mgmt., LP</i> , No. 09-cv-8811, ___ F. Supp. 2d ___, 2010 WL 445068 (S.D.N.Y. Feb. 9, 2010).....	iii
<i>SEC v. Glotzer</i> , 374 F.3d 184 (2d Cir. 2004).....	53
<i>Smith v. Lipton</i> , 990 F.2d 1015 (8th Cir. 1993) (en banc).....	29
<i>Stein v. KPMG, LLP</i> , 486 F.3d 753 (2d Cir. 2007).....	49, 51
<i>Swint v. Chambers County Comm’n</i> , 514 U.S. 35 (1995).....	18
<i>Union of Needletrades, Indus. &amp; Textile Employees, AFL-CIO, CLC v. Immigration &amp; Naturalization Serv.</i> , 336 F.3d 200 (2d Cir. 2003).....	27
<i>United Kingdom v. United States</i> , 238 F.3d 1312 (11th Cir. 2001).....	29



<i>United States v. Andreas</i> , 150 F.3d 766 (7th Cir. 1998).....	24, 25
<i>United States v. Calandra</i> , 414 U.S. 338 (1974).....	22
<i>United States v. Cianfrani</i> , 573 F.2d 835 (3d Cir. 1978).....	30
<i>United States v. Coppa</i> , 267 F.3d 132 (2d Cir. 2001).....	53
<i>United States v. Demeritt</i> , 196 F.3d 138 (2d Cir. 1999).....	36
<i>United States v. Dorfman</i> , 690 F.2d 1230 (7th Cir. 1982).....	24, 26, 30, 41
<i>United States v. Far</i> , No. 09-cr-1009 (S.D.N.Y.).....	9
<i>United States v. Fleming</i> , 547 F.2d 872 (5th Cir. 1977).....	40, 41
<i>United States v. Gerena</i> , 869 F.2d 82 (2d Cir. 1989).....	<i>passim</i>
<i>United States v. Giordano</i> , 158 F. Supp. 2d 242 (D. Conn. 2001).....	<i>passim</i>
<i>United States v. Goffer, et al.</i> No. 10-cr-0056 (S.D.N.Y.).....	9
<i>United States v. Huss</i> , 482 F.2d 38 (2d Cir. 1973).....	21, 28, 38
<i>United States v. Lee</i> , No. 09-cr-0972 (S.D.N.Y.) (Castel, J.) .....	9

<i>United States v. Marion</i> , 535 F.2d 697 (2d Cir. 1976).....	29
<i>United States v. Masciarelli</i> , 558 F.2d 1064 (2d Cir. 1977).....	36
<i>United States v. Miller</i> , 14 F.3d 761 (2d Cir. 1994).....	26, 27
<i>United States v. Nixon</i> , 418 U.S. 683 (1974).....	44
<i>United States v. Rajaratnam</i> , 09 CR 1184 (RJH) .....	46
<i>United States v. Ricco</i> , 566 F.2d 433 (2d Cir. 1977).....	35
<i>United States v. Rood</i> , 281 F.3d 353 (2d Cir. 2002).....	28
<i>United States v. Sells Eng'g</i> , 463 U.S. 418 (1983).....	44, 45
<i>United States v. United States Dist. Court for Eastern Dist. of Mich.</i> , 407 U.S. 297 (1972).....	21
<i>United States v. White</i> , 237 F.3d 170 (2d Cir. 2001).....	17
<i>Wills v. Amerada Hess Corp.</i> , 379 F.3d 32 (2d Cir. 2004) (Sotomayor, J.) .....	28
<i>Zweibon v. Mitchell</i> , 516 F.2d 594 (D.C. Cir. 1975) .....	21, 26

## STATUTES AND REGULATIONS

15 U.S.C. § 77 .....	iii, 1
----------------------	--------

15 U.S.C. § 78.....	iii, 1, 3
17 C.F.R. § 240.10b-5 .....	1
18 U.S.C. § 1348.....	3
18 U.S.C. § 2510.....	<i>passim</i>
18 U.S.C. § 2511 .....	<i>passim</i>
18 U.S.C. § 2515.....	5
18 U.S.C. § 2516.....	<i>passim</i>
18 U.S.C. § 2517.....	<i>passim</i>
18 U.S.C. § 2518.....	<i>passim</i>
28 U.S.C. § 511 .....	7
28 U.S.C. § 512.....	iii, 7
28 U.S.C. § 1291 .....	17
28 U.S.C. § 1292.....	1, 12
USA PATRIOT ACT, Pub. L. No. 107-56, 115 Stat. 272 (2001) .....	7

#### **OTHER AUTHORITIES**

Fed. R. App. P. 26.....	33
Prepared Remarks for Preet Bharara, U.S. Attorney, S.D.N.Y., October 16, 2009 .....	46
Off. Legal Counsel, <i>Best Practices for OLC Opinions</i> 1 (May 16, 2005) .....	7
Op. Off. Legal Counsel, <i>Sharing Title III Electronic Surveillance Materials with the Intelligence Community</i> , 2000 WL 33716983 (Oct. 17, 2000).....	6, 30, 31

## JURISDICTIONAL STATEMENT

The district court (Rakoff, J.) had jurisdiction over this case arising under Section 20(b) of the Securities Act of 1933 and Section 21(d) of the Securities Exchange Act of 1934, pursuant to 15 U.S.C. §§ 77t(b), 77t(d), 77v(a), 78u(d), 78u(e), and 78aa, and 28 U.S.C. § 1331. On February 9, 2010, the district court issued an order requiring the disclosure of sealed wiretap materials in civil discovery by February 15, 2010. *S.E.C. v. Galleon Mgmt., LP*, No. 09-cv-8811, \_\_\_ F. Supp. 2d \_\_\_, 2010 WL 445068 (S.D.N.Y. Feb. 9, 2010). The appellants/petitioners filed a timely notice of appeal and a petition for a writ of mandamus on February 11, 2010.

As explained in Argument Section I, *infra*, this Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291; *Cohen v. Beneficial Industrial Loan Corp.*, 337 U.S. 541 (1949); and *United States v. Gerena*, 869 F.2d 82 (2d Cir. 1989). This Court has jurisdiction to issue a writ of mandamus under 28 U.S.C. § 1651(a).

## STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

The district court issued an order compelling the immediate disclosure to the Securities and Exchange Commission and fourteen private civil litigants of 18,150 sealed wiretaps recording the private conversations of more than 550 individuals. The court ordered that release prior to any determination of the intercepts' lawfulness in a motion to suppress, prior to the separate statutory review required by 18 U.S.C. § 2517(5), prior to the wiretaps' disclosure in a criminal proceeding, prior to the conclusion of the pending criminal trial, and without the participation of the judge with jurisdiction over the sealed wiretaps. The issues presented for review are:

1. Whether this Court should continue to adhere to its prior decision in *United States v. Gerena*, 869 F.2d 82 (2d Cir. 1989), and exercise jurisdiction under the collateral order doctrine over the district court's disclosure order because Congress's overriding concern for privacy and the fairness of both the civil and criminal trials cannot be protected if review awaits a final judgment.

2. Whether, notwithstanding the narrowly cabined disclosure provisions of the federal wiretap statute that deny the SEC the authority to obtain wiretaps for insider trading investigations, a court that lacks jurisdiction over the sealed wiretaps may order the wholesale release of more than 18,000 intercepted telephone calls to the SEC and fourteen private litigants as part of routine civil

discovery, prior to a determination of the intercepts' lawfulness, prior to their authorized disclosure under Title III, and prior to the conclusion of the criminal proceeding in which the wiretaps are sealed.

3. Whether issuance of a writ of mandamus is warranted because the district court clearly abused its discretion in adopting an unprecedented rule of civil discovery that (i) contravenes plain statutory text and settled caselaw, (ii) implicates profound privacy and fair trial interests that cannot be vindicated meaningfully post-judgment, and (iii) has far reaching consequences for the administration of justice.

## **STATEMENT OF THE CASE**

On October 16, 2009, the United States Attorney's Office for the Southern District of New York ("USAO") unsealed criminal complaints against Mr. Rajaratnam and Ms. Chiesi charging them with securities fraud and conspiracy. That same day, the SEC initiated this civil action, alleging that Mr. Rajaratnam, Ms. Chiesi, and several co-defendants were liable for insider trading under 15 U.S.C. § 78j(b) and 17 C.F.R. § 240.10b-5, and for securities fraud under 15 U.S.C. § 77q(a). Subsequently, the USAO indicted Mr. Rajaratnam and Ms. Chiesi for insider trading and conspiracy. The USAO provided Mr. Rajaratnam and Ms. Chiesi with copies of the wiretap applications and the intercepted communications for use in their criminal defense.

Following the indictment, the SEC issued civil discovery requests to Mr. Rajaratnam and Ms. Chiesi seeking copies of the intercepted wiretap communications. Mr. Rajaratnam and Ms. Chiesi opposed the demands as contrary to law. The SEC moved to compel disclosure and, on February 9, 2010, the district court ordered Mr. Rajaratnam and Ms. Chiesi to produce the wiretap materials to the SEC by February 15, 2010, and to produce the same materials to any other party to the case who so demanded in writing.

After the district court denied both certification of its decision under 28 U.S.C. § 1292(b) and a stay pending appeal, Mr. Rajaratnam and Ms. Chiesi jointly

filed an emergency motion in this Court for a stay pending appeal and/or a petition for writ of mandamus. This Court granted a temporary stay on February 11, 2010, and a full stay pending appeal on March 24, 2010.

## **STATEMENT OF LEGAL AND FACTUAL BACKGROUND**

### **A. Constitutional And Statutory Framework**

1. The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The Fourth Amendment strictly limits the government’s use of wiretaps to record private telephone conversations. *Katz v. United States*, 389 U.S. 347, 359 (1967). Moreover, because wiretaps, unlike ordinary governmental searches, are conducted without notice to the multiple individuals affected, are ongoing for months, and indiscriminately capture all persons on all conversations regardless of relevance, more than the ordinary standard of probable cause used to support “conventional warrants” is required. *Berger v. New York*, 388 U.S. 41, 60 (1967). For a wiretap to pass constitutional muster, “special facts” demonstrating “exigency,” *ibid.*, must create a “genuine need” for government officials to secretly intercept private conversations, *Dalia v. United States*, 441 U.S. 238, 250 (1979).



**2. a.** In the wake of *Berger* and *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), 18 U.S.C. §§ 2510-2522, to establish a “comprehensive scheme for the regulation of wiretapping and electronic surveillance.” *Gelbard v. United States*, 408 U.S. 41, 46 (1972).<sup>1</sup> Congress broadly outlawed, with criminal felony sanctions, all interceptions of wiretapped communications “[e]xcept as otherwise specifically provided in this chapter,” largely confining wiretap authority to the statutorily specified criminal law-enforcement purposes. 18 U.S.C. § 2511(1); *see* 18 U.S.C. § 2516.

To that end, Congress housed all federal governmental wiretap authority in the Attorney General, and carefully confined wiretap authority to “certain major types of offenses and specific categories of crimes.” 18 U.S.C. § 2510 note (congressional findings); *see* 18 U.S.C. § 2516 (specifying the offenses for which wiretaps might be authorized); *see generally* *Gelbard*, 408 U.S. at 46 (use of wiretaps confined to investigating “specified serious crimes”). Congress’s detailed enumeration of the crimes for which the investigatory use of wiretaps would be authorized, 18 U.S.C. § 2516, does not include securities fraud, 18 U.S.C. § 1348, 15 U.S.C. § 77q, or insider trading, 15 U.S.C. § 78j(b). Even for those crimes for

---

<sup>1</sup> The relevant constitutional and statutory provisions are reproduced in an addendum to this brief.

which Congress authorized the use of wiretaps, Title III imposes “important preconditions to obtaining any intercept authority at all.” *United States v. Giordano*, 416 U.S. 505, 515 (1974). Thus, interception is “allowed only when authorized by a court of competent jurisdiction” upon a particularized showing of probable cause and necessity, 18 U.S.C. § 2518(1) & (2), and the interceptions “should remain under the control and supervision of the authorizing court,” 18 U.S.C. § 2510 note.

**b.** “To safeguard the privacy of innocent persons,” Congress teamed its strict limitations on intercepting private communications and requirement of close judicial supervision with equally “stringent conditions” on the use and disclosure of wiretap materials, *Gelbard*, 408 U.S. at 46. For example, Congress imposed felony criminal sanctions on anyone who “intentionally uses or endeavors to use” or “intentionally discloses, or endeavors to disclose the contents” of any wiretapped communication if that person “know[s] or ha[s] reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.” 18 U.S.C. § 2511(1)(c) & (d). Title III also proscribes the disclosure of wiretap material obtained as part of a criminal investigation with the intent to obstruct justice. *Id.* § 2511(1)(e).

To further “assur[e] \* \* \* that the information obtained [under Title III] will not be misused,” Congress “define[d] on a uniform basis the circumstances and

conditions” for “use of the contents” of wiretaps as evidence “in courts and administrative proceedings.” *Id.* § 2510 note (congressional findings).

*First*, Congress broadly proscribed the use of any wiretap information, and any “evidence derived therefrom,” as evidence “in any trial, hearing, or other proceeding in or before any court \* \* \* or other authority of the United States \* \* \* if the disclosure of that information would be in violation of this chapter.” *Id.* § 2515.

*Second*, Title III requires that the contents of wiretaps be immediately sealed upon conclusion of the wiretapping, *id.* § 2518(8), and that notice be provided prior to the use of the wiretaps in any court proceeding, *id.* § 2518(9). That permits an “aggrieved person” – an individual whose communications have been intercepted, *id.* § 2510(11) – to move to suppress those wiretaps before they are used in that proceeding. *Id.* §§ 2518(9) & (10); *see also id.* § 2511(1)(c). Furthermore, Title III provides a distinct statutory rule of exclusion that applies to both criminal and civil proceedings, *id.* §§ 2515, 2518(10), and supplements the Fourth Amendment’s own “judicially fashioned exclusionary rule,” *see Giordano*, 416 U.S. at 524. Title III “require[s] suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations

clearly calling for the employment of this extraordinary investigative device.” *Id.* at 527.

*Third*, Title III authorizes the disclosure of wiretap applications only if “good cause” is shown. 18 U.S.C. § 2518(8)(b). Title III, however, contains no parallel good-cause exception for the disclosure of the intercepted communications themselves. Instead, Section 2517 separately prescribes rules governing the use and disclosure of the “contents” of intercepted communications. Sections 2517(1) and (2) provide that law enforcement officers and investigators may use or disclose the contents of wiretaps as “appropriate to the proper performance of the official duties of the officer.” *Id.* § 2517(1) & (2). Title III defines the relevant law enforcement officers and investigators as a state or federal officer “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.” *Id.* § 2510(7). Except as otherwise provided, those authorized uses and disclosures are narrowly confined to the investigation and prosecution of Title III’s enumerated offenses, and do not include disclosing the materials to other governmental agencies for non-Title III enforcement purposes. *See American Friends Serv. Comm. v. Webster*, 720 F.2d 29, 73 (D.C. Cir. 1983) (no disclosure to Archives); Op. Off. Legal Counsel, *Sharing Title III Electronic*

*Surveillance Materials with the Intelligence Community*, 2000 WL 33716983, at \*8 (Oct. 17, 2000).<sup>2</sup>

Section 2517(3) separately provides that “[a]ny person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom \* \* \* may disclose the contents of that communication \* \* \* while giving testimony under oath or affirmation,” but only if the communication was “intercepted in accordance with the provisions of this chapter.” 18 U.S.C. § 2517(3). Such testimonial usage is conditioned on “[t]he presence of the seal” required by Congress on all wiretap intercepts, *id.* § 2518(8)(a), “or a satisfactory explanation for the absence thereof,” *id.* § 2518(8)(b).

Finally, Section 2517(5) directs that, when an investigative or law enforcement officer obtains information through a wiretap that “relate[s] to offenses other than those specified in the order of authorization or approval,” the “contents” of that communication and any evidence derived therefrom may be used

---

<sup>2</sup> Formal published OLC opinions embody the Attorney General’s exercise of his authority to direct the legal positions of the Executive Branch, 28 U.S.C. §§ 511-512, and thus are “controlling on questions of law within the Executive Branch.” Off. Legal Counsel, *Best Practices for OLC Opinions* 1 (May 16, 2005), available at <http://www.justice.gov/olc/best-practices-memo.pdf> (last visited Apr. 22, 2010). The Attorney General’s analysis has been ratified by Congress, which found it necessary subsequently to amend Title III to allow law enforcement agencies to share wiretap information with intelligence officials. See 18 U.S.C. § 2517(6); USA PATRIOT ACT, Pub. L. No. 107-56, 115 Stat. 272 (2001).

under Section 2517(3) only if a judge “finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter.” 18 U.S.C. § 2517(5).

## **B. Factual and Procedural Background**

1. Raj Rajaratnam is the founder and managing general partner of Galleon Management, LP, a hedge fund investment partnership. He was born in Sri Lanka in 1957 and was educated in England and the United States, graduating near the top of his class from Wharton Business School in 1983.

Danielle Chiesi is a hedge fund manager and investment consultant. Ms. Chiesi served as a consultant to New Castle Funds LLC. Prior to becoming an independent company, New Castle Funds LLC was part of Bear Stearns Asset Management.

2. On October 16, 2009, the United States Attorney’s Office for the Southern District of New York (“USAO”) unsealed criminal complaints against Mr. Rajaratnam and Ms. Chiesi. That same day, the SEC filed a civil complaint against Mr. Rajaratnam, Ms. Chiesi and, as amended on January 29, 2010, fifteen other defendants, including four corporate entities. A110. Three of the civil defendants (Ali Far, Choo-Beng Lee, and the Schottenfeld Group) were subsequently dismissed from the SEC action due to separate settlement agreements.

The criminal complaints revealed that the government had intercepted telephone conversations as part of its criminal investigation. Those conversations involve 18,150 communications intercepted from ten different telephones, including Mr. Rajaratnam's cell phone and Ms. Chiesi's cell and two home/office telephones.<sup>3</sup> The intercepted communications capture the private communications of more than 550 separate individuals over a sixteen-month period. The overwhelming majority of those individuals have not been charged in any criminal proceeding, and many may not have been provided inventory notices from the government alerting them that their conversations were intercepted, 18 U.S.C. § 2518(8)(d), and thus that their private communications were at issue when the district court ruled. *See also* A217-A218. Included among the calls intercepted were private discussions between Mr. Rajaratnam and his wife, his minor daughter, other family members, and his doctor. *See* A82. The calls intercepted on Ms. Chiesi's phones likewise contain discussions about highly personal matters, as well as conversations to which Ms. Chiesi was not a party.

---

<sup>3</sup> Ms. Chiesi worked out of her home. The government also intercepted calls on seven phones belonging to Zvi Goffer, Craig Drimal, Jason Goldfarb, Ali Far, and Choo-Beng Lee. Messrs. Goffer, Drimal, and Goldfarb are not defendants in this SEC action, but are defendants in *SEC v. Cutillo et. al*, No. 1:09-cv-9208 (Sullivan, J.), and *United States v. Goffer, et al.* No. 10-cr-0056 (S.D.N.Y.) (Sullivan, J.) (Indictment filed 1/21/10). Messrs. Far and Lee pled to informations filed against them in *United States v. Lee*, No. 09-cr-0972 (S.D.N.Y.) (Castel, J.), and *United States v. Far*, No. 09-cr-l009 (S.D.N.Y.) (Patterson, J.).

The USAO subsequently indicted Mr. Rajaratnam and Ms. Chiesi on sixteen counts of insider trading and conspiracy.<sup>4</sup> Following indictment, the USAO provided Mr. Rajaratnam and Ms. Chiesi with copies of the wiretap applications and all 18,150 intercepted communications. Prior to providing those materials, the USAO requested that Mr. Rajaratnam and Ms. Chiesi stipulate that the USAO could provide copies of the intercepts to the SEC. Mr. Rajaratnam and Ms. Chiesi refused to so stipulate.

3. On November 16, 2009, the SEC issued a civil discovery request to Mr. Rajaratnam and Ms. Chiesi that sought, *inter alia*, copies of intercepted wiretap communications. Both defendants objected on relevance (and other) grounds on December 21, 2009. On December 28, 2009 – five days after the USAO first produced wiretap materials to the defendants – the SEC issued civil discovery requests targeted specifically to all intercepted communications and the wiretap applications. A56-57. When Mr. Rajaratnam and Ms. Chiesi opposed the demand as precluded by Title III, the SEC requested that the district court compel production.<sup>5</sup>

---

<sup>4</sup> A superseding indictment was issued on February 9, 2010.

<sup>5</sup> Both also objected to the demand again on relevance grounds. *See* Letter from Terence Lynam to Hon. Jed S. Rakoff (Jan. 22, 2010) (S.D.N.Y. Docket No. 104) at 1; Letter from Alan Kaufman to Hon. Jed S. Rakoff (Jan. 29, 2010) (S.D.N.Y. Docket No. 115) at 4.



In deciding the motion to compel, Judge Rakoff requested the views of the USAO. The USAO first represented that it intended to seek authorization from Judge Holwell, who is presiding over the criminal case against Mr. Rajaratnam and Ms. Chiesi and has jurisdiction over the sealed wiretaps, to release the wiretaps to the SEC. The USAO, however, never sought such permission from Judge Holwell. At a subsequent hearing, the USAO argued that it had the independent authority to release the wiretaps to the SEC without court approval. *See* A74, A91. The USAO, however, never made any such disclosure. Mr. Rajaratnam and Ms. Chiesi subsequently filed a motion for a protective order to prevent such disclosure by the USAO, which remains pending before Judge Holwell.

On February 9, 2010, the district court ordered Mr. Rajaratnam and Ms. Chiesi to produce the wiretap materials to the SEC by February 15, 2010. The court further ordered Mr. Rajaratnam and Ms. Chiesi to “promptly produce the same materials to any” of the “other part[ies] to this case who so demand[] in writing.” A179. In so ruling, the court acknowledged that Title III itself “specifies the conditions under which the Government is authorized to disclose the contents of wiretap recordings,” A177, and that this Court recently held that “turning Title III into a general civil discovery mechanism would simply ignore the privacy rights of those whose conversations are overheard,” A176 (quoting *In re Application of the New York Times Co. to Unseal Wiretap & Search Warrant*

*Materials*, 577 F.3d 401, 407 (2d Cir. 2009) (*New York Times*), and *In re Application of NBC*, 735 F.2d 51, 54 (2d Cir. 1984)). The court nevertheless concluded that “principles of civil discovery” permitted the court to go beyond Title III’s terms and order the disclosure of all 18,150 wiretaps by the criminal defendants of their (and other persons’) intercepted communications prior to the wiretaps’ disclosure in any criminal proceeding, prior to the adjudication of a motion to suppress, and prior to the conclusion of the criminal prosecution, A177-A178. The district court distinguished this Court’s decision in *New York Times* on the ground that government agencies enjoy civil discovery rights that “a purely private plaintiff” does not. A178 n.1. The court further held that issuance of a discovery-phase protective order was the “simple way to satisfy” “Congress’ concern with privacy.” A178.

Two days later, the district court denied as “frivolous” Mr. Rajaratnam’s and Ms. Chiesi’s requests to certify its ruling under 28 U.S.C. § 1292(b) and denied a stay pending appeal. A180-A181.

4. On February 11, 2010, this Court granted Mr. Rajaratnam’s and Ms. Chiesi’s joint motion for a temporary stay and, on March 24, 2010, the Court granted a stay pending appeal.

5. Also on March 24, 2010, the district court granted the parties’ joint request to postpone the SEC action until after the conclusion of the pending

criminal prosecution, scheduling the trial to commence on February 14, 2011. A221. While the district court has also stayed all testimonial discovery, the court did not stay documentary discovery. A223. Accordingly, the order to disclose the wiretap materials remains in effect.

6. The district court (Holwell, J.) in the pending criminal proceeding against Mr. Rajaratnam and Ms. Chiesi has scheduled a hearing for June 17, 2010, on their motions to suppress the intercepted communications and evidence derived from the wiretaps on their four telephones. A219-A220. The criminal trial is scheduled to commence on October 25, 2010. No date for a suppression motion pertaining to the Goffer, Drimal and Goldfarb intercepts has yet been scheduled in their separate criminal action.<sup>6</sup>

### **SUMMARY OF ARGUMENT**

Twenty-six years ago, this Court said it was “sure that Congress did not utilize a provision in the Organized Crime Control Act to make the fruits of wiretapping broadly available to all civil litigants who show a need for them,” and denied a civil plaintiff discovery of wiretap materials for use in pending civil litigation. *In re Application of NBC*, 735 F.2d 51, 54 (2d Cir. 1984). Even though

---

<sup>6</sup> Mr. Rajaratnam and Ms. Chiesi are also reserving their rights to move to suppress any of the Goffer, Drimal, Goldfarb, Far or Lee intercepts to which they were a party should the government subsequently provide notice that they will attempt to use those specific calls as evidence in their criminal prosecution or any other proceeding.

the lawfulness of the wiretaps was not in question and the criminal prosecution had long since terminated, this Court held that “turning Title III into a general civil discovery mechanism would simply ignore the privacy rights of those whose conversations are overheard.” *Id.* at 52-53, 54.

With barely a nod to *NBC* and invoking nothing more than general “principles of civil discovery,” A176, A177, the district court in this case has ordered two criminal defendants to release wholesale to the SEC and fourteen other litigants more than 18,000 untested wiretap recordings of their own and more than 550 other individuals’ private telephone conversations. To be sure, the procedural posture is different. Here, disclosure has been ordered *prior to* adjudication of the wiretaps’ lawfulness, *prior to* any unsealing and disclosure pursuant to Title III’s terms, *prior to* conclusion of the pending criminal prosecutions, and *without* the participation of the judge with custody over the sealed wiretaps. But those factors make the district court’s decision constitutionally and statutorily far worse, not better.

Nothing in the text of Title III permits that sweeping disclosure. Quite the opposite, the district court’s order defies the statute’s plain text at every turn, ignoring the narrow limitations on and preconditions to disclosure of wiretap material that Congress designed to protect individual privacy and to ensure that the wiretap law comported with the Fourth Amendment. For example, while Title III

permits the disclosure of wiretap applications upon a showing of “good cause,” the district court has broadly ordered the release of both wiretap applications and the even more sensitive contents of intercepted conversations on the far lesser discovery standard of mere relevance to the civil litigation. While Title III authorizes private individuals to make only testimonial disclosures under oath or affirmation after the lawfulness of an intercept has been adjudicated, the district court has compelled sweeping non-testimonial disclosures, not under oath or affirmation, and heedless of the intercepts’ lawfulness. Further, while Title III tightly constrains law enforcement officials’ disclosures to the enforcement of Title III predicate crimes, the district court has held that federal agencies and private litigants ineligible to obtain wiretaps or even to receive wiretap materials from law enforcement officials can circumvent that barrier by forcing the criminal defendants themselves to reveal their private conversations in civil discovery. And all of that is without any involvement by the judge presiding over both the sealed wiretaps and the pending criminal prosecution.

Only major surgery on Title III’s text could sustain that order. Even more fundamentally, neither the district court nor the SEC has ever explained why Congress would enact a law that comprehensively and tightly constrains the disclosure of wiretap materials to specified law enforcement ends under the close superintendence of a judge, but then permits any savvy civil litigant to force

wholesale disclosure from the *victim* of the privacy invasion, rather than from the prosecutors who conducted the wiretaps or from the judge presiding over the seal. That crabbed statutory scheme makes no sense and bears no resemblance to the comprehensive scheme for protecting privacy that this Court has long held Title III provides and that the Fourth Amendment requires.

Finally, this Court has the necessary jurisdiction to vacate the district court's order. Controlling precedent of this Court holds that the ordered disclosure of Title III wiretaps in litigation collateral to the criminal proceeding is reviewable under the collateral order doctrine. The Supreme Court's recent decision in *Mohawk Industries, Inc. v. Carpenter*, 130 S. Ct. 599 (2009), reconfirms the correctness of that decision because the Supreme Court itself has ruled that Title III advances privacy interests of the highest order – statutory interests enforcing protections for conversational privacy and autonomy that are of constitutional magnitude and are enforced by felony prohibitions. In addition, this Court has jurisdiction to issue a writ of mandamus, which is warranted in this case because (i) the district court's wide departure from precedent presents a significant question of first impression in this Circuit; (ii) no other remedy can adequately vindicate the constitutional and statutory rights at stake; and (iii) the resolution of this question will aid in the administration of justice, not only in the pending civil and criminal cases, but also

in the large number of other wiretap cases susceptible to parallel civil and criminal proceedings.

## **ARGUMENT**

### **I. THIS COURT HAS JURISDICTION UNDER THE COLLATERAL ORDER DOCTRINE**

#### **A. Standard of Review**

Legal questions pertaining to subject matter jurisdiction are reviewed *de novo*. *United States v. White*, 237 F.3d 170, 172 (2d Cir. 2001).

#### **B. The *Gerena* Decision Correctly Establishes Jurisdiction**

This Court has specifically ruled that when, as here, criminal defendants awaiting trial seek to protect their privacy and fair trial rights by preventing the disclosure of Title III wiretap evidence in a proceeding collateral to their criminal action, this Court has appellate jurisdiction to review that disclosure order under the collateral order doctrine of *Cohen v. Beneficial Industrial Loan Corp.*, 337 U.S. 541, 546 (1949). *United States v. Gerena*, 869 F.2d 82, 83-84 (2d Cir. 1989) (citing *Richardson-Merrell, Inc. v. Koller*, 472 U.S. 424, 430-431 (1985), and *In re New York Times Co.*, 828 F.2d 110, 113 (2d Cir. 1987) (*In re New York Times*), *cert. denied*, 485 U.S. 977 (1988)). That ruling controls this case.

Courts of appeals generally have jurisdiction under 28 U.S.C. § 1291 to review “final decisions” of district courts. The Supreme Court has long held that the phrase “final decision[]” includes a “small class” of collateral rulings issued

prior to final judgment in litigation, *Cohen*, 337 U.S. at 545-546, “that are conclusive, that resolve important questions separate from the merits, and that are effectively unreviewable on appeal from the final judgment in the underlying action,” *Swint v. Chambers County Comm’n*, 514 U.S. 35, 42 (1995). *See also Mohawk Indus. Inc. v. Carpenter*, 130 S. Ct. 599, 605 (2009) (same).

The appropriateness of permitting such appeals turns primarily on the importance of the question presented and whether the right is “adequately vindicable” if review is delayed until after final judgment. *Mohawk*, 130 S. Ct. at 605. “[T]he decisive consideration is whether delaying review until the entry of final judgment ‘would imperil a substantial public interest’ or ‘some particular value of a high order.’” *Ibid*. That determination must be made on a category-by-category basis. *Ibid*.

In *Gerena*, this Court specifically ruled that it had jurisdiction under the collateral order doctrine to review an appeal by two criminal defendants seeking to prevent the government’s public disclosure of previously sealed intercepts in a separate criminal proceeding (a guilty plea of a co-defendant). 869 F.2d at 83-84. Even though the district court had denied a motion to suppress the intercepts at issue, *id.* at 83, this Court held that the order permitting disclosure and rejecting the defendants’ Title III rights “is appealable under the ‘collateral order doctrine’ of *Cohen*.” *Ibid*. The Court explained that the order “conclusively rejects appellants’



claim of statutorily guaranteed privacy rights,” a ruling that was “completely separate from the merits of the action.” *Ibid.* The Court further held that the question of Title III’s protection “would be effectively unreviewable on appeal from a final judgment since the alleged damage to [the defendant’s] privacy rights would have occurred long before the end of the trial.” *Ibid.* Furthermore, because there was “sufficient overlap in the factors relevant to [the defendant’s] ‘privacy’ and ‘fair trial’ arguments,” the Court held that “concern for judicial economy dictates that” it should exercise its plenary authority to consider in parallel the defendant’s fair trial arguments. *Id.* at 84 (citing *San Filippo v. United States Trust Co.*, 737 F.2d 246, 255 (2d Cir. 1984), *cert. denied*, 470 U.S. 1035 (1985)). That ruling was correct.

*First*, the SEC has never disputed that the district court’s disclosure order is both conclusive and collateral to the merits of the underlying securities fraud litigation. Nor could it. The order is conclusive because it compels Mr. Rajaratnam and Ms. Chiesi to turn over material protected by constitutional and statutory privacy rights to fifteen different civil litigants. Once disclosed, their claim to privacy will be irretrievably lost. The legal dispute over the disclosures permitted by Title III and the Constitution, moreover, is completely separate from the merits of the underlying securities law claims.

*Second*, wiretap disclosures to third parties map directly onto the *Mohawk* framework for identifying appealable collateral orders. Title III’s “stringent conditions” on the disclosure of wiretap materials reflect an “overriding congressional concern” with “the protection of privacy,” *Gelbard v. United States*, 408 U.S. 41, 46, 48 (1972) – a concern rooted in fundamental Fourth Amendment protections, *see Katz v. United States*, 389 U.S. 347, 357-359 (1967). That privacy interest is not just “of a high order,” *Mohawk*, 130 S. Ct. at 605. It is an “interest of the highest order.” *Bartnicki v. Vopper*, 532 U.S. 514, 545 (2001); *see In re New York Times*, 828 F.2d at 115 (“The right of privacy protected by Title III is extremely important.”).

The privacy interest has such distinctive magnitude because, unlike the attorney-client privilege at issue in *Mohawk*, Title III does far more than create an evidentiary privilege for legal proceedings. Title III was “the culmination of a long battle between those who would have altogether prohibited wiretaps and \* \* \* those who wanted to allow the government to use wiretap material in criminal prosecutions.” *NBC*, 735 F.2d at 53. Its terms are thus designed to “foster[] private speech,” *Bartnicki*, 532 U.S. at 518, which sits at the core of the First and Fourth Amendments and is an indispensable component of individual freedom in a system of limited government, personal autonomy, and the freedom of political thought and dialogue upon which representative government depends. As this

Court has explained, Congress enacted Title III's "rigorous, carefully drawn standards" to enforce the Nation's "historic" "protection of privacy" and "the spirit of liberty which has distinguished this nation from its birth." *United States v. Huss*, 482 F.2d 38, 52 (2d Cir. 1973). *See United States v. United States Dist. Court for Eastern Dist. of Mich.*, 407 U.S. 297, 314 (1972) ("Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."); *Zweibon v. Mitchell*, 516 F.2d 594, 633 (D.C. Cir. 1975) (en banc) (plurality) (Title III's strict protections "protect the privacy interests of those whose conversations the Government seeks to overhear, but also \* \* \* protect free and robust exercise of the First Amendment rights of speech and association by those who might otherwise be chilled by the fear of unsupervised and unlimited Executive power to institute electronic surveillances.").

Title III thus provides a foundational protection for the substantive privacy of all speech in the home, in the car, in social settings, in political meetings, and in the boardroom. *See Berger v. New York*, 388 U.S. 41, 64-65 (1967) (Douglas, J., concurring) (the wiretap places an "invisible policeman \* \* \* in the bedroom, in the business conference, in the social hour"). That is why Title III goes far beyond creating an evidentiary rule and instead directly proscribes all private wiretapping,

*NBC*, 735 F.2d at 54, and strictly limits the terms and conditions on which specifically designated governmental entities can obtain, use, and disclose wiretaps and their contents. Underscoring the depth of the statutory and constitutional interests at stake – and quite unlike the common-law attorney-client privilege – Title III’s prohibitions and limitations are enforced by felony criminal sanctions, 18 U.S.C. § 2511(1), as well as judicial imposition and superintendence of the statutorily mandated seal over all such wiretaps, 18 U.S.C. § 2518(8)-(10), in order “[t]o safeguard the privacy of innocent persons.” 18 U.S.C. § 2510 note.<sup>7</sup>

*Third*, the constitutional and statutory privacy concerns that Title III enforces cannot be adequately protected through post-final judgment appeals. Once the conversations are disclosed, the harm both to the involved individuals’ privacy and to Congress’s larger concern for conversational privacy is done. Indeed, the “disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself.” *Bartnicki*, 532 U.S. at 533. And “[e]ach time the illicitly obtained recording is replayed to a new and different listener, the scope of the invasion widens and the aggrieved party’s injury is aggravated.” *Fultz v. Gilliam*, 942 F.2d 396, 402 (6th Cir. 1991). A new trial

---

<sup>7</sup> Title III’s “special safeguards against the unique problems” posed by wiretapping also include enhancing the rights of grand jury witnesses to refuse to provide testimony. *See United States v. Calandra*, 414 U.S. 338, 355 n.11 (1974) (discussing *Gelbard*).

simply cannot “unsay the confidential information that [will have] been revealed.” *In re von Bulow*, 828 F.2d 94, 99 (2d Cir. 1987).

Furthermore, as *Gerena*’s fair-trial discussion recognized, 869 F.2d at 85-86, disclosures in collateral litigation can have a spillover effect in the criminal case, as witnesses’ minds become contaminated, plea deals are struck, and evidentiary materials are leaked to the press. “In a highly publicized case” like this, “the premature publication of damaging communications that are later determined to have been unlawfully obtained might make a fair trial impossible” and would “vitate the privacy protections of [Title III].” *In re Globe Newspaper Co.*, 729 F.2d 47, 55 (1st Cir. 1984). Yet that injury cannot possibly be reviewed or remedied upon final judgment in the civil litigation.

The privacy interests and speech affected by disclosure, moreover, are not limited to the particular defendants in this case. They involve every person on every one of the 18,150 telephone calls. In this case, that is more than 550 individuals, including children, those involved in intimate relationships, friends, and a host of individuals who have nothing to do with the pending civil or criminal prosecutions. In fact, while the district court here ordered the wholesale release of every single intercepted conversation, even the USAO agrees that “tons and tons of [those] calls” “at the end of the day \* \* \* [are]n’t going to be played at this [criminal] trial.” A184. The vast majority are also likely unaware that verbatim

recordings of their conversations are about to be disclosed to fifteen civil litigants because neither the SEC nor the district court afforded them notice and, to the defendants' knowledge, inventory notices from the USAO may not yet have reached all of them.

“The privacy interests of [those] innocent third parties \* \* \* that may be harmed by disclosure of the Title III material should \* \* \* weigh[] heavily with the trial judge, since all the parties who may be harmed by disclosure are typically not before the court.” *In re New York Times*, 828 F.2d at 116. Indeed, Congress’s “overriding concern,” *Gelbard*, 408 U.S. at 48, for “fostering private speech,” *Bartnicki*, 532 U.S. at 518, and assuring the public of the communicative confidentiality that is so essential to democratic functioning and individual autonomy will become empty promises if hundreds upon hundreds of individuals see their private conversations transformed into civil discovery fodder in cases in which they have no capacity to seek timely judicial review.

In sum, *Gerena*’s binding jurisdictional precedent reflects a correct and faithful application of the *Cohen* collateral order doctrine, and its judgment has been reinforced by the rulings of other circuits. *See United States v. Dorfman*, 690 F.2d 1230, 1231-1232 (7th Cir. 1982) (permitting appeal of wiretap disclosure order under collateral order doctrine); *see also United States v. Andreas*, 150 F.3d

766, 768 (7th Cir. 1998) (same); *Anthony v. United States*, 667 F.2d 870 (10th Cir. 1981) (same).

**C. *Gerena* Is Consistent with *Mohawk***

The SEC's argument (Stay Opp. Br. 6) that *Mohawk* vitiated *Gerena* is wrong for three reasons.

*First*, the Supreme Court could not have been clearer in *Mohawk* that collateral order decisions must be made on a category by category basis and that its decision with respect to the attorney-client privilege was specific to the “category to which [the] claim belong[ed],” and its analysis turned on the characteristics of the specific “class of claims” at issue. *Mohawk*, 130 S. Ct. at 605. Taking the Supreme Court at its word, *Mohawk* thus textually limited the reach of its decision to the common-law evidentiary attorney-client privilege. Neither the *Mohawk* opinion nor its analysis speaks to the appealability of statutorily created privacy rights that have “constitutional overtones” of the magnitude that Title III does, *Giordano*, 416 U.S. at 526. Quite the opposite, the Supreme Court stated explicitly that its decision did not address whether a different rule would apply when, as here, the confidential nature of the material had constitutional roots. *Mohawk*, 130 S. Ct. at 609 n.4.

*Second*, the Supreme Court explained that, given the nature of the attorney-client privilege and its exceptions, “clients and counsel must account for the

possibility that they will later be required by law to disclose their communications for a variety of reasons.” *Id.* at 607. Congress made precisely the opposite judgment in Title III, striving to assure the public that the protections for conversational privacy remained steadfast, so that individuals, in “deciding how freely to speak,” would *not* have to account for the possibility that the government was eavesdropping and citizens could rest assured that there will be no “erroneous disclosure” by the government of their private conversations. *Ibid.* The chilling effect of permitting unreviewed disclosures of wiretaps on “those who might otherwise be chilled by the fear of unsupervised and unlimited Executive power to institute electronic surveillances” is thus very real and its effects reach far beyond the confines of courtroom evidentiary privileges. *Zweibon*, 516 F.2d at 633.

*Third*, most disputed invocations of attorney-client privilege “involve the routine application of settled legal principles” and are “unlikely to be reversed on appeal, particularly when they rest on factual determinations for which appellate deference is the norm.” *Mohawk*, 130 S. Ct. at 607. The same cannot be said for appeals of wiretap disclosure orders, which commonly present important questions of law, as this case does, and just last year prompted an order of reversal, *see New York Times*, 577 F.3d at 411.<sup>8</sup>

---

<sup>8</sup> The SEC’s reliance on *United States v. Miller*, 14 F.3d 761 (2d Cir. 1994), is misplaced. *See* SEC FRAP 28(j) Letter (Mar. 22, 2010) (Docket No. 64).



In short, nothing in *Gerena* is irreconcilable with the “fundamental point” of the Supreme Court decision, *Boothe v. Hammock*, 605 F.2d 661, 663 (2d Cir. 1979), nor is *Mohawk*’s “reasoning \* \* \* so broad” that it compels the abandonment of circuit precedent, *Union of Needletrades, Indus. & Textile Employees, AFL-CIO, CLC v. Immigration & Naturalization Serv.*, 336 F.3d 200, 210 (2d Cir. 2003). *See also European Cmty. v. RJR Nabisco, Inc.*, 424 F.3d 175, 179 (2d Cir. 2005) (Sotomayor, J.) (“reinstat[ing]” panel decision as “controlling precedent” because an intervening Supreme Court decision “[did] not substantively ‘cast doubt’ on [that decision]”). *Gerena* thus remains both sound and binding precedent.

## **II. TITLE III AND THE CONSTITUTION FORBID THE MASS DISCLOSURE OF UNTESTED WIRETAP INTERCEPTS IN CIVIL DISCOVERY**

### **A. Standard of Review**

A district court’s discovery rulings are reviewed for abuse of discretion. *In re Agent Orange Prod. Liab. Litig.*, 517 F.3d 76, 102 (2d Cir. 2008). “A district court abuses its discretion when (1) its decision rests on an error of law . . . or a

---

Unlike *Gerena*, *Dorfman*, and this case, Miller sought interlocutory review after “the admissibility of the wiretap evidence ha[d] been adjudicated in [his] \* \* \* criminal trial[,]” after that evidence had been introduced, and after he was convicted, but before his sentencing. *Miller*, 14 F.3d at 765. Those objections could timely “be[] reviewed on appeal from a final judgment” as soon as his sentencing was completed. *Ibid.*

clearly erroneous factual finding, or (2) its decision – though not necessarily the product of a legal error or a clearly erroneous factual finding – cannot be located within the range of permissible decisions.” *In re Fitch, Inc.*, 330 F.3d 104, 108 (2d Cir. 2003) (per curiam). “A district court by definition abuses its discretion when it makes an error of law.” *Koon v. United States*, 518 U.S. 81, 100 (1996). Furthermore, “[a] district court abuses its discretion ‘when the action taken was improvident and affected the substantial rights of the parties.’” *Wills v. Amerada Hess Corp.*, 379 F.3d 32, 51 (2d Cir. 2004) (Sotomayor, J.). Whether Title III and the Fourth Amendment authorize the disclosure of wiretaps as part of general civil discovery are questions of law that this Court reviews *de novo*. See *United States v. Rood*, 281 F.3d 353, 355 (2d Cir. 2002) (statutory construction); *Melzer v. Bd. of Educ.*, 336 F.3d 185, 198 (2d Cir. 2003) (constitutional questions).

**B. Title III’s Strict Textual Limitations Protecting Privacy And Strong Presumption Against Disclosure Foreclose The Compelled Civil Discovery Of Wiretap Materials From Criminal Defendants**

“Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.” *Berger*, 388 U.S. at 63. Yet the district court’s order in this case cast aside the “rigorous” limitations that were “carefully drawn” by Congress in Title III to protect privacy, *Huss*, 482 F.2d at 52, substituting in their place a regime in which the privacy of hundreds of individuals and Fourth Amendment protections must take a backseat to general “principles of civil

discovery,” A177. That holding lacks any foundation in Title III’s text or precedent, and it opens the door to widespread circumvention of the limitations on wiretap usage that Congress carefully crafted to meet the Constitution’s demands.

### ***1. The Order Is Presumptively Invalid***

The starting point in this case is also its ending point. As this Court reconfirmed just last year, Title III establishes a “strong presumption *against* disclosure of the fruits of wiretap applications,” *New York Times*, 577 F.3d at 406, “prohibit[ing], in all but a few instances, the \* \* \* disclosure of wire or oral communications,” *United States v. Marion*, 535 F.2d 697, 700 (2d Cir. 1976). That “strong presumption,” which continues to govern disclosure questions even after the denial of a motion to suppress and after conclusion of the criminal litigation, *see id.* at 699-700, applies with its greatest force to this pre-suppression and pre-trial disclosure order. And the SEC cannot overcome it.

Consistent with that presumption, courts of appeals have repeatedly emphasized that “Title III prohibits all disclosures not authorized therein.” *Smith v. Lipton*, 990 F.2d 1015, 1018 (8th Cir. 1993) (en banc); *see also United Kingdom v. United States*, 238 F.3d 1312, 1322-1323 (11th Cir. 2001) (“Courts interpreting these provisions have held that [Title III] generally bars the disclosure of the contents of conversations intercepted through a wiretap absent a specific statutory authorization.”); *Nix v. O’Malley*, 160 F.3d 343, 351 (6th Cir. 1998) (federal

wiretap statute permits disclosure in limited instances, but its plain language allows no additional exceptions); *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.”); *Fultz v. Gilliam*, 942 F.2d 396, 401-402 (6th Cir. 1991) (“[Title III] ‘implies that what is not permitted is forbidden.’”); *Lam Lek Chong v. Drug Enforcement Admin.*, 929 F.2d 729, 732-733 (D.C. Cir. 1991) (Title III is “a comprehensive statutory scheme” with “strictly limited disclosure provisions”); *United States v. Dorfman*, 690 F.2d 1230, 1232 (7th Cir. 1982) (“Title III implies that what is not permitted is forbidden \* \* \* [and] [t]he implication is reinforced by the emphasis the draftsmen put on the importance of protecting privacy.”); *United States v. Cianfrani*, 573 F.2d 835, 856 (3d Cir. 1978) (“Congress intended to regulate strictly disclosure of intercepted communications, limiting the public revelation of even interceptions obtained in accordance with the Act to certain narrowly defined circumstances.”). The Attorney General of the United States agrees that “Title III prohibits every disclosure that it does not explicitly authorize.” Op. Off. Legal Counsel, *Sharing Title III Electronic Surveillance Materials with the Intelligence Community*, 2000 WL 33716983, at \*8 (Oct. 17, 2000).

The district court ignored that presumption and ignored the undisputed absence of any explicit textual authorization for compelled discovery in Title III, relying instead on general principles of civil discovery. But when wiretap materials are at issue, Title III is the “statute on point.” *New York Times*, 577 F.3d at 406. And that statute forbids a district court that does not have jurisdiction over the sealed wiretaps from forcing a criminal defendant to release them wholesale prior to resolution of a motion to suppress, prior to their authorized disclosure under Title III’s text, and prior to the conclusion of the criminal case.

## **2. Title III’s Text Forecloses Compelled Discovery**

Title III is a “comprehensive scheme for the regulation of wiretapping,” *Gelbard v. United States*, 408 U.S. 41, 46 (1972), crafted by a Congress that had “the protection of privacy” as its “overriding congressional concern..” The statute imposes “stringent conditions” on all aspects of wiretap usage by the government, *ibid.*, “authorizing the use of evidence obtained by electronic surveillance [only] on specified conditions, and prohibiting its use otherwise,” *Bartnicki*, 532 U.S. at 523. *See NBC*, 735 F.2d at 53 (Title III places “strict limits on wiretapping and how it [can] be used.”).

Nothing in Title III’s detailed textual regulation of disclosures, however, authorizes the compelled disclosure of wiretap materials as a part of routine civil discovery, let alone empower civil litigants to compound the “invasion of [a

defendant's] privacy by adding to the injury of interception the insult of compelled disclosure.” *Gelbard*, 408 U.S. at 52. Quite the opposite, allowing government agencies from which Congress specifically withheld wiretap authority to compel criminal defendants to turn over their taped conversations just by timing their civil lawsuits to coincide with a criminal prosecution would require the Court to erase substantial amounts of statutory text and would transform Title III’s comprehensive limitations into empty gestures.

*First*, this Court has long been “sure that Congress did not utilize a provision in the Organized Crime Control Act to make the fruits of wiretapping broadly available to all civil litigants who show a need for them.” *NBC*, 735 F.2d at 54. Title III “ma[de] an exception from the general ban [on wiretaps] for purposes of enforcement of the criminal law,” not the civil law. *Ibid.*; see 18 U.S.C. § 2516 (authorizing wiretap usage only for specified crimes). “[T]urning Title III into a general civil discovery mechanism would simply ignore the privacy rights of those whose conversations are overheard.” *NBC*, 735 F.2d at 54.

*Second*, not only is an authorization for civil discovery absent, but Title III’s text says exactly the opposite. The statute requires a particularized showing of “good cause” for disclosure of just the wiretap *applications*. 18 U.S.C. § 2518(8)(b). The SEC’s civil discovery request indisputably did not and could not meet that test because the SEC is not an “aggrieved person” under Title III. *See*

*New York Times*, 577 F.3d at 408 (“In *NBC* we further refined the required showing of ‘good cause’ by requiring that the party claiming access be an ‘aggrieved person’” under Title III, 18 U.S.C. § 2510(11)). The district court’s order thus simply reads that “good cause” limitation right out of the statute, supplanting it with a disclosure rule that requires nothing more than the very capacious relevance standard of civil discovery, *see* Fed. R. App. P. 26.

And with respect to disclosure of the *contents* of the wiretaps themselves – the actual intercepted communications – Congress did not authorize relief even upon a showing of good cause, choosing instead to limit disclosures strictly to the provision of testimony or to the government’s use and disclosure in conjunction with Title III law enforcement functions, 18 U.S.C. § 2517(1)-(3).<sup>9</sup> None of those exceptions applies here, making the district court’s authorization of disclosure under a mere relevance standard an even more profound repudiation of statutory text.

To begin with, forcing criminal defendants to open their private conversations to scrutiny by civil government agents and a swath of private civil

---

<sup>9</sup> The Constitution itself supplements the statutorily authorized disclosures by permitting their provision to the defense in a criminal case, under the Fifth and Sixth Amendments, and allowing speech as required by the First Amendment’s Free Speech Clause, *see Bartnicki, supra*. The SEC, however, has no constitutional claim to these wiretap materials.

litigants does not remotely constitute a use or disclosure by “investigative or law enforcement officer[s]” in the “proper performance of the[ir] official duties,” within the meaning of Sections 2517(1) and (2). OLC Op., 2000 WL 33716983, at \*3-4 (“appropriate to the proper performance of \* \* \* official duties” must “be construed narrowly” to permit disclosures only for the prescribed Title III law enforcement functions). While the SEC and USAO contended in district court that the USAO could provide the wiretap materials itself to the SEC under Sections 2517(1) and (2), *see* Letter from Valerie A. Szczepanik to Hon. Jed S. Rakoff (Jan. 27, 2010) (S.D.N.Y. Docket No. 126) at 3; Letter from Jonathan R. Streeter to Hon. Jed S. Rakoff (Jan. 27, 2010) (S.D.N.Y. Docket No. 114) at 1-5, that argument defied the Attorney General’s official position, *see* OLC Op., 2000 WL 33716983, at \*\*3-4. The USAO, for its part, has chosen neither to provide the materials to the SEC nor to seek permission from Judge Holwell to do so.

With no luck at the front door, the SEC resorted to the backdoor approach of forcing the defendants to make the very disclosure of wiretap materials that the government itself is unwilling and legally unable to make and that the judge presiding over the sealed wiretaps has never authorized. But surely if Congress intended to provide civil agencies open access to wiretap materials, it would have authorized intra-governmental exchanges directly or under the superintendence of the judge presiding over the sealed wiretaps, rather than through the convoluted



route of filing a civil suit and then asking a different judge to compel disclosure through civil discovery from the criminal defendant.

Section 2517(3) does not apply either. While it does address the disclosure of wiretaps by private persons, its helpfulness to the SEC ends there. Section 2517(3) only permits the disclosure of wiretap material in court proceedings by persons already in possession of wiretap information, not coercive discovery by government agents. The Section 2517(3) disclosure, moreover, is limited to “testimony under oath or affirmation.” 18 U.S.C. § 2517(3). *See United States v. Ricco*, 566 F.2d 433, 435 (2d Cir. 1977) (Section 2517(3) “does not, by its terms, apply to nontestimonial uses”); *see also Certain Interested Individuals v. Pulitzer Publ’g Co.*, 895 F.2d 460, 465 (8th Cir. 1990) (Section 2517(3) limited to testimonial disclosure). Document productions in civil discovery are neither testimonial nor filed under oath or affirmation. Even worse for the SEC, Title III textually predicates a disclosure under Section 2517(3) on a *prior* determination of the intercepts’ lawfulness. 18 U.S.C. §§ 2517(5), 2518 (9) & (10); *see Berry v. Funk*, 146 F.3d 1003, 1012 (D.C. Cir. 1998); *Chandler v. United States Army*, 125 F.3d 1296, 1300 (9th Cir. 1997); *Forsyth v. Barr*, 19 F.3d 1527, 1544 (5th Cir. 1994). And when, as here, the proposed evidentiary use of the wiretaps pertains to non-Title III offenses, like securities fraud and insider trading, Section 2517(5) requires a separate judicial determination that the capture of evidence pertaining to

non-predicate offenses was incidental to an otherwise proper Title III warrant. *See United States v. Masciarelli*, 558 F.2d 1064, 1067 (2d Cir. 1977). The district court's order erased all of those conditions from the statutory text. But this Court's task is to "apply the provision as written, not as [it] would write it." *See United States v. Demerritt*, 196 F.3d 138, 143 (2d Cir. 1999).

*Third*, the SEC points to Section 2511(1)(e), and emphasizes that Title III would not permit a criminal prosecution of Mr. Rajaratnam or Ms. Chiesi for complying with the order to compel because that criminal prohibition applies only to disclosures intended to obstruct justice. Stay Opp. Br. 8. It would no doubt be worse if Mr. Rajaratnam and Ms. Chiesi were both forced to compound their loss of privacy by turning over the wiretaps *and* were then sent to jail for doing so. But if that is the SEC's premise, the argument is flawed because Section 2511 elsewhere criminally proscribes the disclosure of wiretap material by persons who "hav[e] reason to know that the information was obtained through [a] \* \* \* violation of this subsection," 18 U.S.C. § 2511(1)(c), as Mr. Rajaratnam's and Ms. Chiesi's motions to suppress reflect they do.

In any event, Title III neither requires nor authorizes everything that is not a felony. The issue in this case is whether the SEC can force its "uninvited ear" and the ears of fourteen other civil litigants into the private conversations of more than 550 individuals. *Katz*, 389 U.S. at 352. More specifically, Congress in Title III –

as required by the Fourth Amendment, *see Berger, supra* – forbade the SEC to use wiretaps for civil insider trading investigations. *See* 18 U.S.C. § 2516.<sup>10</sup> The question thus is whether, by the simple expedient of filing tag-team criminal and civil actions, the SEC (and countless other agencies with parallel civil authority) can end-run those statutory and constitutional constraints and obtain unhindered access to 18,150 untested, never-disclosed wiretaps in aid of its civil case.<sup>11</sup>

The SEC’s only answer to that is to argue that Title III permits all disclosures not expressly forbidden. Stay Opp. Br. 7-12. But the federal government, in an appeal approved by the Solicitor General, told this Court exactly the opposite just last year, arguing that, “‘when addressing the 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.’” U.S. App. Br. at 16-17, *New York Times, supra* (endorsing *Smith*, 990 F.2d at 1018) (emphasis omitted).

The government was right last year. Allowing easy access to wiretaps via civil discovery or any other non-forbidden mechanism would render Congress’s

---

<sup>10</sup> Indeed, there is a substantial constitutional question whether wiretap authority could be housed outside the direct control of the Attorney General. *Cf. Morrison v. Olson*, 487 U.S. 654 (1988).

<sup>11</sup> In fact, the intercepts contain some profoundly private discussions about personal, medical, and family issues that should have been minimized as required by the statute. The injury from those minimization failures would only be compounded by disclosure to others.

“good cause” limitation on the disclosure of wiretap applications nugatory. Parties that cannot satisfy the good cause standard could obtain the applications – and the interceptions, to boot – by demonstrating nothing more than mere relevance in a civil discovery request. Likewise, the elaborate statutory constraints on the disclosure of wiretap contents codified in Sections 2517(1) through (3) would be honored more in the breach than in their observance. Section 2517(3)’s strict limitation to testimonial disclosures under oath in court proceedings after a motion to suppress is resolved would be nothing more than a Maginot Line, since parties would also be able to obtain in discovery non-testimonial disclosures not under oath not in court proceedings and before a motion to suppress. The district court’s order thus would leave vast amounts of Title III’s text with “no job to do.” *Doe v. Chao*, 540 U.S. 614, 623 (2004). That is statutory re-construction, and it “makes a mockery of the labors of Congress to tailor the statute with precision” to protect the “important public and individual concern for privacy.” *Huss*, 482 F.2d at 52.

To make matters worse, as happened here, discovery orders in collateral civil proceedings tear wiretaps out from “under the control and supervision of the authorizing court” in the criminal case that Congress expressly intended. 18 U.S.C. § 2510 note; *see* 18 U.S.C. § 2518(8)(a) (testimonial disclosures under Section 2517(3) should bear the district court’s seal).

In short, the ordered disclosure of more than 18,000 wiretapped conversations as part of routine civil discovery turns Title III's statutory scheme inside out by inviting the use of civil litigation to end run the extensive statutory prohibitions on disclosure that Congress prescribed and to force criminal defendants to make the very wiretap disclosures to a civil agency that the USAO itself cannot or will not make.

**3.     *The Disclosure Order Lacks Support in Precedent and Logic***

**a.     The cases cited by the SEC are inapt**

Both the SEC and the district court relied on this Court's decision in *In re Application of Newsday, Inc.*, 895 F.2d 74 (2d Cir. 1990), for the proposition that Section 2517 permits public "access by \* \* \* other means" to wiretaps. A177. But "other means" does not mean "any means." The "other means" that *Newsday* was talking about were Section 2517's exceptions for authorized law enforcement uses, 18 U.S.C. § 2517(1) and (2), which this Court held provided a means not just for internal law enforcement sharing of wiretap materials, but also public disclosure as part of a public filing. In particular, the Court authorized the use of wiretaps in a search warrant application filed as a "public document" as part of a court record. 895 F.2d at 77. Once those wiretap materials were lawfully made part of the public record as authorized by Section 2517, the public could exercise a common-law right of access "incident to, or after, their use under § 2517." *Id.* at 78.

That holding has no application here. The public right to access specific wiretap materials that were disclosed in a “public document” in accordance with Section 2517’s enumerated exceptions says nothing about whether a civil litigant can obtain wholesale access to thousands upon thousands of wiretap intercepts completely *outside* of Section 2517 and *prior to* (not “incident to, or after,” *ibid.*) any authorized disclosure under Section 2517. In fact, this Court stressed in *Newsday* that, “[a]side from these permitted uses [under Section 2517], Title III requires sealing of intercepted communications.” *Id.* at 77. Further, the Court specifically distinguished public access to wiretap materials included in a “public document” that was “filed in the court’s records,” *ibid.*, from efforts to obtain materials, such as those involved here, that have never been publicly disclosed in any form. *See New York Times*, 577 F.3d at 407 n.3 (reiterating that *Newsday* governs public access to materials already in the court record).

The district court’s reliance (A177) on *United States v. Fleming*, 547 F.2d 872 (5th Cir. 1977), is equally misplaced. *Fleming* “h[e]ld only that evidence derived from communications *lawfully* intercepted as part of a bona fide criminal investigation that results in a taxpayer’s conviction may properly be admitted in a civil tax proceeding, *at least when the evidence is already part of the public record of the prior criminal prosecution.*” *Id.* at 875 (emphases added). That is precisely Mr. Rajaratnam’s and Ms. Chiesi’s point. In stark contrast to the situation here, the

disclosure in *Fleming* postdated the criminal trial, was limited to information publicly disclosed in that trial, and involved wiretaps the lawfulness of which was not in dispute. *Id.* at 873, 875. None of those conditions are present here.

The court's invocation (A177) of dictum in *In re High Fructose Corn Syrup Antitrust Litigation*, 216 F.3d 621 (7th Cir. 2000), fares no better, because that case involved consensual recordings to which Title III does not apply. *Id.* at 624. Where Title III does apply, the rule in the Seventh Circuit is that "what is not permitted is forbidden." *Dorfman*, 690 F.2d at 1232.

**b. There is no relevant informational imbalance**

The district court's central reason for opening wiretaps up to civil discovery was to cure a purported informational disparity between the defendants who possess the wiretaps and the SEC and other litigants. A177-A178. That rationale fails for five reasons.

*First*, any asymmetrical access to wiretap information is entirely of Congress's design. The defendants possess the wiretap material solely by virtue of their status as criminal defendants vested with the constitutional right to defend themselves in a criminal prosecution. The reason the SEC does not have wiretaps to litigate its civil case is because Congress specifically withheld wiretap authority from the SEC and determined as a matter of law that wiretaps are not necessary to prosecute insider trading and securities fraud. *See* 18 U.S.C. § 2516. The SEC's

independent choice to file its civil case simultaneously with the initiation of the criminal action does not and cannot alter that congressional judgment. Indeed, to hold that it takes nothing more than the concurrent timing of civil and criminal litigation and a discovery request to empower every government agency and every interested private litigant to obtain wiretap materials would turn Title III into the very type of general warrant for the use of wiretaps that the Supreme Court has condemned. *Berger*, 388 U.S. at 58-59.<sup>12</sup>

*Second*, the perceived “unfairness” is entirely hypothesized. *See Stay Opp.* Br. 12-13. If the SEC wants to learn about the substance of and participants in Mr. Rajaratnam’s and Ms. Chiesi’s telephone calls, it can depose them in civil discovery. To be sure, the defendants would likely invoke the Fifth Amendment because of the pending criminal proceeding. But that problem is entirely of the SEC’s own making. Had it waited to file its civil suit until after the criminal case concluded, as is the usual practice, then there would have been no Fifth Amendment barrier to its discovery. The SEC’s litigation tactics provide no sound reason to contort Title III’s longstanding protections for individual privacy.

---

<sup>12</sup> Given the scores of federal agencies with civil enforcement powers that overlap with substantive crimes (*e.g.*, the SEC, IRS, FTC, DHS, DOJ, Treasury, Inspectors General, False Claims Act offices), and their unilateral control over the timing of their litigation, the district court’s order opens a gaping hole in Title III’s previously strong wall against public disclosure.



Furthermore, the supposedly unfair uses of the wiretap materials by the defendants about which the SEC complains (Stay Opp. Br. 13) are all uses by the defendants that are related to the preparation of their defense in the *criminal* case, not the civil case. Those uses, of course, are protected by the defendants' Fifth and Sixth Amendment rights to defend themselves at trial. And even in that respect, the defendants have not disclosed the wiretap intercepts to any co-defendants or to anyone else outside their legal defense team. In the SEC case, the defendants have committed to *not* using the wiretaps in their defense and, indeed, are moving to suppress the wiretaps in the criminal case, which would bar their use in any proceeding. 18 U.S.C. § 2518(10). Thus, if anything is unfair, it is the SEC's effort to whipsaw criminal defendants between exercising their constitutional rights to defend themselves in the criminal action and surrendering their constitutional and statutory privacy rights as defendants in a parallel civil action filed by the government.

Moreover, should an attempt to introduce a particular wiretap intercept as evidence ever materialize, the court could address the informational concern through a motion to preclude or a disclosure order tailored to the particular usage. Given the profound privacy and fair trial rights at stake, that course is far preferable to releasing all 18,150 intercepts now based on nothing more than the specter of hypothesized use.

*Third*, the quest for informational equality is misplaced. There certainly is no such parity for the defendants. In this litigation, the SEC's close partnership with the USAO has provided it access to witnesses, such as cooperators, to whom the defendants have no access. Beyond that, the law has long recognized and tolerated differential rules of access to certain types of sensitive information for parties in criminal and civil cases, whether grand jury material that defendants have but civil agencies do not, *United States v. Sells Eng'g*, 463 U.S. 418, 445-446 (1983); *Douglas Oil Co. of California v. Petrol Stops Nw.*, 441 U.S. 211, 222-224 (1979), or materials protected by executive privilege that criminal defendants can obtain, but civil litigants cannot, *compare United States v. Nixon*, 418 U.S. 683 (1974), *with Cheney v. U.S. District Court*, 542 U.S. 367, 383 (2004) (noting the "fundamental difference" under *Nixon* between civil and criminal discovery).

*Fourth*, contrary to the district court's conclusion, A178, there is no special exception authorizing disclosure of Title III material through discovery when the requesting party is a government agency rather than a private litigant. Indeed, the notion that the government is entitled to greater discovery rights than a private party belies the fundamental premise of the SEC's argument – namely, that access to the wiretaps is necessary to ensure "even-handed discovery and trial preparation" and "mutual knowledge" by all parties to litigation. Stay Opp. Br. 1. The SEC cannot have it both ways.

Beyond that, the district court's and the SEC's reasoning makes no sense in relation to the ruling at issue here, which ordered disclosure not only to the SEC but also to fourteen private parties. More importantly, the Supreme Court has already rejected the identical argument in the grand jury context, holding that statutorily protected material obtained in a criminal case cannot be released to civil enforcement agencies, in part because disclosures in civil litigation inherently "increase the risk of inadvertent or illegal release." *Sells Eng'g*, 463 U.S. at 432.<sup>13</sup>

*Fifth* and finally, the disclosure is not needed to prevent significant informational harm to the SEC or other litigants. Contrary to the district court's assumption (A175), the defendants have never "agree[d] that the recordings are highly relevant to this case" and, in fact, have lodged relevance objections to them. *See* Letter from Terence Lynam to Hon. Jed S. Rakoff, *supra*, note 6. The USAO agrees that "tons and tons" of these calls ultimately will not be used in the criminal

---

<sup>13</sup> The risk is real. In this case, the government has already improperly disclosed Title III information at the public bail hearing without court authorization and without prior notification to the defendants in violation of 18 U.S.C. § 2518(9). *See United States v. Giordano*, 158 F. Supp. 2d 242, 246 (D. Conn. 2001) ("Until the defendant has had this opportunity [to inspect the order authorizing the surveillance and the documents supporting the request for authorization], the fruits of an electronic surveillance should not be publicly disseminated."). In addition, the USAO has admitted that it improperly disclosed 21 wiretap communications to the SEC on December 15, 2009. On April 20, 2010, counsel for Mr. Rajaratnam sent a letter to Attorney General Eric Holder objecting to approximately two dozen improper disclosures and leaks of material in this case.

case, A184, and both Mr. Rajaratnam and Ms. Chiesi will be making minimization objections in their motions to suppress.

There thus has been no determination that all 18,150 wiretaps, or even a statistically significant percentage of them, have any relevance to this action. Indeed, unless the simultaneous civil and criminal prosecutions were calculated to end run Title III, then the SEC must have initiated this action and intended to litigate it without the wiretaps from the outset, just as it has presumably done in every other insider trading action in its history. *See* Prepared Remarks for Preet Bharara, U.S. Attorney, S.D.N.Y., October 16, 2009 (“[T]his case represents the first time that court-authorized wiretaps have been used to target significant insider trading on Wall Street.”), *available at* <http://www.justice.gov/usao/nys/hedgefund/hedgefundinsidertradingremarks101609.pdf>. Accordingly, far from prejudicing its case, denying the SEC a windfall use of wiretap materials simply keeps the SEC where Congress and Title III left it – in the same litigation position it has occupied in every one of its prior insider trading actions for the last half century.

***4. Release of the Wiretaps Would Significantly Harm the Defendants’ Privacy and Fair Trial Rights***

Opening wiretaps to disclosure in civil discovery would profoundly erode “the protection of privacy” that was the “overriding congressional concern” in enacting Title III, *Gelbard*, 408 U.S. at 48 – a concern rooted in fundamental Fourth Amendment protections, *see Katz v. United States*, 389 U.S. 347, 357-359

(1967); *NBC*, 735 F.2d at 53 (Title III enacted in response to *Katz*). Importantly, the privacy interests at stake are not just those of Mr. Rajaratnam and Ms. Chiesi, but also of the more than 550 participants in their telephone calls, whose private conversations will now become freely accessible reading material for any civil litigant with a well-timed lawsuit.

Allowing the disclosure of wiretaps in collateral civil litigation while a criminal prosecution is pending would cause irreparable harm to the defendants' Title III and Fourth Amendment rights to seek suppression of the wiretaps, and to their Fifth and Sixth Amendment rights to a fair criminal trial. Indeed, if suppression were later granted in the criminal case, it would be virtually impossible to unscramble the impact of disclosure on potential witnesses and parties, and derivative uses of the material after the fact. Nor could the problem be avoided by having the suppression motion adjudicated first in the civil case. It makes little sense for a civil litigation schedule to drive judicial decisions that sit at the core of the criminal law enforcement process, and even less sense to have suppression motions adjudicated in cases to which the USAO is not a party.

Throwing a discovery-stage-only protective order over the disclosure does not solve the problem either. A46, A178. At best, the protective order merely slows the bleeding of privacy interests caused by disclosure; it does nothing to prevent the privacy injury in the first instance. As the Supreme Court has

recognized, the “disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself,” *Bartnicki*, 532 U.S. at 533, and thus “[e]ach time the illicitly obtained recording is replayed to a new and different listener, the scope of the invasion widens and the aggrieved party’s injury is aggravated,” *Fultz v. Gilliam*, 942 F.2d 396, 402 (6th Cir. 1991). Title III reflects that understanding, treating “the victim’s privacy as an end in itself,” and “recogniz[ing] that the invasion of privacy is not over when the interception occurs, but is compounded by disclosure.” *Providence Journal Co. v. FBI*, 602 F.2d 1010, 1013 (1st Cir. 1979). It is precisely for that reason that Title III does not require a threshold volume of disclosures before its protections attach. Furthermore, no protective order can forestall the snowballing volume of disclosures that will occur once access to wiretap materials is thrown open to any would-be litigant willing to time a civil lawsuit to coincide with a criminal prosecution.

At bottom, the district court’s order making wiretaps available for the asking in civil discovery defies Title III’s text, structure, and precedent, and will derail Title III’s carefully calibrated balancing of individual privacy and the genuine needs of criminal law enforcement. If such a profound change is to be made in wiretap law, it should be made by Congress. Until then, the language of Title III simply does not support the court’s order compelling disclosure.

### **III. IN THE ALTERNATIVE, A WRIT OF MANDAMUS SHOULD BE GRANTED**

The district court's order equally merits reversal or vacatur through the issuance of a writ of mandamus both because it was a clear abuse of discretion and because it involves the type of exceptionally important discovery question for which this Court's pre-judgment correction is critical. *See Mohawk*, 130 S. Ct. at 608 (mandamus is an alternative means to seek review of disclosure orders).<sup>14</sup>

#### **A. The Order Was A Clear Abuse Of Discretion That Cannot Otherwise Be Remedied**

Mandamus is proper when (i) “the party seeking issuance of the writ \* \* \* [has] no other adequate means to attain the relief he desires”; (ii) the petitioner shows “that his right to issuance of the writ is clear and indisputable”; and (iii) “the issuing court, in the exercise of its discretion, [is] satisfied that the writ is appropriate under the circumstances.” *Cheney*, 542 U.S. at 380-381. All three factors are satisfied here.

*First*, absent exercise of this Court's appellate jurisdiction under *Gerena*, Mr. Rajaratnam and Ms. Chiesi have no adequate alternative remedy for the constitutional and statutory rights that will be irretrievably lost once disclosure is made. The district court denied their motion for certification under 28 U.S.C.

---

<sup>14</sup> This Court may exercise its mandamus power without resolving the question of appellate jurisdiction. *Stein v. KPMG, LLP*, 486 F.3d 753, 759 (2d Cir. 2007).

§ 1292(b) as “frivolous,” A181, notwithstanding the Supreme Court’s direction just two months earlier that “district courts should not hesitate to certify an interlocutory appeal” in a case that presents a “new legal question or is of special consequence,” *Mohawk*, 130 S. Ct. at 607. As explained in Point I, *supra*, a post-judgment appeal would not provide a sufficient remedy either, because it could not “unsay the confidential information that [will have] been revealed” as a result of compelled disclosure. *In re von Bulow*, 828 F.2d at 99; *see also id.* at 98 (“Compliance with the order destroys the right sought to be protected.”). Nor could such an appeal reverse the profound injury to their fair trial rights that would result from disclosing the wiretaps to numerous potential witnesses in the criminal case or from leaks of the wiretapped conversations to the press in a case of such high profile. The Court also has no alternative avenue for protecting the rights of the more than 550 other individuals whose private conversations are threatened with disclosure outside of Title III’s framework.

Review by way of a contempt citation is not feasible either. *See Mohawk*, 130 S. Ct. at 608. Any contempt order intended to coerce compliance with a discovery order would be civil in nature. *See, e.g., New York State Nat’l Org. for Women v. Terry*, 886 F.2d 1339, 1351 (2d Cir. 1989). A civil contempt order against a party to the litigation is not appealable until the entry of final judgment,



*OSRecovery, Inc. v. One Groupe Int'l, Inc.*, 462 F.3d 87, 92 (2d Cir. 2006), which, at that juncture, would be “an exercise in futility,” *In re von Bulow*, 828 F.2d at 99.

*Second*, in light of the district court’s sharp break from both the text of Title III and four decades of Title III jurisprudence from this and other courts, the disclosure order is ““a clear abuse of discretion,”” *Mohawk*, 130 S. Ct. at 608, making Mr. Rajaratnam’s and Ms. Chiesi’s right to mandamus clear and indisputable. Whatever debates about Title III’s protections may occur at the boundaries, “boundaries there must be,” and the atextual, pre-suppression, pre-criminal trial, pre-Title III disclosure order issued here by a court lacking jurisdiction over the sealed wiretaps “is clearly outside those boundaries.” *Stein v. KPMG, LLP*, 486 F.3d 753, 760 (2d Cir. 2007). Because the order thus conflicts with even the most impoverished conception of the statute’s protections, issuance of the writ is warranted.

*Third*, “the reasons underlying the traditional reluctance to resort to the writ are either not present or favor granting the writ.” *Ibid*. Adjudication of this matter will not require any complicated inquiry into the proceedings below, as it involves pure questions of law. Nor, given the district court’s recent delay of the civil trial, would issuance of the writ frustrate or complicate ongoing litigation. Furthermore, resolution of this matter now will promote the efficient handling of both this case and the criminal proceeding by resolving the question of disclosure (i) before

unauthorized disclosures pervade the proceedings, (ii) before the SEC is required to establish a duplicative “clean” litigation team, unexposed to the wiretaps, to serve as backup litigators if the disclosure order is later reversed, *see* A205, A210, and (iii) before enormous litigant and judicial resources are invested in two lengthy and complex trials that will just have to be reversed later.

### **B. Supervisory Mandamus Is Warranted**

Mandamus is separately warranted because the court’s pretrial order is “the first of its kind in any reported decision in the federal courts,” and raises an important “issue of first impression that call[s] for the construction and application” of a legal rule “in a new context.” *Schlagenhauf v. Holder*, 379 U.S. 104, 110-111 (1964). In such cases, the Court may review “all of the issues presented by the petition,” regardless of whether they independently would warrant mandamus review, in order to “avoid piecemeal litigation and to settle new and important problems.” *Id.* at 111.

Those principles apply with particular force in the discovery context. This Court has consistently ruled that, “[w]hen a discovery question is of extraordinary significance or there is extreme need for reversal of the district court’s mandate before the case goes to judgment, the writ of mandamus provides an escape hatch from the finality rule.” *In re von Bulow*, 828 F.2d at 97. In those circumstances, “mandamus provides a logical method by which to supervise the administration of

justice within the Circuit.” *Ibid.* Thus, this Court has approved the use of mandamus to correct defective discovery orders where “the petitioner demonstrates ‘(1) the presence of a novel and significant question of law; (2) the inadequacy of other available remedies; and (3) the presence of a legal issue whose resolution will aid in the administration of justice.’” *United States v. Coppa*, 267 F.3d 132, 137-138 (2d Cir. 2001); *see SEC v. Glotzer*, 374 F.3d 184, 187 (2d Cir. 2004). Each of those factors is met here.

*First*, this case presents a novel and significant issue of first impression because no court, to defendants’ knowledge, has ever ordered such a wholesale disclosure of wiretap materials in civil litigation, prior to resolution of a motion to suppress, release of the materials under Title III, and conclusion of the criminal proceedings, and without the participation of the judge superintending the sealed wiretaps. Indeed, the unprecedented nature of the district court’s ruling is underscored by both the district court’s and the SEC’s failure to cite even a single case from any point in Title III’s four-decade-long history in which a court ordered the wholesale disclosure of untested wiretaps as part of routine civil discovery. The sheer novelty and expansiveness of the district court’s ruling, not to mention its implications, place this case squarely in line with this Court’s past exercises of its mandamus authority. *See, e.g., In re Sims*, 534 F.3d 117, 129 (2d Cir. 2008) (granting mandamus petition that raised a “novel and far-reaching question”);

*Coppa*, 267 F.3d at 138 (granting mandamus petition where Court’s “research \* \* \* unearthed no case from a Court of Appeals that [had] adopted the District Court’s rule”); *In re von Bulow*, 828 F.2d at 97 (granting petition where district court’s decision “raise[d] an issue which, so far as discernible, [had] not been previously litigated in this Circuit,” and represented a “novel and unprecedented ruling”); *see also Orange County Water Dist. v. Unocal Corp.*, 584 F.3d 43, 48 (2d Cir. 2009) (“unique nature” of mandamus petition “counsel[ed] in favor of review”).

*Second*, as explained *supra*, no alternative remedial avenue remains open (unless this Court exercises appellate jurisdiction).

*Third*, resolution of this ““important, undecided issue will forestall future error in trial courts, eliminate uncertainty and add importantly to the efficient administration of justice.”” *In re von Bulow*, 828 F.2d at 99. The district court’s holding that “principles of civil discovery,” A177, are sufficient to override the protections of Title III profoundly unsettles the law and opens the door to a feeding frenzy of parasitic civil litigation against criminal defendants by non-Title III federal agencies, state agencies, private parties, and the media seeking access to wiretap materials long understood to be protected by Title III. *Cf. Chase Manhattan Bank, N.A. v. Turner & Newell, PLC*, 964 F.2d 159, 164 (2d Cir. 1992) (granting writ because, “were we to fail to act now, use of the procedure might become widespread”).

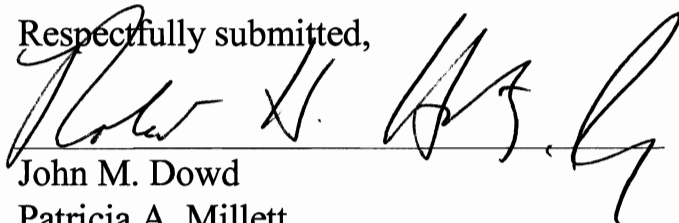
Moreover, that disruption of settled principles is not readily confined to the discovery context. Indeed, if wiretap materials are freely available for civil litigants' asking, then it will be hard to continue to explain why interests of constitutional stature like the First Amendment do not warrant equivalent respect. *Contrast New York Times*, 577 F.3d at 410 (no First Amendment right of access to wiretap applications); *cf. Bartnicki*, 532 U.S. at 534 (recognizing that, in some circumstances, First Amendment interests would outweigh privacy interests). Given the far reaching effect of the district court's reasoning on the administration of justice in this Circuit, the decision "merits prompt attention and resolution" through the exercise of this Court's mandamus power. *In re von Bulow*, 828 F.2d at 100.

### CONCLUSION

For the foregoing reasons, the district court's disclosure order of February 9, 2010, should be reversed or, in the alternative, vacated by a writ of mandamus.

Dated: April 23, 2010  
New York, New York

Respectfully submitted,

A handwritten signature in black ink, appearing to read "John M. Dowd", is written over a horizontal line.

John M. Dowd  
Patricia A. Millett  
Terence J. Lynam  
William E. White  
Kevin R. Amer

Isaac J. Lidsky  
Anne J. Lee  
Akin Gump Strauss Hauer & Feld LLP  
1333 New Hampshire Ave, NW  
Washington, DC 20036  
(202) 887-4386 (phone)  
(202) 887-4288 (fax)

Robert H. Hotz, Jr.  
Samidh Guha  
Akin Gump Strauss Hauer & Feld LLP  
One Bryant Park  
New York, NY 10036  
(212) 872-1028 (phone)  
(212) 872-1002 (fax)

*Attorneys for Raj Rajaratnam*

Alan R. Kaufman  
James M. Keneally  
Thomas B. Kinzler  
Kelley Drye & Warren LLP  
101 Park Avenue  
New York, NY 10178  
(212) 808-5195 (phone)  
(212) 808-7897 (fax)

*Attorneys for Danielle Chiesi*

## CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 13,614 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Office Word 2003 in 14-point Times New Roman font for the main text, and 14-point Times New Roman font for the footnotes.

A handwritten signature in black ink, appearing to read "Robert H. Hotz, Jr.", written in a cursive style.

---

Robert H. Hotz, Jr.

# **ADDENDUM**



## TABLE OF CONTENTS

U.S. Constitution, amendment IV .....	1a
18 U.S.C. §§ 2510-2522 .....	2a
Federal Rule of Civil Procedure 26 .....	25a

## 1a



U.S.C.A. Const. Amend. IV-Search and Seizure

Page 1



United States Code Annotated Currentness

Constitution of the United States

Annotated

Amendment IV. Searches and Seizures (Refs &amp; Annos)

→ **Amendment IV. Search and Seizure**

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Current through P.L. 111-156 (excluding P.L. 111-148 and 111-152) approved 4-7-10

Westlaw. (C) 2010 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

END OF DOCUMENT

© 2010 Thomson Reuters. No Claim to Orig. US Gov. Works.

States law, in the same manner as other administrative regulations.

“(D) Nothing in this section shall be construed to affect the constitutional functions and responsibilities of Congress and the judicial branch of the United States.

“(4) DEFINITIONS.—In this subsection:

“(A) GENEVA CONVENTIONS.—The term ‘Geneva Conventions’ means—

“(i) the Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, done at Geneva August 12, 1949 (6 UST 3217);

“(ii) the Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea, done at Geneva August 12, 1949 (6 UST 3217);

“(iii) the Convention Relative to the Treatment of Prisoners of War, done at Geneva August 12, 1949 (6 UST 3316); and

“(iv) the Convention Relative to the Protection of Civilian Persons in Time of War, done at Geneva August 12, 1949 (6 UST 3516).

“(B) THIRD GENEVA CONVENTION.—The term ‘Third Geneva Convention’ means the international convention referred to in subparagraph (A)(iii).”

## CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.	Definitions.
2510.	Interception and disclosure of wire, oral, or electronic communications prohibited.
2511.	Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.
2512.	Confiscation of wire, oral, or electronic communication intercepting devices.
2513.	Repealed.]
[2514.	Prohibition of use as evidence of intercepted wire or oral communications.
2515.	Authorization for interception of wire, oral, or electronic communications.
2516.	Authorization for disclosure and use of intercepted wire, oral, or electronic communications.
2517.	Procedure for interception of wire, oral, or electronic communications.
2518.	Reports concerning intercepted wire, oral, or electronic communications.
2519.	Recovery of civil damages authorized.
2520.	Injunction against illegal interception.
2521.	Enforcement of the Communications Assistance for Law Enforcement Act.
2522.	

### AMENDMENTS

1994—Pub. L. 103-414, title II, § 201(b)(3), Oct. 25, 1994, 108 Stat. 4290, added item 2522.

1988—Pub. L. 100-690, title VII, § 7035, Nov. 18, 1988, 102 Stat. 4398, substituted “wire, oral, or electronic” for “wire or oral” in items 2511, 2512, 2513, 2516, 2517, 2518, and 2519.

1986—Pub. L. 99-508, title I, §§ 101(c)(2), 110(b), Oct. 21, 1986, 100 Stat. 1851, 1859, inserted “AND ELECTRONIC COMMUNICATIONS” in chapter heading and added item 2521.

1970—Pub. L. 91-452, title II, § 227(b), Oct. 15, 1970, 84 Stat. 930, struck out item 2514 “Immunity of witnesses”, which section was repealed four years following the sixtieth day after Oct. 15, 1970.

1968—Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 212, added chapter 119 and items 2510 to 2520.

### § 2510. Definitions

As used in this chapter—

(1) “wire communication” means any aural transfer made in whole or in part through the

use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.<sup>1</sup>

(5) “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) “person” means 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;

(7) “Investigative or law enforcement officer” means 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;

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) “Judge of competent jurisdiction” means—

<sup>1</sup> So in original. The period probably should be a semicolon.

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not

exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"—

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

(Added Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 212; amended Pub. L. 99-508, title I, § 101(a), (c)(1)(A), (4), Oct. 21, 1986, 100 Stat. 1848, 1851; Pub. L. 103-414, title II, §§ 202(a), 203, Oct. 25, 1994, 108 Stat. 4290, 4291; Pub. L. 104-132, title VII, § 731, Apr. 24, 1996, 110 Stat. 1303; Pub. L. 107-56, title II, §§ 203(b)(2), 209(1), 217(1), Oct. 26, 2001, 115 Stat. 280, 283, 290; Pub. L. 107-108, title III, § 314(b), Dec. 28, 2001, 115 Stat. 1402; Pub. L. 107-273, div. B, title IV, § 4002(e)(10), Nov. 2, 2002, 116 Stat. 1810.)

## REFERENCES IN TEXT

Section 3 of the Communications Act of 1934, referred to in par. (10), is classified to section 153 of Title 47, Telegraphs, Telephones, and Radiotelegraphs.

## AMENDMENTS

2002—Par. (10). Pub. L. 107-273 substituted “has the meaning given that term in section 3 of the Communications Act of 1934,” for “shall have the same meaning which is given the term ‘common carrier’ by section 153(h) of title 47 of the United States Code;”.

2001—Par. (1). Pub. L. 107-56, § 209(1)(A), struck out “and such term includes any electronic storage of such communication” before semicolon at end.

Par. (14). Pub. L. 107-56, § 209(1)(B), inserted “wire or” after “transmission of”.

Par. (19). Pub. L. 107-108 inserted “, for purposes of section 2517(6) of this title,” before “means” in introductory provisions.

Pub. L. 107-56, § 203(b)(2), added par. (19).

Pars. (20), (21). Pub. L. 107-56, § 217(1), added pars. (20) and (21).

1996—Par. (12)(D). Pub. L. 104-132, § 731(1), added subpar. (D).

Par. (16)(F). Pub. L. 104-132, § 731(2), struck out subpar. (F) which read as follows: “an electronic communication;”.

1994—Par. (1). Pub. L. 103-414, § 202(a)(1), struck out before semicolon at end “, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit”.

Par. (12). Pub. L. 103-414, § 202(a)(2), redesignated subpars. (B) to (D) as (A) to (C), respectively, and struck out former subpar. (A) which read as follows: “the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;”.

Par. (16)(F). Pub. L. 103-414, § 203, added subpar. (F).

1986—Par. (1). Pub. L. 99-508, § 101(a)(1), substituted “any aural transfer” for “any communication”, inserted “(including the use of such connection in a switching station)” after “reception”, struck out “as a common carrier” after “person engaged”, and inserted “or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit” before the semicolon at end.

Par. (2). Pub. L. 99-508, § 101(a)(2), inserted “, but such term does not include any electronic communication” before the semicolon at end.

Par. (4). Pub. L. 99-508, § 101(a)(3), inserted “or other” after “aural” and “, electronic,” after “wire”.

Par. (5). Pub. L. 99-508, § 101(a)(4), (c)(1)(A), (4), substituted “wire, oral, or electronic” for “wire or oral” in introductory provisions, substituted “provider of wire or electronic communication service” for “communications common carrier” in subpars. (a)(i) and (ii), and inserted “or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business” before the semicolon in subpar. (a)(i).

Par. (8). Pub. L. 99-508, § 101(a)(5), (c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral” and struck out “identity of the parties to such communication or the existence,” after “concerning the”.

Pars. (9)(b), (11). Pub. L. 99-508, § 101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral”.

Pars. (12) to (18). Pub. L. 99-508, § 101(a)(6), added pars. (12) to (18).

## TERMINATION DATE OF 2001 AMENDMENT

Pub. L. 107-56, title II, § 224, Oct. 26, 2001, 115 Stat. 295, as amended by Pub. L. 109-160, § 1, Dec. 30, 2005, 119 Stat. 2957; Pub. L. 109-170, § 1, Feb. 3, 2006, 120 Stat. 3, which provided that title II of Pub. L. 107-56 and the amend-

ments made by that title would cease to have effect on Mar. 10, 2006, with certain exceptions, was repealed by Pub. L. 109-177, title I, § 102(a), Mar. 9, 2006, 120 Stat. 194.

## EFFECTIVE DATE OF 1986 AMENDMENT

Section 111 of title I of Pub. L. 99-508 provided that: “(a) IN GENERAL.—Except as provided in subsection (b) or (c), this title and the amendments made by this title [enacting sections 2521 and 3117 of this title, amending this section and sections 2232, 2511 to 2513, and 2516 to 2520 of this title, and enacting provisions set out as notes under this section] shall take effect 90 days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

“(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

“(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

“(2) the date two years after the date of the enactment of this Act [Oct. 21, 1986].

“(c) EFFECTIVE DATE FOR CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.—Section 104 of this Act [amending section 2516 of this title] shall take effect on the date of enactment of this Act [Oct. 21, 1986].”

## SHORT TITLE OF 1997 AMENDMENT

Pub. L. 105-112, § 1, Nov. 21, 1997, 111 Stat. 2273, provided that: “This Act [amending section 2512 of this title] may be cited as the ‘Law Enforcement Technology Advertisement Clarification Act of 1997.’”

## SHORT TITLE OF 1986 AMENDMENT

Section 1 of Pub. L. 99-508 provided that: “This Act [enacting sections 1367, 2521, 2701 to 2710, 3117, and 3121 to 3126 of this title, amending sections 2232, 2511 to 2513, and 2516 to 2520 of this title, and enacting provisions set out as notes under this section and sections 2701 and 3121 of this title] may be cited as the ‘Electronic Communications Privacy Act of 1986.’”

## INTELLIGENCE ACTIVITIES

Section 107 of Pub. L. 99-508 provided that:

“(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act [see Short Title of 1986 Amendment note above] constitutes authority for the conduct of any intelligence activity.

“(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

“(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

“(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. 1801 et seq.]; or

“(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.”

## CONGRESSIONAL FINDINGS

Section 801 of Pub. L. 90-351 provided that: “On the basis of its own investigations and of published studies, the Congress makes the following findings:

"(a) Wire communications are normally conducted through the use of facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings, and by persons whose activities affect interstate commerce. The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

"(b) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

"(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

"(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused."

#### NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE

Section 804 of Pub. L. 90-351, as amended by Pub. L. 91-452, title XII, §1212, Oct. 15, 1970, 84 Stat. 961; Pub. L. 91-644, title VI, §20, Jan. 2, 1971, 84 Stat. 1892; Pub. L. 93-609, §§1-4, Jan. 2, 1975, 88 Stat. 1972, 1973; Pub. L. 94-176, Dec. 23, 1975, 89 Stat. 1031, established a National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, provided for its membership, Chairman, powers and functions, compensation and allowances, required the Commission to study and review the operation of the provisions of this chapter to determine their effectiveness and to submit interim reports and a final report to the President and to the Congress of its findings and recommendations on or before Apr. 30, 1976, and also provided for its termination sixty days after submission of the final report.

#### § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except

for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such

interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies

monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

(Added Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 213; amended Pub. L. 91-358, title II, § 211(a), July 29, 1970, 84 Stat. 654; Pub. L. 95-511, title II, § 201(a)-(c), Oct. 25, 1978, 92 Stat. 1796, 1797; Pub. L. 98-549, § 6(b)(2), Oct. 30, 1984, 98 Stat. 2804; Pub. L. 99-508, title I, §§ 101(b), (c)(1), (5), (6), (d), (f)[(1)], 102, Oct. 21, 1986, 100 Stat. 1849, 1851-1853; Pub. L. 103-322, title XXXII, § 320901, title XXXIII, § 330016(1)(G), Sept. 13, 1994, 108 Stat. 2123, 2147; Pub. L. 103-414, title II, §§ 202(b), 204, 205, Oct. 25, 1994, 108 Stat. 4290, 4291; Pub. L. 104-294, title VI, § 604(b)(42), Oct. 11, 1996, 110 Stat. 3509; Pub. L. 107-56, title II, §§ 204, 217(2), Oct. 26, 2001, 115 Stat. 281, 291; Pub. L. 107-296, title II, § 225(h)(2), (j)(1), Nov. 25, 2002, 116 Stat. 2158.)

#### REFERENCES IN TEXT

The Foreign Intelligence Surveillance Act of 1978, referred to in par. (2)(e), (f), is Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, which is classified principally to chapter 36 (§ 1801 et seq.) of Title 50, War and National Defense. Section 101 of the Foreign Intelligence Surveillance



Act of 1978, referred to in par. (2)(a)(ii), (e), and (f), is classified to section 1801 of Title 50. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of Title 50 and Tables.

Sections 633, 705, and 706 of the Communications Act of 1934, referred to in par. (2)(e), (f), (g)(iii), are classified to sections 553, 605, and 606 of Title 47, Telegraphs, Telephones, and Radiotelegraphs, respectively.

#### AMENDMENTS

2002—Par. (2)(a)(ii). Pub. L. 107-296, § 225(h)(2), inserted “, statutory authorization,” after “terms of a court order” in concluding provisions.

Par. (4)(b), (c). Pub. L. 107-296, § 225(j)(1), redesignated subpar. (c) as (b) and struck out former subpar. (b) which read as follows: “If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then—

“(i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

“(ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.”

2001—Par. (2)(f). Pub. L. 107-56, § 204, substituted “this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934” for “this chapter or chapter 121, or section 705 of the Communications Act of 1934” and “wire, oral, and electronic communications” for “wire and oral communications”.

Par. (2)(i). Pub. L. 107-56, § 217(2), added subpar. (i).

1996—Par. (1)(e)(i). Pub. L. 104-294 substituted “sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter” for “sections 2511(2)(A)(ii), 2511(b)-(c), 2511(e), 2516, and 2518 of this subchapter”.

1994—Par. (1)(e). Pub. L. 103-322, § 320901, added par. (1)(e).

Par. (2)(a)(i). Pub. L. 103-414, § 205, inserted “or electronic” after “transmission of a wire”.

Par. (4)(b). Pub. L. 103-414, § 204, in introductory provisions substituted “, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then” for “or encrypted, then”.

Par. (4)(b)(i). Pub. L. 103-414, § 202(b)(1), inserted “a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit,” after “cellular telephone communication.”

Par. (4)(b)(ii). Pub. L. 103-414, § 202(b)(2), inserted “a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit,” after “cellular telephone communication.”

Pub. L. 103-322, § 330016(1)(G), substituted “fined under this title” for “fined not more than \$500”.

1986—Pub. L. 99-508, § 101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral” in section catchline.

Par. (1). Pub. L. 99-508, § 101(c)(1)(A), (d)(1), (f)(1), substituted “intentionally” for “fully” in subpars. (a) to (d) and “wire, oral, or electronic” for “wire or oral” wherever appearing in subpars. (a), (c), and (d),

and in concluding provisions substituted “shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)” for “shall be fined not more than \$10,000 or imprisoned not more than five years, or both”.

Par. (2)(a)(i). Pub. L. 99-508, § 101(c)(5), substituted “a provider of wire or electronic communication service” for “any communication common carrier” and “of the provider of that service, except that a provider of wire communication service to the public” for “of the carrier of such communication: *Provided*, That said communication common carriers”.

Par. (2)(a)(ii). Pub. L. 99-508, § 101(b)(1), (c)(1)(A), (6), substituted “providers of wire or electronic communication service” for “communication common carriers”, “wire, oral, or electronic” for “wire or oral”, “if such provider” for “if the common carrier”, “provider of wire or electronic communication service” for “communication common carrier” wherever appearing, “such disclosure” for “violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof”, “render such person liable” for “render the carrier liable”, and “a court order or certification under this chapter” for “an order or certification under this subparagraph” in two places.

Par. (2)(b). Pub. L. 99-508, § 101(c)(1)(B), inserted “or electronic” after “wire”.

Par. (2)(c). Pub. L. 99-508, § 101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral”.

Par. (2)(d). Pub. L. 99-508, § 101(b)(2), (c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral” and struck out “or for the purpose of committing any other injurious act” after “of any State”.

Par. (2)(f). Pub. L. 99-508, § 101(b)(3), inserted “or chapter 121” in two places and substituted “foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means” for “foreign communications by a means”.

Par. (2)(g), (h). Pub. L. 99-508, § 101(b)(4), added subpars. (g) and (h).

Par. (3). Pub. L. 99-508, § 102, added par. (3).

Pars. (4), (5). Pub. L. 99-508, § 101(d)(2), added pars. (4) and (5).

1984—Par. (2)(e). Pub. L. 98-549, § 6(b)(2)(A), substituted “section 705 or 706” for “section 605 or 606”.

Par. (2)(f). Pub. L. 98-549, § 6(b)(2)(B), substituted “section 705” for “section 605”.

1978—Par. (2)(a)(ii). Pub. L. 95-511, § 201(a), substituted provisions authorizing communication common carriers etc., to provide information to designated persons, prohibiting disclosure of intercepted information, and rendering violators civilly liable for provision exempting communication common carriers from criminality for giving information to designated officers.

Par. (2)(e), (f). Pub. L. 95-511, § 201(b), added par. (2)(e) and (f).

Par. (3). Pub. L. 95-511, § 201(c), struck out par. (3) which provided that nothing in this chapter or section 605 of title 47 limited the President’s constitutional power to gather necessary intelligence to protect the national security and stated the conditions necessary for the reception into evidence and disclosure of communications intercepted by the President.

1970—Par. (2)(a). Pub. L. 91-358 designated existing provisions as cl. (i) and added cl. (ii).

#### EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

#### EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104-294 effective Sept. 13, 1994, see section 604(d) of Pub. L. 104-294, set out as a note under section 13 of this title.

#### EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court

order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

#### EFFECTIVE DATE OF 1984 AMENDMENT

Amendment by Pub. L. 98-549 effective 60 days after Oct. 30, 1984, see section 9(a) of Pub. L. 98-549, set out as an Effective Date note under section 521 of Title 47, Telegraphs, Telephones, and Radiotelegraphs.

#### EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95-511 effective Oct. 25, 1978, except as specifically provided, see section 401 of Pub. L. 95-511, set out as an Effective Date note under section 1801 of Title 50, War and National Defense.

#### EFFECTIVE DATE OF 1970 AMENDMENT

Amendment by Pub. L. 91-358 effective on first day of seventh calendar month which begins after July 29, 1970, see section 901(a) of Pub. L. 91-358.

### § 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

(Added Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 214; amended Pub. L. 99-508, title I, § 101(c)(1)(A), (7), (f)(2), Oct. 21, 1986, 100 Stat. 1851, 1853; Pub. L. 103-322, title XXXIII, §§ 330016(1)(L), 330022, Sept. 13, 1994, 108 Stat. 2147, 2150; Pub. L. 104-294, title VI, § 604(b)(45), Oct. 11, 1996, 110 Stat. 3509; Pub. L. 105-112, § 2, Nov. 21, 1997, 111 Stat. 2273; Pub. L. 107-296, title II, § 225(f), Nov. 25, 2002, 116 Stat. 2158.)

#### AMENDMENTS

2002—Par. (1)(c). Pub. L. 107-296, in introductory provisions, inserted “or disseminates by electronic means” after “or other publication” and, in concluding provisions, inserted “knowing the content of the advertisement and” before “knowing or having reason to know”.

1997—Par. (3). Pub. L. 105-112 added par. (3).

1996—Par. (2). Pub. L. 104-294 amended directory language of Pub. L. 103-322, § 330022. See 1994 Amendment note below.

1994—Par. (1). Pub. L. 103-322, § 330016(1)(L), substituted “fined under this title” for “fined not more than \$10,000” in concluding provisions.

Par. (2). Pub. L. 103-322, § 330022, as amended by Pub. L. 104-294, realigned margins of concluding provisions.

1986—Pub. L. 99-508, § 101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral” in section catchline.

Par. (1). Pub. L. 99-508, § 101(c)(1)(A), (f)(2), substituted “intentionally” for “willfully” in introductory provision and “wire, oral, or electronic” for “wire or oral” in subpars. (a), (b), and (c)(i), (ii).

Par. (2)(a). Pub. L. 99-508, § 101(c)(7), substituted “a provider of wire or electronic communication service or” for “a communications common carrier or”, “such a provider, in” for “a communications common carrier, in”, and “business of providing that wire or electronic communication service” for “communications common carrier’s business”.

Par. (2)(b). Pub. L. 99-508, § 101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral”.

#### EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

#### EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104-294 effective Sept. 13, 1994, see section 604(d) of Pub. L. 104-294, set out as a note under section 13 of this title.

## EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

**§ 2513. Confiscation of wire, oral, or electronic communication intercepting devices**

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

(Added Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 215; amended Pub. L. 99-508, title I, § 101(c)(1)(A), Oct. 21, 1986, 100 Stat. 1851.)

## AMENDMENTS

1986—Pub. L. 99-508 substituted “wire, oral, or electronic” for “wire or oral” in section catchline.

## EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

**[§ 2514. Repealed. Pub. L. 91-452, title II, § 227(a), Oct. 15, 1970, 84 Stat. 930]**

Section, Pub. L. 90-351, title II, § 802, June 19, 1968, 82 Stat. 216, provided for immunity of witnesses giving testimony or producing evidence under compulsion in Federal grand jury or court proceedings. Subject matter is covered in sections 6002 and 6003 of this title.

## EFFECTIVE DATE OF REPEAL

Sections 227(a) and 260 of Pub. L. 91-452 provided for repeal of this section effective four years following sixtieth day after date of enactment of Pub. L. 91-452, which was approved Oct. 15, 1970, such repeal not affect-

ing any immunity to which any individual was entitled under this section by reason of any testimony or other information given before such date. See section 260 of Pub. L. 91-452, set out as an Effective Date; Savings Provision note under section 6001 of this title.

**§ 2515. Prohibition of use as evidence of intercepted wire or oral communications**

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

(Added Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 216.)

**§ 2516. Authorization for interception of wire, oral, or electronic communications**

(1) The Attorney General, Deputy Attorney General, Associate Attorney General,<sup>1</sup> or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons)<sup>2</sup> chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 (re-

<sup>1</sup> See 1984 Amendment note below.

<sup>2</sup> So in original. Probably should be followed by a comma.

lating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft

parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus) section 956 (conspiracy to harm persons or property overseas),<sup>3</sup> section<sup>4</sup> a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline),<sup>5</sup> section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

<sup>3</sup>So in original.

<sup>4</sup>So in original. The word "section" probably should not appear.

<sup>5</sup>So in original. The comma probably should follow the closing parenthesis.

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents, section 1028A (relating to aggravated identity theft))<sup>6</sup> of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or<sup>7</sup>

(q) any criminal violation of section 229 (relating to chemical weapons) or section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h<sup>2</sup>, 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3); or

(s) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in con-

formity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

(Added Pub. L. 90-351, title III, §802, June 19, 1968, 82 Stat. 216; amended Pub. L. 91-452, title VIII, §810, title IX, §902(a), title XI, §1103, Oct. 15, 1970, 84 Stat. 940, 947, 959; Pub. L. 91-644, title IV, §16, Jan. 2, 1971, 84 Stat. 1891; Pub. L. 95-598, title III, §314(h), Nov. 6, 1978, 92 Stat. 2677; Pub. L. 97-285, §§2(e), 4(e), Oct. 6, 1982, 96 Stat. 1220, 1221; Pub. L. 98-292, §8, May 21, 1984, 98 Stat. 206; Pub. L. 98-473, title II, §1203(c), Oct. 12, 1984, 98 Stat. 2152; Pub. L. 99-508, title I, §§101(c)(1)(A), 104, 105, Oct. 21, 1986, 100 Stat. 1851, 1855; Pub. L. 99-570, title I, §1365(c), Oct. 27, 1986, 100 Stat. 3207-35; Pub. L. 100-690, title VI, §6461, title VII, §§7036, 7053(d), 7525, Nov. 18, 1988, 102 Stat. 4374, 4399, 4402, 4502; Pub. L. 101-298, §3(b), May 22, 1990, 104 Stat. 203; Pub. L. 101-647, title XXV, §2531, title XXXV, §3568, Nov. 29, 1990, 104 Stat. 4879, 4928; Pub. L. 103-272, §5(e)(11), July 5, 1994, 108 Stat. 1374; Pub. L. 103-322, title XXXIII, §§330011(c)(1), (q)(1), (r), 330021(1), Sept. 13, 1994, 108 Stat. 2144, 2145, 2150; Pub. L. 103-414, title II, §208, Oct. 25, 1994, 108 Stat. 4292; Pub. L. 103-429, §7(a)(4)(A), Oct. 31, 1994, 108 Stat. 4389; Pub. L. 104-132, title IV, §434, Apr. 24, 1996, 110 Stat. 1274; Pub. L. 104-208, div. C, title II, §201, Sept. 30, 1996, 110 Stat. 3009-564; Pub. L. 104-287, §6(a)(2), Oct. 11, 1996, 110 Stat. 3398; Pub. L. 104-294, title I, §102, title VI, §601(d), Oct. 11, 1996, 110 Stat. 3491, 3499; Pub. L. 105-318, §6(b), Oct. 30, 1998, 112 Stat. 3011; Pub. L. 106-181, title V, §506(c)(2)(B), Apr. 5, 2000, 114 Stat. 139; Pub. L. 107-56, title II, §§201, 202, Oct. 26, 2001, 115 Stat. 278; Pub. L. 107-197, title III, §301(a), June 25, 2002, 116 Stat. 728; Pub. L. 107-273, div. B, title IV, §§4002(c)(1), 4005(a)(1), Nov. 2, 2002, 116 Stat. 1808, 1812; Pub. L. 108-21, title II, §201, Apr. 30, 2003, 117 Stat. 659; Pub. L. 108-458, title VI, §6907, Dec. 17, 2004, 118 Stat. 3774; Pub. L. 109-162, title XI, §1171(b), Jan. 5, 2006, 119 Stat. 3123; Pub. L. 109-177, title I, §§110(b)(3)(C), 113, title V, §506(a)(6), Mar. 9, 2006, 120 Stat. 208, 209, 248.)

#### REFERENCES IN TEXT

The Atomic Energy Act of 1954, referred to in par. (1)(a), is act Aug. 1, 1946, ch. 724, as added by act Aug. 30, 1954, ch. 1073, §1, 68 Stat. 921, and amended, which is classified generally to chapter 23 (§2011 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 42 and Tables.

The Arms Export Control Act, referred to in par. (1)(k), is Pub. L. 90-269, Oct. 22, 1968, 82 Stat. 1320, as amended, which is classified principally to chapter 39 (§2751 et seq.) of Title 22, Foreign Relations and Intercourse. For complete classification of this Act to the Code, see Short Title note set out under section 2751 of Title 22 and Tables.

Section 5861 of the Internal Revenue Code of 1986, referred to in par. (1)(o), is classified to section 5861 of Title 26, Internal Revenue Code.

The Federal Rules of Criminal Procedure, referred to in par. (3), are set out in the Appendix to this title.

<sup>6</sup> So in original. The second closing parenthesis probably should follow "other documents".

<sup>7</sup> So in original. The word "or" probably should not appear.

## AMENDMENTS

2006—Par. (1). Pub. L. 109-177, §506(a)(6), inserted “or National Security Division” after “the Criminal Division” in introductory provisions.

Par. (1)(a). Pub. L. 109-177, §113(a), inserted “chapter 10 (relating to biological weapons)” after “under the following chapters of this title:”.

Par. (1)(c). Pub. L. 109-177, §§110(b)(3)(C), 113(b), struck out “1992 (relating to wrecking trains),” before “a felony violation of section 1028” and inserted “section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction),” after “the following sections of this title:”, “section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities),” after “section 751 (relating to escape),”, “section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials),” after “section 1014 (relating to loans and credit applications generally; renewals and discounts),”, “section 1992 (relating to terrorist attacks against mass transportation),” after “section 1344 (relating to bank fraud),”, “section 2340A (relating to torture),” after “section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts),”, and “section 956 (conspiracy to harm persons or property overseas),” after “section 175c (relating to variola virus)”.

Par. (1)(g). Pub. L. 109-177, §113(c), inserted “, or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited)” before semicolon at end.

Par. (1)(j). Pub. L. 109-177, §113(d)(2), inserted “, the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft)” before “of title 49”.

Pub. L. 109-177, §113(d)(1), which directed amendment of par. (1)(i) by inserting a comma after “section 60123(b) (relating to the destruction of a natural gas pipeline)”, was executed by making the insertion after “section 60123(b) (relating to destruction of a natural gas pipeline)”, to reflect the probable intent of Congress.

Pub. L. 109-177, §113(d)(1), struck out “or” before “section 46502 (relating to aircraft piracy)”.

Par. (1)(p). Pub. L. 109-177, §113(e), inserted “, section 1028A (relating to aggravated identity theft)” after “other documents”.

Par. (1)(q). Pub. L. 109-177, §113(f), inserted “2339” after “2332h” and substituted “2339C, or 2339D” for “or 2339C”.

Pub. L. 109-162 struck out semicolon after “(relating to chemical weapons)” and substituted “section 2332” for “sections 2332”.

Par. (1)(r), (s). Pub. L. 109-177, §113(g), added subpar. (r) and redesignated former subpar. (r) as (s).

2004—Par. (1)(a). Pub. L. 108-458, §6907(1), inserted “2122 and” after “sections”.

Par. (1)(c). Pub. L. 108-458, §6907(2), inserted “section 175c (relating to variola virus),” after “section 175 (relating to biological weapons),”.

Par. (1)(q). Pub. L. 108-458, §6907(3), inserted “2332g, 2332h,” after “2332f,”.

2003—Par. (1)(a). Pub. L. 108-21, §201(1), inserted “chapter 55 (relating to kidnapping),” after “chapter 37 (relating to espionage),”.

Par. (1)(c). Pub. L. 108-21, §201(2), inserted “section 1591 (sex trafficking of children by force, fraud, or coercion),” after “section 1511 (obstruction of State or local law enforcement),” and “section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422,

2423, and 2425 (relating to transportation for illegal sexual activity and related crimes),” after “sections 2251 and 2252 (sexual exploitation of children),”.

2002—Par. (1)(n). Pub. L. 107-273, §4002(c)(1), repealed Pub. L. 104-294, §601(d)(2). See 1996 Amendment note below.

Par. (1)(q). Pub. L. 107-273, §4005(a)(1), realigned margins.

Pub. L. 107-197 inserted “2332f,” after “2332d,” and substituted “2339B, or 2339C” for “or 2339B”.

2001—Par. (1)(c). Pub. L. 107-56, §202, substituted “section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),” for “and section 1341 (relating to mail fraud),”.

Par. (1)(p). Pub. L. 107-56, §201(1), redesignated subpar. (p), relating to conspiracy, as (r).

Par. (1)(q). Pub. L. 107-56, §201(2), added subpar. (q).

Par. (1)(r). Pub. L. 107-56, §201(1), redesignated subpar. (p), relating to conspiracy, as (r).

2000—Par. (1)(c). Pub. L. 106-181 inserted “section 38 (relating to aircraft parts fraud),” after “section 32 (relating to destruction of aircraft or aircraft facilities),”.

1998—Par. (1)(a). Pub. L. 105-318 inserted “chapter 90 (relating to protection of trade secrets),” after “chapter 37 (relating to espionage),”.

1996—Par. (1)(c). Pub. L. 104-294, §102, which directed amendment of par. 1(c) by inserting “chapter 90 (relating to protection of trade secrets),” after “chapter 37 (relating to espionage),” could not be executed because phrase “chapter 37 (relating to espionage),” did not appear.

Pub. L. 104-208, §201(1), substituted “section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents)” for “or section 1992 (relating to wrecking trains)” before semicolon at end.

Par. (1)(j). Pub. L. 104-287, §6(a)(2), amended directory language of Pub. L. 103-272, §5(e)(11) as amended by Pub. L. 103-429, §7(a)(4)(A). See 1994 Amendment note below.

Par. (1)(l). Pub. L. 104-208, §201(2), and Pub. L. 104-294, §601(d)(1), amended subpar. (l) identically, striking out “or” after semicolon at end.

Par. (1)(m). Pub. L. 104-208, §201(3), (4), added subpar. (m). Former subpar. (m) redesignated (n).

Par. (1)(n). Pub. L. 104-294, §601(d)(2), which could not be executed because of prior amendments by Pub. L. 104-132, §434(1) and Pub. L. 104-208, §201(3), was repealed by Pub. L. 107-273, §4002(c)(1). See below.

Pub. L. 104-208, §201(3), redesignated subpar. (m) as (n). Former subpar. (n) redesignated (o).

Pub. L. 104-132, §434(1), struck out “and” at end.

Par. (1)(o). Pub. L. 104-208, §201(3), redesignated subpar. (n) as (o). Former subpar. (o) redesignated (p).

Pub. L. 104-132 added subpar. (o) and redesignated former subpar. (o) as (p).

Par. (1)(p). Pub. L. 104-208, §201(3), redesignated subpar. (o), relating to felony violation of section 1028, etc., as (p).

Pub. L. 104-132, §434(2), redesignated subpar. (o), relating to conspiracy, as (p).

1994—Par. (1). Pub. L. 103-414 in introductory provisions inserted “or acting Deputy Assistant Attorney General” after “Deputy Assistant Attorney General”.

Par. (1)(c). Pub. L. 103-322, §330021(1), substituted “kidnapping” for “kidnaping” in two places.

Pub. L. 103-322, §330011(c)(1), amended directory language of Pub. L. 101-298, §3(b). See 1990 Amendment note below.

Par. (1)(j). Pub. L. 103-322, § 330011(r), amended directory language of Pub. L. 101-647, § 2531(3). See 1990 Amendment note below.

Pub. L. 103-322, § 330011(q)(1), repealed Pub. L. 101-647, § 3568. See 1990 Amendment note below.

Pub. L. 103-272, § 5(e)(11), as amended by Pub. L. 103-429, § 7(a)(4)(A); Pub. L. 104-287, § 6(a)(2), substituted "section 60123(b) (relating to destruction of a natural gas pipeline) or section 46502 (relating to aircraft piracy) of title 49;" for "section 11(c)(2) of the Natural Gas Pipeline Safety Act of 1968 (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 902 of the Federal Aviation Act of 1958 (relating to aircraft piracy);".

1990—Par. (1)(c). Pub. L. 101-647, § 2531(1), inserted "section 215 (relating to bribery of bank officials)," before "section 224", "section 1032 (relating to concealment of assets)," before section 1084, "section 1014 (relating to loans and credit applications generally; renewals and discounts)," before "sections 1503," and "section 1344 (relating to bank fraud)," before "sections 2251 and 2252" and struck out "the section in chapter 65 relating to destruction of an energy facility," after "retaliating against a Federal official".

Pub. L. 101-298, § 3(b), as amended by Pub. L. 103-322, § 330011(c)(1), inserted "section 175 (relating to biological weapons)," after "section 33 (relating to destruction of motor vehicles or motor vehicle facilities)."

Par. (1)(j). Pub. L. 101-647, § 3568, which directed amendment of subsec. (j) by substituting "any violation of section 11(c)(2) of the Natural Gas Pipeline Safety Act of 1968 (relating to destruction of a natural gas pipeline) or section 902(i) or (n) of the Federal Aviation Act of 1958 (relating to aircraft piracy)" for "any violation of section 1679a(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 1472 (relating to aircraft piracy) of title 49, of the United States Code", and which was probably intended as an amendment to par. (1)(j), was repealed by Pub. L. 103-322, § 330011(q)(1).

Pub. L. 101-647, § 2531(3), as amended by Pub. L. 103-322, § 330011(r), substituted "any violation of section 11(c)(2) of the Natural Gas Pipeline Safety Act of 1968 (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 902 of the Federal Aviation Act of 1958 (relating to aircraft piracy)" for "any violation of section 1679a(c)(2) (relating to destruction of a natural gas pipeline) or subsection (i) or (n) of section 1472 (relating to aircraft piracy) of title 49, of the United States Code".

Par. (1)(m). Pub. L. 101-647, § 2531(2)(A), struck out subpar. (m) relating to conspiracy which read as follows: "any conspiracy to commit any of the foregoing offenses."

Par. (1)(o). Pub. L. 101-647, § 2531(2)(B)-(D), added subpar. (o).

1988—Par. (1). Pub. L. 100-690, § 7036(a)(1), inserted "or" after "Associate Attorney General," in introductory provisions.

Par. (1)(a). Pub. L. 100-690, § 7036(c)(1), which directed the amendment of subpar. (a) by substituting "(relating to riots)," for "(relating to riots)," was executed by substituting "(relating to riots)," for "(relating to riots)" as the probable intent of Congress.

Par. (1)(c). Pub. L. 100-690, § 7053(d), which directed the amendment of section 2516(c) by substituting "1958" for "1952A" and "1959" for "1952B" was executed by making the substitutions in par. (1)(c) as the probable intent of Congress.

Pub. L. 100-690, § 7036(b), struck out "section 2252 or 2253 (sexual exploitation of children)," after "wire, radio, or television)," and substituted "section 2321" for "the second section 2320".

Pub. L. 100-690, § 7036(a)(2), which directed the amendment of par. (1) by striking the comma that follows a comma was executed to subpar. (c) by striking out the second comma after "to mail fraud)".

Par. (1)(i). Pub. L. 100-690, § 7525, added subpar. (i) and redesignated former subpar. (i) as (j).

Par. (1)(j). Pub. L. 100-690, § 7525, redesignated former subpar. (i) as (j). Former subpar. (j) redesignated (k).

Pub. L. 100-690, § 7036(c)(2), which directed amendment of subpar. (j) by striking "or;" was executed by striking "or" after "Export Control Act);" to reflect the probable intent of Congress.

Par. (1)(k). Pub. L. 100-690, § 7525, redesignated former subpar. (j) as (k). Former subpar. (k) redesignated (l).

Pub. L. 100-690, § 7036(c)(3), struck out "or" at end.

Par. (1)(l). Pub. L. 100-690, § 7525, redesignated former subpar. (k) as (l). Former subpar. (l) redesignated (m).

Par. (1)(m). Pub. L. 100-690, § 7525, redesignated former subpar. (l) relating to conspiracy as (m).

Pub. L. 100-690, § 6461, added subpar. (m) relating to sections 922 and 924.

Par. (1)(n). Pub. L. 100-690, § 6461, added subpar. (n).

1986—Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic" for "wire or oral" in section catchline.

Par. (1). Pub. L. 99-508, § 104, substituted "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division" for "or any Assistant Attorney General" in introductory provisions.

Par. (1)(a). Pub. L. 99-508, § 105(a)(5), inserted "section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel)," struck out "or" after "(relating to treason)," and inserted "chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy)".

Par. (1)(c). Pub. L. 99-570, which directed the amendment of subpar. (c) by inserting "section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity)," after "section 1955 (prohibition of relating to business enterprises of gambling)," was executed by inserting this phrase after "section 1955 (prohibition of business enterprises of gambling)," as the probable intent of Congress.

Pub. L. 99-508, § 105(a)(1), inserted "section 751 (relating to escape)," "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," and "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," substituted "2312, 2313, 2314," for "2314", inserted ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," substituted "section 351" for "or section 351", and inserted ", section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), or section 1992 (relating to wrecking trains)".

Par. (1)(h) to (l). Pub. L. 99-508, § 105(a)(2)-(4), added subpars. (h) to (k) and redesignated former subpar. (h) as (l).

Par. (2). Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic" for "wire or oral" in two places.

Par. (3). Pub. L. 99-508, § 105(b), added par. (3).

1984—Par. (1). Pub. L. 98-473, § 1203(c)(4), which directed the amendment of the first par. of par. (1) by inserting "Deputy Attorney General, Associate Attorney General," after "Attorney General," was executed by making the insertion after the first reference to "Attorney General," to reflect the probable intent of Congress.

Par. (1)(c). Pub. L. 98-473, § 1203(c)(2), inserted references to sections 1512 and 1513 after "1503".

Pub. L. 98-473, § 1203(c)(1), inserted "section 1343 (fraud by wire, radio, or television), section 2252 or 2253 (sexual exploitation of children)," after "section 664 (embezzlement from pension and welfare funds)".



Pub. L. 98-292 inserted "sections 2251 and 2252 (sexual exploitation of children)," after "section 664 (embezzlement from pension and welfare funds)."

Par. (1)(g), (h). Pub. L. 98-473, § 1203(c)(3), added par. (g) and redesignated former par. (g) as (h).

1982—Par. (1)(c). Pub. L. 97-285 substituted "(Presidential and Presidential staff assassination, kidnaping, and assault)" for "(Presidential assassinations, kidnaping, and assault)" after "section 1751" and substituted "(violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnaping, and assault)" for "(violations with respect to congressional assassination, kidnaping, and assault)" after "section 351".

1978—Par. (1)(e). Pub. L. 95-598 substituted "fraud connected with a case under title 11" for "bankruptcy fraud".

1971—Par. (1)(c). Pub. L. 91-644 inserted reference to section 351 offense (violations with respect to congressional assassination, kidnaping, and assault).

1970—Par. (1)(c). Pub. L. 91-452 inserted reference to sections 844(d), (e), (f), (g), (h), or (i), 1511, 1955, and 1963 of this title.

#### EFFECTIVE DATE OF 2002 AMENDMENT

Pub. L. 107-273, div. B, title IV, § 4002(c)(1), Nov. 2, 2002, 116 Stat. 1808, provided that the amendment made by section 4002(c)(1) is effective Oct. 11, 1996.

#### EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106-181 applicable only to fiscal years beginning after Sept. 30, 1999, see section 3 of Pub. L. 106-181, set out as a note under section 106 of Title 49, Transportation.

#### EFFECTIVE DATE OF 1996 AMENDMENT

Section 6(a) of Pub. L. 104-287 provided that the amendment made by that section is effective July 5, 1994.

#### EFFECTIVE DATE OF 1994 AMENDMENTS

Section 7(a) of Pub. L. 103-429 provided that the amendment made by section 7(a)(4)(A) of Pub. L. 103-429 is effective July 5, 1994.

Section 330011(c)(1) of Pub. L. 103-322 provided that the amendment made by that section is effective as of the date on which section 3(b) of Pub. L. 101-298 took effect.

Section 330011(q)(1) of Pub. L. 103-322 provided that the amendment made by that section is effective as of the date on which section 3568 of Pub. L. 101-647 took effect.

Section 330011(r) of Pub. L. 103-322 provided that the amendment made by that section is effective as of the date on which section 2531(3) of Pub. L. 101-647 took effect.

#### EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by sections 101(c)(1)(A) and 105 of Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions pursuant to section 2516(2) of this title, and amendment by section 104 of Pub. L. 99-508 effective Oct. 21, 1986, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

#### EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95-598 effective Oct. 1, 1979, see section 402(a) of Pub. L. 95-598, set out as an Effective Date note preceding section 101 of Title 11, Bankruptcy.

#### SAVINGS PROVISION

Amendment by section 314 of Pub. L. 95-598 not to affect the application of chapter 9 (§151 et seq.), chapter 96 (§1961 et seq.), or section 2516, 3057, or 3284 of this

title to any act of any person (1) committed before Oct. 1, 1979, or (2) committed after Oct. 1, 1979, in connection with a case commenced before such date, see section 403(d) of Pub. L. 95-598, set out as a note preceding section 101 of Title 11, Bankruptcy.

### § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents 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.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence 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.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or



foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign 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, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

(Added Pub. L. 90-351, title III, §802, June 19, 1968, 82 Stat. 217; amended Pub. L. 91-452, title IX, §902(b), Oct. 15, 1970, 84 Stat. 947; Pub. L. 99-508, title I, §101(c)(1)(A), Oct. 21, 1986, 100 Stat. 1851; Pub. L. 107-56, title II, §203(b)(1), Oct. 26, 2001, 115 Stat. 280; Pub. L. 107-296, title VIII, §896, Nov. 25, 2002, 116 Stat. 2257.)

#### AMENDMENTS

2002—Pars. (7), (8). Pub. L. 107-296 added pars. (7) and (8).

2001—Par. (6). Pub. L. 107-56 added par. (6).

1986—Pub. L. 99-508 substituted “wire, oral, or electronic” for “wire or oral” in section catchline and wherever appearing in text.

1970—Par. (3). Pub. L. 91-452 substituted “proceeding held under the authority of the United States or of any State or political subdivision thereof” for “criminal proceeding in any court of the United States or of any State or in any Federal or State grand jury proceeding”.

#### CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 401 of Title 50, War and National Defense.

#### EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

#### EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

#### PROCEDURES FOR DISCLOSURE OF INFORMATION

Pub. L. 107-56, title II, §203(c), Oct. 26, 2001, 115 Stat. 280, as amended by Pub. L. 107-296, title VIII, §897(b), Nov. 25, 2002, 116 Stat. 2258; Pub. L. 108-458, title VI, §6501(b), Dec. 17, 2004, 118 Stat. 3760, provided that: “The Attorney General shall establish procedures for the disclosure of information pursuant to paragraphs (6) and (8) of section 2517 of title 18, United States Code, and Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure [18 U.S.C. App.] that identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) [sic].”

#### § 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person,

if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon

as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

- (i) immediate danger of death or serious physical injury to any person,
- (ii) conspiratorial activities threatening the national security interest, or
- (iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be de-

stroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

- (1) the fact of the entry of the order or the application;
- (2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
- (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, depart-

ment, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, 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.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

- (a) in the case of an application with respect to the interception of an oral communication—

- (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

- (ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

- (iii) the judge finds that such specification is not practical; and

- (b) in the case of an application with respect to a wire or electronic communication—

- (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

- (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

- (iii) the judge finds that such showing has been adequately made; and

- (iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

(Added Pub. L. 90-351, title III, § 802, June 19, 1968, 82 Stat. 218; amended Pub. L. 91-358, title II, § 211(b), July 29, 1970, 84 Stat. 654; Pub. L. 95-511, title II, § 201(d)-(g), Oct. 25, 1978, 92 Stat. 1797, 1798; Pub. L. 98-473, title II, § 1203(a), (b), Oct. 12, 1984, 98 Stat. 2152; Pub. L. 99-508, title I, §§ 101(c)(1)(A), (8), (e), 106(a)-(d)(3), Oct. 21, 1986, 100 Stat. 1851-1853, 1856, 1857; Pub. L. 103-414, title II, § 201(b)(1), Oct. 25, 1994, 108 Stat. 4290; Pub. L. 105-272, title VI, § 604, Oct. 20, 1998, 112 Stat. 2413.)

#### REFERENCES IN TEXT

The Communications Assistance for Law Enforcement Act, referred to in par. (4), is title I of Pub. L. 103-414, Oct. 25, 1994, 108 Stat. 4279, which is classified generally to subchapter I (§1001 et seq.) of chapter 9 of Title 47, Telegraphs, Telephones, and Radiotelegraphs. For complete classification of this Act to the Code, see Short Title note set out under section 1001 of Title 47 and Tables.

#### AMENDMENTS

1998—Par. (11)(b)(ii). Pub. L. 105-272, § 604(a)(1), substituted “that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;” for “of a purpose, on the part of that person, to thwart interception by changing facilities; and”.

Par. (11)(b)(iii). Pub. L. 105-272, § 604(a)(2), substituted “such showing has been adequately made; and” for “such purpose has been adequately shown.”

Par. (11)(b)(iv). Pub. L. 105-272, § 604(a)(3), added cl. (iv).

Par. (12). Pub. L. 105-272, § 604(b), substituted "by reason of subsection (11)(a)" for "by reason of subsection (11)", struck out "the facilities from which, or" after "shall not begin until", and struck out comma after "the place where".

1994—Par. (4). Pub. L. 103-414 inserted at end of concluding provisions "Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act."

1986—Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic" for "wire or oral" in section catchline.

Par. (1). Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic" for "wire or oral" in introductory provisions.

Par. (1)(b)(ii). Pub. L. 99-508, § 106(d)(1), inserted "except as provided in subsection (11),".

Par. (1)(e). Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic" for "wire or oral".

Par. (3). Pub. L. 99-508, §§ 101(c)(1)(A), 106(a), in introductory provisions, substituted "wire, oral, or electronic" for "wire or oral" and inserted "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)".

Par. (3)(d). Pub. L. 99-508, §§ 101(c)(1)(A), 106(d)(2), inserted "except as provided in subsection (11), and substituted "wire, oral, or electronic" for "wire or oral".

Par. (4). Pub. L. 99-508, §§ 101(c)(1)(A), (8), 106(b), substituted "wire, oral, or electronic" for "wire or oral" wherever appearing and, in closing provisions, substituted "provider of wire or electronic communication service" for "communication common carrier" wherever appearing, "such service provider" for "such carrier", and "for reasonable expenses incurred in providing such facilities or assistance" for "at the prevailing rates".

Par. (5). Pub. L. 99-508, §§ 101(c)(1)(A), 106(c), substituted "wire, oral, or electronic" for "wire or oral" and inserted provisions which related to beginning of thirty-day period, minimization where intercepted communication is in code or foreign language and expert in that code or foreign language is not immediately available, and conduct of interception by Government personnel or by individual operating under Government contract, acting under supervision of investigative or law enforcement officer authorized to conduct interception.

Pars. (7), (8)(a), (d)(3), (9). Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic" for "wire or oral" wherever appearing.

Par. (10)(c). Pub. L. 99-508, § 101(e), added subpar. (c).

Pars. (11), (12). Pub. L. 99-508, § 106(d)(3), added pars. (11) and (12).

1984—Par. (7). Pub. L. 98-473, § 1203(a), inserted ", the Deputy Attorney General, the Associate Attorney General," after "Attorney General" in provisions preceding subpar. (a).

Par. (7)(a). Pub. L. 98-473, § 1203(b), amended subpar. (a) generally, adding cl. (i) and designated existing provisions as cls. (ii) and (iii).

1978—Par. (1). Pub. L. 95-511, § 201(d), inserted "under this chapter" after "communication".

Par. (4). Pub. L. 95-511, § 201(e), inserted "under this chapter" after "wire or oral communication" wherever appearing.

Par. (9). Pub. L. 95-511, § 201(e), substituted "any wire or oral communication intercepted pursuant to this chapter" for "any intercepted wire or oral communication".

Par. (10). Pub. L. 95-511, § 201(g), substituted "any wire or oral communication intercepted pursuant to this chapter," for "any intercepted wire or oral communication,".

1970—Par. (4). Pub. L. 91-358 inserted the provision that, upon the request of the applicant, an order authorizing the interception of a wire or oral communication direct that a communication common carrier,

landlord, custodian, or other person furnish the applicant with all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services provided.

#### EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

#### EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95-511 effective Oct. 25, 1978, except as specifically provided, see section 401 of Pub. L. 95-511, set out as an Effective Date note under section 1801 of Title 50, War and National Defense.

#### EFFECTIVE DATE OF 1970 AMENDMENT

Amendment by Pub. L. 91-358 effective on first day of seventh calendar month which begins after July 29, 1970, see section 901(a) of Pub. L. 91-358.

### § 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including

(i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

(Added Pub. L. 90-351, title III, §802, June 19, 1968, 82 Stat. 222; amended Pub. L. 95-511, title II, §201(h), Oct. 25, 1978, 92 Stat. 1798; Pub. L. 99-508, title I, §§101(c)(1)(A), 106(d)(4), Oct. 21, 1986, 100 Stat. 1851, 1857; Pub. L. 106-197, §2(a), May 2, 2000, 114 Stat. 247.)

#### AMENDMENTS

2000—Par. (2)(b)(iv), (v). Pub. L. 106-197 added cl. (iv) and redesignated former cl. (iv) as (v).

1986—Pub. L. 99-508, §101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral” in section catchline.

Par. (1)(b). Pub. L. 99-508, §106(d)(4), inserted “(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)”.

Par. (3). Pub. L. 99-508, §101(c)(1)(A), substituted “wire, oral, or electronic” for “wire or oral”.

1978—Par. (3). Pub. L. 95-511 inserted “pursuant to this chapter” after “wire or oral communications” and “granted or denied”.

#### EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

#### EFFECTIVE DATE OF 1978 AMENDMENT

Amendment by Pub. L. 95-511 effective Oct. 25, 1978, except as specifically provided, see section 401 of Pub. L. 95-511, set out as an Effective Date note under section 1801 of Title 50, War and National Defense.

#### REPORT ON USE OF DCS 1000 (CARNIVORE) TO IMPLEMENT ORDERS UNDER SECTION 2518

Pub. L. 107-273, div. A, title III, §305(b), Nov. 2, 2002, 116 Stat. 1782, provided that: “At the same time that the Attorney General, or Assistant Attorney General specially designated by the Attorney General, submits to the Administrative Office of the United States Courts the annual report required by section 2519(2) of title 18, United States Code, that is respectively next due after the end of each of the fiscal years 2002 and 2003, the Attorney General shall also submit to the Chairmen and ranking minority members of the Committees on the Judiciary of the Senate and of the House of Representatives a report, covering the same respective time period, that contains the following information with respect to those orders described in that annual report that were applied for by law enforcement agencies of the Department of Justice and whose implementation involved the use of the DCS 1000 program (or any subsequent version of such program)—

“(1) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of title 18, United States Code, did not apply by reason of section 2518 (11) of title 18);

“(2) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

“(3) the offense specified in the order or application, or extension of an order;

“(4) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application;

“(5) the nature of the facilities from which or place where communications were to be intercepted;

“(6) a general description of the interceptions made under such order or extension, including—

“(A) the approximate nature and frequency of incriminating communications intercepted;

“(B) the approximate nature and frequency of other communications intercepted;

“(C) the approximate number of persons whose communications were intercepted;

“(D) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order; and

“(E) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

“(7) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

“(8) the number of trials resulting from such interceptions;

“(9) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

“(10) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

"(11) the specific persons authorizing the use of the DCS 1000 program (or any subsequent version of such program) in the implementation of such order."

#### ENCRYPTION REPORTING REQUIREMENTS

Pub. L. 106-197, §2(b), May 2, 2000, 114 Stat. 247, provided that: "The encryption reporting requirement in subsection (a) [amending this section] shall be effective for the report transmitted by the Director of the Administrative Office of the Courts for calendar year 2000 and in subsequent reports."

### § 2520. Recovery of civil damages authorized

(a) IN GENERAL.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In an action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) COMPUTATION OF DAMAGES.—(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$50 and not more than \$500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) IMPROPER DISCLOSURE IS VIOLATION.—Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

(Added Pub. L. 90-351, title III, §802, June 19, 1968, 82 Stat. 223; amended Pub. L. 91-358, title II, §211(c), July 29, 1970, 84 Stat. 654; Pub. L. 99-508, title I, §103, Oct. 21, 1986, 100 Stat. 1853; Pub. L. 107-56, title II, §223(a), Oct. 26, 2001, 115 Stat. 293; Pub. L. 107-296, title II, §225(e), Nov. 25, 2002, 116 Stat. 2157.)

#### AMENDMENTS

2002—Subsec. (d)(3). Pub. L. 107-296 inserted "or 2511(2)(i)" after "2511(3)".

2001—Subsec. (a). Pub. L. 107-56, §223(a)(1), inserted " , other than the United States," after "person or entity".

Subsecs. (f), (g). Pub. L. 107-56, §223(a)(2), (3), added subsecs. (f) and (g).

1986—Pub. L. 99-508 amended section generally. Prior to amendment, section read as follows: "Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

"(a) actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;

"(b) punitive damages; and

"(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law."

1970—Pub. L. 91-358 substituted provisions that a good faith reliance on a court order or legislative authorization constitute a complete defense to any civil or criminal action brought under this chapter or under any other law, for provisions that a good faith reliance on a court order or on the provisions of section 2518(7) of this chapter constitute a complete defense to any civil or criminal action brought under this chapter.

#### EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

#### EFFECTIVE DATE OF 1986 AMENDMENT

Amendment by Pub. L. 99-508 effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as a note under section 2510 of this title.

#### EFFECTIVE DATE OF 1970 AMENDMENT

Amendment by Pub. L. 91-358 effective on first day of seventh calendar month which begins after July 29, 1970, see section 901(a) of Pub. L. 91-358.

### § 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

(Added Pub. L. 99-508, title I, § 110(a), Oct. 21, 1986, 100 Stat. 1859.)

#### REFERENCES IN TEXT

The Federal Rules of Civil Procedure, referred to in text, are set out in the Appendix to Title 28, Judiciary and Judicial Procedure.

The Federal Rules of Criminal Procedure, referred to in text, are set out in the Appendix to this title.

#### EFFECTIVE DATE

Section effective 90 days after Oct. 21, 1986, and, in case of conduct pursuant to court order or extension, applicable only with respect to court orders and extensions made after such date, with special rule for State authorizations of interceptions, see section 111 of Pub. L. 99-508, set out as an Effective Date of 1986 Amendment note under section 2510 of this title.

### § 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) ENFORCEMENT BY COURT ISSUING SURVEILLANCE ORDER.—If a court authorizing an inter-

ception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) ENFORCEMENT UPON APPLICATION BY ATTORNEY GENERAL.—The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

#### (c) CIVIL PENALTY.—

(1) IN GENERAL.—A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to \$10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) CONSIDERATIONS.—In determining whether to impose a civil penalty and in determining its amount, the court shall take into account—

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(C) such other matters as justice may require.

(d) DEFINITIONS.—As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

(Added Pub. L. 103-414, title II, § 201(a), Oct. 25, 1994, 108 Stat. 4289.)

#### REFERENCES IN TEXT

The Foreign Intelligence Surveillance Act of 1978, referred to in subsec. (a), is Pub. L. 95-511, Oct. 25, 1978, 92 Stat. 1783, as amended, which is classified principally to chapter 36 (§ 1801 et seq.) of Title 50, War and National Defense. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of Title 50 and Tables.

The Communications Assistance for Law Enforcement Act, referred to in subsecs. (a) and (b), is title I of Pub. L. 103-414, Oct. 25, 1994, 108 Stat. 4279, which is classified generally to subchapter I (§ 1001 et seq.) of chapter 9 of Title 47, Telegraphs, Telephones, and Radiotelegraphs. Sections 102 and 108 of the Act are classified to sections 1001 and 1007, respectively, of Title 47.



For complete classification of this Act to the Code, see Short Title note set out under section 1001 of Title 47 and Tables.

# CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSMISSIONAL RECORDS ACCESS

Sec.	
2701.	Unlawful access to stored communications.
2702.	Voluntary disclosure of customer communications or records.
2703.	Required disclosure of customer communications or records.
2704.	Backup preservation.
2705.	Delayed notice.
2706.	Cost reimbursement.
2707.	Civil action.
2708.	Exclusivity of remedies.
2709.	Counterintelligence access to telephone toll and transactional records.
2710.	Wrongful disclosure of video tape rental or sale records.
2711.	Definitions for chapter.
2712.	Civil actions against the United States.

## AMENDMENTS

2002—Pub. L. 107-273, div. B, title IV, § 4005(b), Nov. 2, 2002, 116 Stat. 1812, made technical correction to directory language of Pub. L. 107-56, title II, § 223(c)(2), Oct. 26, 2001, 115 Stat. 295, effective Oct. 26, 2001. See 2001 Amendment note below.

2001—Pub. L. 107-56, title II, §§ 223(c)(2), 224, Oct. 26, 2001, 115 Stat. 295, as amended by Pub. L. 107-273, div. B, title IV, § 4005(b), Nov. 2, 2002, 116 Stat. 1812, temporarily added item 2712.

Pub. L. 107-56, title II, §§ 212(a)(2), (b)(2), 224, Oct. 26, 2001, 115 Stat. 285, 295, temporarily substituted "Voluntary disclosure of customer communications or records" for "Disclosure of contents" in item 2702 and "Required disclosure of customer communications or records" for "Requirements for governmental access" in item 2703.

1988—Pub. L. 100-690, title VII, § 7067, Nov. 18, 1988, 102 Stat. 4405, which directed amendment of item 2710 by inserting "for chapter" after "Definitions" was executed by making the insertion in item 2711 to reflect the probable intent of Congress and the intervening redesignation of item 2710 as 2711 by Pub. L. 100-618, see below.

Pub. L. 100-618, § 2(b), Nov. 5, 1988, 102 Stat. 3197, added item 2710 and redesignated former item 2710 as 2711.

## § 2701. Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- (2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

- (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the

case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 103-322, title XXXIII, § 330016(1)(K), (U), Sept. 13, 1994, 108 Stat. 2147, 2148; Pub. L. 104-294, title VI, § 601(a)(3), Oct. 11, 1996, 110 Stat. 3498; Pub. L. 107-296, title II, § 225(j)(2), Nov. 25, 2002, 116 Stat. 2158.)

## AMENDMENTS

2002—Subsec. (b)(1). Pub. L. 107-296, § 225(j)(2)(A), in introductory provisions, inserted ", or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State" after "commercial gain".

Subsec. (b)(1)(A). Pub. L. 107-296, § 225(j)(2)(B), substituted "5 years" for "one year".

Subsec. (b)(1)(B). Pub. L. 107-296, § 225(j)(2)(C), substituted "10 years" for "two years".

Subsec. (b)(2). Pub. L. 107-296, § 225(j)(2)(D), added par. (2) and struck out former par. (2) which read as follows: "a fine under this title or imprisonment for not more than six months, or both, in any other case."

1996—Subsec. (b)(1)(A), (2). Pub. L. 104-294 substituted "fine under this title" for "fine of under this title".

1994—Subsec. (b)(1)(A). Pub. L. 103-322, § 330016(1)(U), substituted "under this title" for "not more than \$250,000".

Subsec. (b)(2). Pub. L. 103-322, § 330016(1)(K), substituted "under this title" for "not more than \$5,000".

## EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

## EFFECTIVE DATE

Section 202 of title II of Pub. L. 99-508 provided that: "This title and the amendments made by this title [enacting this chapter] shall take effect ninety days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect."

## SHORT TITLE OF 1988 AMENDMENT

Pub. L. 100-618, § 1, Nov. 5, 1988, 102 Stat. 3195, provided that: "This Act [enacting section 2710 of this title and renumbering former section 2710 as 2711 of this

**C**

United States Code Annotated Currentness

Federal Rules of Civil Procedure for the United States District Courts (Refs &amp; Annos)

▢ Title V. Disclosures and Discovery (Refs &amp; Annos)

→ **Rule 26. Duty to Disclose; General Provisions Governing Discovery****(a) Required Disclosures.****(1) Initial Disclosure.**

**(A) In General.** Except as exempted by Rule 26(a)(1)(B) or as otherwise stipulated or ordered by the court, a party must, without awaiting a discovery request, provide to the other parties:

**(i)** the name and, if known, the address and telephone number of each individual likely to have discoverable information--along with the subjects of that information--that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment;

**(ii)** a copy--or a description by category and location--of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment;

**(iii)** a computation of each category of damages claimed by the disclosing party--who must also make available for inspection and copying as under Rule 34 the documents or other evidentiary material, unless privileged or protected from disclosure, on which each computation is based, including materials bearing on the nature and extent of injuries suffered; and

**(iv)** for inspection and copying as under Rule 34, any insurance agreement under which an insurance business may be liable to satisfy all or part of a possible judgment in the action or to indemnify or reimburse for payments made to satisfy the judgment.

**(B) Proceedings Exempt from Initial Disclosure.** The following proceedings are exempt from initial disclosure:

**(i)** an action for review on an administrative record;

**(ii)** a forfeiture action in rem arising from a federal statute;

## 26a

- (iii) a petition for habeas corpus or any other proceeding to challenge a criminal conviction or sentence;
- (iv) an action brought without an attorney by a person in the custody of the United States, a state, or a state subdivision;
- (v) an action to enforce or quash an administrative summons or subpoena;
- (vi) an action by the United States to recover benefit payments;
- (vii) an action by the United States to collect on a student loan guaranteed by the United States;
- (viii) a proceeding ancillary to a proceeding in another court; and
- (ix) an action to enforce an arbitration award.

**(C) Time for Initial Disclosures--In General.** A party must make the initial disclosures at or within 14 days after the parties' Rule 26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in this action and states the objection in the proposed discovery plan. In ruling on the objection, the court must determine what disclosures, if any, are to be made and must set the time for disclosure.

**(D) Time for Initial Disclosures--For Parties Served or Joined Later.** A party that is first served or otherwise joined after the Rule 26(f) conference must make the initial disclosures within 30 days after being served or joined, unless a different time is set by stipulation or court order.

**(E) Basis for Initial Disclosure; Unacceptable Excuses.** A party must make its initial disclosures based on the information then reasonably available to it. A party is not excused from making its disclosures because it has not fully investigated the case or because it challenges the sufficiency of another party's disclosures or because another party has not made its disclosures.

**(2) Disclosure of Expert Testimony.**

**(A) In General.** In addition to the disclosures required by Rule 26(a)(1), a party must disclose to the other parties the identity of any witness it may use at trial to present evidence under Federal Rule of Evidence 702, 703, or 705.

**(B) Written Report.** Unless otherwise stipulated or ordered by the court, this disclosure must be accompanied by a written report--prepared and signed by the witness--if the witness is one retained or specially employed to provide expert testimony in the case or one whose duties as the party's employee regularly involve giving expert testimony. The report must contain:

- (i) a complete statement of all opinions the witness will express and the basis and reasons for them;
- (ii) the data or other information considered by the witness in forming them;
- (iii) any exhibits that will be used to summarize or support them;
- (iv) the witness's qualifications, including a list of all publications authored in the previous 10 years;
- (v) a list of all other cases in which, during the previous four years, the witness testified as an expert at trial or by deposition; and
- (vi) a statement of the compensation to be paid for the study and testimony in the case.

**(C) *Time to Disclose Expert Testimony.*** A party must make these disclosures at the times and in the sequence that the court orders. Absent a stipulation or a court order, the disclosures must be made:

- (i) at least 90 days before the date set for trial or for the case to be ready for trial; or
- (ii) if the evidence is intended solely to contradict or rebut evidence on the same subject matter identified by another party under Rule 26(a)(2)(B), within 30 days after the other party's disclosure.

**(D) *Supplementing the Disclosure.*** The parties must supplement these disclosures when required under Rule 26(e).

### **(3) *Pretrial Disclosures.***

**(A) *In General.*** In addition to the disclosures required by Rule 26(a)(1) and (2), a party must provide to the other parties and promptly file the following information about the evidence that it may present at trial other than solely for impeachment:

- (i) the name and, if not previously provided, the address and telephone number of each witness--separately identifying those the party expects to present and those it may call if the need arises;
- (ii) the designation of those witnesses whose testimony the party expects to present by deposition and, if not taken stenographically, a transcript of the pertinent parts of the deposition; and
- (iii) an identification of each document or other exhibit, including summaries of other evidence--separately identifying those items the party expects to offer and those it may offer if the need arises.

**(B) Time for Pretrial Disclosures; Objections.** Unless the court orders otherwise, these disclosures must be made at least 30 days before trial. Within 14 days after they are made, unless the court sets a different time, a party may serve and promptly file a list of the following objections: any objections to the use under Rule 32(a) of a deposition designated by another party under Rule 26(a)(3)(A)(ii); and any objection, together with the grounds for it, that may be made to the admissibility of materials identified under Rule 26(a)(3)(A)(iii). An objection not so made--except for one under Federal Rule of Evidence 402 or 403--is waived unless excused by the court for good cause.

**(4) Form of Disclosures.** Unless the court orders otherwise, all disclosures under Rule 26(a) must be in writing, signed, and served.

**(b) Discovery Scope and Limits.**

**(1) Scope in General.** Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense--including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).

**(2) Limitations on Frequency and Extent.**

**(A) When Permitted.** By order, the court may alter the limits in these rules on the number of depositions and interrogatories or on the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

**(B) Specific Limitations on Electronically Stored Information.** A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

**(C) When Required.** On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the

action; or

(iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

**(3) Trial Preparation: Materials.**

**(A) Documents and Tangible Things.** Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent). But, subject to Rule 26(b)(4), those materials may be discovered if:

(i) they are otherwise discoverable under Rule 26(b)(1); and

(ii) the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.

**(B) Protection Against Disclosure.** If the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation.

**(C) Previous Statement.** Any party or other person may, on request and without the required showing, obtain the person's own previous statement about the action or its subject matter. If the request is refused, the person may move for a court order, and Rule 37(a)(5) applies to the award of expenses. A previous statement is either:

(i) a written statement that the person has signed or otherwise adopted or approved; or

(ii) a contemporaneous stenographic, mechanical, electrical, or other recording--or a transcription of it--that recites substantially verbatim the person's oral statement.

**(4) Trial Preparation: Experts.**

**(A) Expert Who May Testify.** A party may depose any person who has been identified as an expert whose opinions may be presented at trial. If Rule 26(a)(2)(B) requires a report from the expert, the deposition may be conducted only after the report is provided.

**(B) Expert Employed Only for Trial Preparation.** Ordinarily, a party may not, by interrogatories or deposition, discover facts known or opinions held by an expert who has been retained or specially employed by

## 30a

another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial. But a party may do so only:

(i) as provided in Rule 35(b); or

(ii) on showing exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means.

(C) *Payment.* Unless manifest injustice would result, the court must require that the party seeking discovery:

(i) pay the expert a reasonable fee for time spent in responding to discovery under Rule 26(b)(4)(A) or (B); and

(ii) for discovery under (B), also pay the other party a fair portion of the fees and expenses it reasonably incurred in obtaining the expert's facts and opinions.

**(5) *Claiming Privilege or Protecting Trial-Preparation Materials.***

(A) *Information Withheld.* When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:

(i) expressly make the claim; and

(ii) describe the nature of the documents, communications, or tangible things not produced or disclosed--and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.

(B) *Information Produced.* If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

**(c) *Protective Orders.***

(1) *In General.* A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending--or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in

good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

- (A) forbidding the disclosure or discovery;
- (B) specifying terms, including time and place, for the disclosure or discovery;
- (C) prescribing a discovery method other than the one selected by the party seeking discovery;
- (D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters;
- (E) designating the persons who may be present while the discovery is conducted;
- (F) requiring that a deposition be sealed and opened only on court order;
- (G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way; and
- (H) requiring that the parties simultaneously file specified documents or information in sealed envelopes, to be opened as the court directs.

(2) **Ordering Discovery.** If a motion for a protective order is wholly or partly denied, the court may, on just terms, order that any party or person provide or permit discovery.

(3) **Awarding Expenses.** Rule 37(a)(5) applies to the award of expenses.

**(d) Timing and Sequence of Discovery.**

(1) **Timing.** A party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order.

(2) **Sequence.** Unless, on motion, the court orders otherwise for the parties' and witnesses' convenience and in the interests of justice:

- (A) methods of discovery may be used in any sequence; and



(B) discovery by one party does not require any other party to delay its discovery.

**(e) Supplementing Disclosures and Responses.**

(1) ***In General.*** A party who has made a disclosure under Rule 26(a)--or who has responded to an interrogatory, request for production, or request for admission--must supplement or correct its disclosure or response:

(A) in a timely manner if the party learns that in some material respect the disclosure or response is incomplete or incorrect, and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing; or

(B) as ordered by the court.

(2) ***Expert Witness.*** For an expert whose report must be disclosed under Rule 26(a)(2)(B), the party's duty to supplement extends both to information included in the report and to information given during the expert's deposition. Any additions or changes to this information must be disclosed by the time the party's pretrial disclosures under Rule 26(a)(3) are due.

**(f) Conference of the Parties; Planning for Discovery.**

(1) ***Conference Timing.*** Except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B) or when the court orders otherwise, the parties must confer as soon as practicable--and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b).

(2) ***Conference Content; Parties' Responsibilities.*** In conferring, the parties must consider the nature and basis of their claims and defenses and the possibilities for promptly settling or resolving the case; make or arrange for the disclosures required by Rule 26(a)(1); discuss any issues about preserving discoverable information; and develop a proposed discovery plan. The attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging the conference, for attempting in good faith to agree on the proposed discovery plan, and for submitting to the court within 14 days after the conference a written report outlining the plan. The court may order the parties or attorneys to attend the conference in person.

(3) ***Discovery Plan.*** A discovery plan must state the parties' views and proposals on:

(A) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement of when initial disclosures were made or will be made;

(B) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;

(C) any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;

(D) any issues about claims of privilege or of protection as trial-preparation materials, including--if the parties agree on a procedure to assert these claims after production--whether to ask the court to include their agreement in an order;

(E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and

(F) any other orders that the court should issue under Rule 26(c) or under Rule 16(b) and (c).

(4) ***Expedited Schedule.*** If necessary to comply with its expedited schedule for Rule 16(b) conferences, a court may by local rule:

(A) require the parties' conference to occur less than 21 days before the scheduling conference is held or a scheduling order is due under Rule 16(b); and

(B) require the written report outlining the discovery plan to be filed less than 14 days after the parties' conference, or excuse the parties from submitting a written report and permit them to report orally on their discovery plan at the Rule 16(b) conference.

**(g) Signing Disclosures and Discovery Requests, Responses, and Objections.**

(1) ***Signature Required; Effect of Signature.*** Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name--or by the party personally, if unrepresented--and must state the signer's address, e-mail address, and telephone number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

(A) with respect to a disclosure, it is complete and correct as of the time it is made; and

(B) with respect to a discovery request, response, or objection, it is:

(i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;

(ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and

(iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

**(2) *Failure to Sign.*** Other parties have no duty to act on an unsigned disclosure, request, response, or objection until it is signed, and the court must strike it unless a signature is promptly supplied after the omission is called to the attorney's or party's attention.

**(3) *Sanction for Improper Certification.*** If a certification violates this rule without substantial justification, the court, on motion or on its own, must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both. The sanction may include an order to pay the reasonable expenses, including attorney's fees, caused by the violation.

#### CREDIT(S)

(Amended December 27, 1946, effective March 19, 1948; January 21, 1963, effective July 1, 1963; February 28, 1966, effective July 1, 1966; March 30, 1970, effective July 1, 1970; April 29, 1980, effective August 1, 1980; April 28, 1983, effective August 1, 1983; March 2, 1987, effective August 1, 1987; April 22, 1993, effective December 1, 1993; April 17, 2000, effective December 1, 2000; April 12, 2006, effective December 1, 2006; April 30, 2007, effective December 1, 2007.)

Amendments received to 01-01-10

Westlaw. (C) 2010 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

END OF DOCUMENT