

WHITE-COLLAR CRIME

Expert Analysis

The Wire: Higher Likelihood Innocent Conversations Are Being Intercepted

Nearly a half-century ago, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. §2510 et seq., to establish a comprehensive scheme for the regulation of wiretapping and electronic surveillance. “To safeguard the privacy of innocent persons,” Title III prohibits all wiretapping and electronic surveillance except that conducted by duly authorized law enforcement officers under narrowly prescribed conditions—including a showing that normal investigative procedures have failed or are likely to fail.¹

Against this backdrop, consider the following: between 2001 and 2010, while there were 19,282 wiretaps authorized, only three wiretap applications were denied. Similarly remarkable is that of all intercept applications made during 2010, only one was denied.

Understandably, there has been a rapid growth in the number of wiretap authorizations, particularly in the last decade since the enactment of the PATRIOT Act. The number of authorized interceptions increased from 1,491 authorized in 2001 to 3,194 in 2010—more than double. Yet, while there has been an increase in the number of intercepts, the number of “incriminating intercepts” has steadily declined. The percentage of authorizations resulting in convictions of individuals wiretapped has likewise declined.

These statistics lead to a disturbing conclusion: The number of innocent people being wiretapped has increased over the past decade. While there has been an increase in the total number of wiretap authorizations, more than two-thirds of the intercepts are capturing non-incriminating content. And only one-third of the intercepts are resulting in conviction. A close examination of wiretap order statistics over the past decade reveals that more innocent people are having their private conversations intercepted with less discerning judicial scrutiny of the government’s requests.

The data raises significant questions about the

ELKAN ABRAMOWITZ is a member of *Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer*. He is a former chief of the criminal division in the U.S. Attorney’s Office for the Southern District of New York. BARRY A. BOHRER is a member of *Morvillo, Abramowitz* and was formerly chief appellate attorney and chief of the major crimes unit in the Southern District U.S. Attorney’s Office. GRETCHAN R. OHLIG, an attorney, assisted in the preparation of this article.



By
**Elkan
Abramowitz**



And
**Barry A.
Bohrer**

role of the judiciary as gatekeeper for this highly intrusive investigative tool. Because significant privacy interests are implicated in the use of wiretaps and because their implementation carries a substantial financial burden, one would expect the judiciary to exercise its powers in this regard by strictly scrutinizing applications. However, wiretap applications are granted almost without exception. Further, recent cases demonstrate inconsistency among federal courts in the application of federal wiretap law intended to protect the crucial interests at stake.

While there has been an increase in the number of intercepts, the number of ‘incriminating intercepts’ has steadily declined.

2010 Wiretap Report

The Administrative Office of the U.S. Courts is required by statute to report annually to Congress on the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The most recent report available to the public covers intercepts concluded in the 2010 calendar year. Ninety-nine percent of those intercepts were obtained over the wire, also known as telephone surveillance, and almost all of those wiretaps were placed on portable devices such as cellular and mobile phones. A comparison of the data contained in the 2010 report with that set forth in the archived reports shows that despite increases in the number of wiretaps and the number of individuals impacted by wiretaps, there has not been a corresponding increase in the number of

incriminating intercepts or arrests and convictions resulting from intercepts.²

• **Number of People Intercepted.** The average number of individuals intercepted per federal wiretap in 2010 was 121. That number multiplied by the 1,027 federal intercepts authorized in that year would mean that the total number of individuals having their private conversations intercepted totaled somewhere in the vicinity of 124,000 people. This reveals an almost 130 percent increase over the approximately 54,000 individuals affected by wiretaps in 2001.

• **Number of Incriminating Intercepts/Convictions Resulting From Intercepts.** In 2010, on average, only 19 percent of the total number of intercepts made were deemed incriminating. Further, of the 2,252 individuals arrested in federal cases involving wiretaps, only 296, or 13 percent, of those individuals have actually been convicted of a federal crime.³ Despite large increases in the number of wiretaps and conversations intercepted, these percentages have held fairly steady, within a few single digits increases and decreases, since 2001. However, a look at the data on wiretaps authorized by state and federal courts combined reveals the same increase in wiretaps authorized and individuals impacted, but a significant decline in the percentages of incriminating intercepts and intercepts resulting in convictions over the past decade.

Judicial Treatment of Act

Non-profit civil liberties organizations refer to the statistics generated by the Administrative Office of the U.S. Courts as “worrisome,” opining that the increase in wiretap authorizations and individuals intercepted without a corresponding increase in convictions and incriminating intercepts reveal that the privacy rights of innocent individuals—purportedly protected by Title III—are endangered by the increase in wiretaps.⁴ These organizations assert that the authorization of such an overwhelming percentage of wiretap applications by courts mandates strict judicial scrutiny and adherence to Title III.⁵

Congress enacted Title III to establish a “comprehensive scheme for the regulation of wiretapping and electronic surveillance” that would both implement the Fourth Amendment’s “stringent” requirements and enforce congressional policy “strictly to limit the employment” of wiretapping.⁶ Federal case law raises legitimate concerns about

judicial adherence to the statutory mandates of Title III and congressional intent, however. Those concerns are now in play in a prominent white-collar prosecution.

• **‘United States v. Rajaratnam’—the Wire and Insider Trading.** According to prosecutors, this high-profile case in the Southern District of New York marks “the first time that court-authorized wiretaps have been used to target significant insider trading on Wall Street.”⁷ In March 2008, the FBI obtained a wiretap order for Rajaratnam’s cell phone, which order was in place for nine months. Rajaratnam moved to suppress the wiretaps, arguing that the government’s wiretap application contained false statements and material omissions that impeded the ability of the authorizing judge to make the statutorily required determinations for the issuance of the wiretap warrant.

Title III requires that the government’s wiretap application: 1) demonstrate probable cause to believe that a suspect is using a location or device to communicate about a crime; and 2) make a showing of the necessity of the wiretap, which includes a full and complete statement as to whether or not other investigative procedures have been tried and failed, are unlikely to succeed if tried, or are too dangerous to attempt.⁸ Rajaratnam argued that the government made false statements and omissions in establishing both requirements.⁹

After a hearing pursuant to *Franks v. Delaware*, Southern District of New York Judge Richard J. Holwell denied the motion. Holwell held that, although the government’s affidavit recklessly omitted mention of a parallel SEC investigation of the defendant into the very same activity at issue in the criminal case, the government’s affidavit in support of its wiretap application “amply supported” a finding of probable cause and necessity once factually corrected and would not have affected the authorizing judge’s findings of probable cause or necessity. Rajaratnam has appealed this decision to the Second Circuit.¹⁰

The government’s response, filed last week, argues that suppression was not appropriate for two reasons: (i) the district court correctly ruled that the challenged wiretap affidavit did not contain errors or omit facts that would have changed the findings of probable cause and necessity; and (ii) the district court committed legal error in determining that the wiretap affiant acted with reckless disregard for the truth.

In a related case, Southern District Judge Jed Rakoff, denied a similar motion, finding Judge Holwell’s *Franks* approach to be the appropriate framework to evaluate the defendants’ attack on the truthfulness of the wiretap affidavit and agreed with his colleague’s conclusions regarding the non-materiality of the omissions.¹¹

• **Title III’s Exclusionary Rule—a Toothless Remedy?** Where intercepts are made in violation of Title III, §2515 of the statute provides that “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.” As wiretap applications are being granted with greater

frequency (and, perhaps, lesser scrutiny), it has been argued that preserving the integrity of Title III’s absolute bar on the use of illegal intercepts becomes even more important. Those arguments, however, have largely foundered as courts have failed consistently to adhere to the plain text of the statute. For example, despite the unequivocal language of Section 2515, courts are divided on whether an exception exists to allow the use of unlawfully obtained wiretaps for impeachment purposes—something noticeably absent in the plain language of the statute.

A number of federal courts have read an impeachment exception into Section 2515, allowing the admission of illegally obtained wiretaps to impeach a criminal defendant’s testimony¹² or a party’s affidavit in a civil case.¹³ In so finding, courts have relied on the Supreme Court’s decision in *Walder v. United States*,¹⁴ which permitted the use of evidence obtained in violation of the Fourth Amendment for impeachment purposes. At the time Title III was passed, a report from the Senate Judiciary Committee specifically cited *Walder* in stating that “Congress did not intend to ‘press the scope of the suppression [rule] beyond present search and seizure law.’”¹⁵

Believing that Congress had the background of the *Walder* impeachment exception in mind when passing Title III, courts have reached the dubious conclusion that “[i]t makes no sense for evidence obtained in violation of a mere statute to be more severely restricted than evidence obtained in violation of the Constitution.”¹⁶ Of course, in Title III, Congress plainly stated such an intention and wrote a statute with a more exacting standard than the Fourth Amendment.

A number of federal courts have read an impeachment exception into Section 2515, allowing the admission of illegally obtained wiretaps to impeach a criminal defendant’s testimony or a party’s affidavit in a civil case.

Other federal circuit courts have rejected this argument, relying on the plain language of Section 2515 to prohibit the use of illegal wiretaps for impeachment in certain circumstances.¹⁷ Notably, however, these courts have only precluded impeachment for criminal defendants or private litigants. These courts have only allowed the government to use illegally obtained wiretap evidence for impeachment in criminal cases. The U.S. Court of Appeals for the First Circuit has applied Section 2515 differently depending on the type of case and the person who invokes it. It has held that *Walder* does not justify deviation from the statute’s plain language and “broad remedial purposes” in civil cases or criminal cases for witnesses other than the defendant.¹⁸

Earlier this year, the Supreme Court declined to consider the federal circuits’ divided interpretation of Section 2515.¹⁹ In addition, other courts have relied on the decisions grafting an impeachment exception into Section 2515 to consider whether other Fourth Amendment

exceptions to the exclusionary rule, such as good faith or clean hands, may be incorporated into Section 2515,²⁰ straying further from the plain language of the statute.

Conclusion

Nearly 50 years after its enactment, important issues remain regarding the strict application of Title III and whether the government is held to the standards set forth therein when seeking a wiretap order to invade an individual’s privacy rights. Answers to these questions are critical because, as the government’s own data shows, privacy invasions are occurring with greater frequency despite the fact that the government has little to show in the way of convictions for its increased reliance on electronic surveillance.

.....●●.....

1. *United States v. Giordano*, 416 U.S. 505, 511 (1974)
2. The Wiretap Reports from 1997 through and including 2010 are available on the Administrative Office of the United States Courts website at http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports_Archive.aspx.
3. Convictions resulting from an intercept often do not occur within the same year in which the intercept was first reported. 2010 Wiretap Report at p. 27, Table 6.
4. Brief of Electronic Frontier Foundation and Center for Constitutional Rights as Amici Curiae in Support of Petitioner at 2, *Simels v. United States*, No. 11-947, (U.S., Feb. 28, 2012).
5. 18 U.S.C. §2510 et. seq.
6. *Gelbard v. United States*, 408 U.S. 41, 46, 47 (1972).
7. Prepared Remarks for U.S. Attorney Preet Bharara, “*United States v. Raj Rajaratnam; United States v. Danielle Chiesi*, Hedge Fund Insider Trading Takedowns” (Oct. 16, 2009).
8. 18 U.S.C. §2518.
9. 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010).
10. *United States v. Rajaratnam*, 11-4416-cr. (2d Cir.), Brief for Defendant-Appellant at 6 (Jan. 25, 2012).
11. *United States v. Gupta*, 2012 WL 1066817 (S.D.N.Y. March 27, 2012).
12. See *United States v. Bafiri*, 263 F.3d 856 (8th Cir. 2001); *United States v. Caron*, 474 F.2d 506 (5th Cir. 1973).
13. See *Culbertson v. Culbertson*, 143 F.3d 825 (4th Cir. 1998).
14. 74 S. Ct. 354 (1954).
15. 654 F.3d at 169 (citing S. Rep. No. 1097, 90th Cong., 2d Sess., at 68 (1968)).
16. *Bafiri*, 263 F.3d at 857.
17. See *United States v. Wuliger*, 981 F.2d 1497 (6th Cir. 1992) (finding Section 2515 prohibits use of illegal wiretaps to impeach any witness in civil cases); *Anthony v. United States*, 667 F.2d 870 (10th Cir. 1981) (prohibiting defendant’s use of illegal wiretaps for impeachment of government witnesses); *United States v. Liddy*, 509 F.2d 428 (D.C. Cir. 1974) (court’s previous order prohibiting defendant from using illegal intercepts to cross-examine witnesses did not violate defendant’s Sixth Amendment rights).
18. See *Williams v. Poulous*, 11 F.3d 271 (1st Cir. 1993). See also *United States v. Lanoue*, 71 F.3d 966 (1st Cir. 1995) (impeachment exception does not apply to witnesses in criminal case other than defendant), abrogated on other grounds by *United States v. Watts*, 519 U.S. 148 (1997).
19. *Simels v. United States*, ___ S. Ct. ___, 2012 WL 297180 (March 5, 2012).
20. See 3A Charles A. Wright and Sarah N. Welling, “Federal Practice and Procedure §685” (4th ed. 2010).