



Is Someone Eavesdropping on Your Attorney-Client Conversations?

A lawyer and his client are sitting in a café having coffee while on recess in a major case. They turn off their cell phones so that no one will interrupt them. They lean forward for a highly confidential tête-à-tête. However, they are not the only ones interested in their discussion. Unknown to them, a third-party — miles away — remotely turns on the lawyer's cell phone and records every word of the conversation. When

the conversation ends the lawyer turns on his phone, calls his investigator, and gets the latest on statements taken from key witnesses. The third-party records that conversation too, and while she is at it, downloads all the text messages and e-mails the lawyer has on his cell phone. She downloads the telephone numbers, dates, exact times, and duration of the conversations. Finally, she downloads information telling her the lawyer's location when he placed or received cell phone calls during the past month. Fantastic? Futuristic? Not at all. It is happening now.

Activity Monitors

Eavesdropping has been around as long as eaves, the beams that form the two long sides of an A-frame roof. Eavesdroppers supposedly climbed up on the eaves to listen in on private conversations. Nowadays, that kind of physical eavesdropping is no longer a credible threat. While it may be trespassing, the Omnibus Crime Control and Safe Streets Act does not prohibit it.¹

Technical surveillants, many of whom prefer to be addressed by the more Orwellian "Activity Monitors" appellation, have developed technical means of invading privacy. Common telephone taps are as old as the 1940s, but have grown progressively more sophisticated. The hook switch bypass was a device that circumvented the off button on the receiver of the old rotary dial telephones. In effect, the telephone microphone could be turned on remotely just as if it were off the hook, and someone miles away could listen to what was being said in a room. In the 1950s, Manny Middleman devised a way to activate a hookswitch bypass by calling a telephone that had one installed on it (which required a previous burglary to install) and blowing a certain key on a harmonica into the phone. He could then listen to conversations for as long as he liked from wherever he liked.

Taps are devices that are placed on telephone lines for purposes of covert eavesdropping. Bugs are devices placed in a room or area for the same purpose. Transmitters are physical objects that are easy to hide because of their incredibly small size, but they still require entry into the target area to plant.² Hal Lipset, a San Francisco private investigator, waltzed around a cocktail party in the 1960s with a transmitter hidden in an olive in his martini.³ The toothpick was hollowed out for the antenna. Considering that he did it at about the time that color televisions were beginning to appear in homes in America, this was a considerable feat.

Eavesdropping devices have kept abreast of the times — advancing from ultrasophisticated electronics such as tiny frequency-hopping burst transmitters that compress and store conversations and transmit them through the air in short bursts that hop about in a preset

BY LOUIS L. AKIN

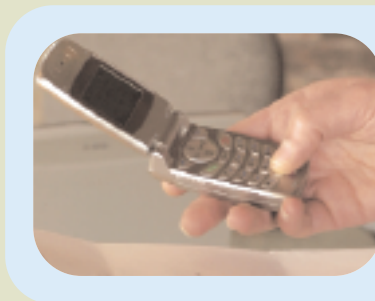
pattern amongst multiple frequencies.⁴ To receive the messages, the eavesdropper has to know not only when they are going to be transmitted, but the exact order of frequency hops they will make during the short burst of transmission. The eavesdropper's receiver has to hop with the transmitter to capture the electronic bursts and then demodulate them.

Eavesdropping devices can be physically installed on cell phones or computers in a matter of seconds by an intruder (a cleaning person, inspector, customer, client, sales person, acquaintance, police officer, or burglar). In the alternative, the device might be sent to the "target" by e-mail or text message. When programs are installed in the latter manner, they are called Trojans, a kind of virus that is packaged as something attractive or expected.

For example, a consumer might get a text message on his cell phone saying, "Call 314-666-1234 to update your Verizon cell phone software," or "Download free new ring tones." When the consumer calls to get the update, he or she gets a Trojan that installs in the cell phone as a digital eavesdropping device. No burglary required. The phone will turn on so the eavesdropper can listen to room conversation or auto-dial the eavesdropper and give such private information as the telephone number, date and exact time of each call, and the location (within feet) of each incoming or outgoing call the cell phone owner makes or receives. It will also send any text messages or e-mail to the eavesdropper.

FlexiSpy Products's FlexiSpy Pro⁵ spyware cell phone tap (\$49.95) is one of the latest commercially available cell phone eavesdropping devices on the market, but it is not the only one. Many competitors produce similar programs. Anti-virus software companies and tech writers condemn the program as blatant spyware that can turn on a cell phone (just like Manny Middleman used to do) and allow an eavesdropper to listen in on every conversation that takes place within earshot of the cell phone while the owner of the phone thinks it is off. Now, since most of us wear our cell phones on our belts . . .

FlexiSpy advertises its product as the "World's Most Powerful Spy Software for Mobile Phones. FlexiSpy Pro is a mobile phone monitoring application that secretly records all activity on a mobile phone that has FlexiSpy Pro installed. Protect your children, catch cheating spouses. The possibilities are endless." The possibilities for abuse are endless, too.



The eavesdropping devices Louis Akin describes in his article (page __) are already being used to listen in on conversations. In *United State v. Tomero*, the FBI used a cell phone's microphone to eavesdrop. The listening devices, called "roving bugs," functioned even when the phone was truned off.

United States v. Tomero, et al.

UNITED STATES v. TOMERO, et al.
U.S. District Court, S.D.N.Y.
No. S2 06 Crim. 0008(LAK); 2006 WL 3404770
Nov. 27, 2006

KAPLAN, District Judge. Thirty-four defendants are charged with various criminal acts associated with the operations of the Genovese organized crime family. Ten move to suppress conversations intercepted by listening devices, colloquially known as "roving bugs," installed in cellular telephones.

Background

A. The Investigation

1. The Traditional Intercepts

The indictment stems from a three-year investigation into the criminal activity of members and associates of the Genovese organized crime family. The investigation initially focused on the crew of John Ardito, a high-ranking member of the family. The FBI learned from cooperating witnesses that Ardito's crew met regularly at a restaurant called Brunello Trattoria in New Rochelle, New York, to conduct family business. In December 2002, the Honorable Barbara S. Jones of this Court authorized the interception of oral communications of Ardito and other subjects at this location.

The intercepted conversations revealed that Ardito and his crew met at three additional restaurants, in part because they were suspicious of law enforcement surveillance. The government applied for, and Judge Jones authorized, the interception of conversations at these three restaurants as well as continued interception at Brunello Trattoria. In July 2003, however, Ardito's crew found the listening devices in three of the restaurants and became even more wary of surveillance whenever they returned to their usual meeting places.

2. The Roving Intercepts

a. Ardito's Cellular Telephone

Based on physical surveillance and the conversations previously intercepted, the FBI learned that Ardito's crew no longer conducted meetings exclusively at the four restaurants, but met also in twelve additional restaurants, automo-

biles, Ardito's home, an auto store, an insurance office, a jewelry store, a doctor's office, a boat, and public streets.

The government applied for a "roving bug," that is, the interception of Ardito's conversations at locations that were "not practical" to specify, as authorized by 18 U.S.C. § 2518(11)(a). Judge Jones granted the application, authorizing continued interception at the four restaurants and the installation of a listening device in Ardito's cellular telephone.¹ The device functioned whether the phone was powered on or off, intercepting conversations within its range wherever it happened to be.

b. Peluso's Cellular Telephone

By February 2004, the government had learned that Peter Peluso, an attorney and close associate of Ardito, was relaying messages to and from high-ranking family members who were wary of government listening devices and who used Peluso as a messenger to avoid meeting together directly. In a renewal application dated February 6, 2004, the government sought, and Judge Jones in due course granted, authority to install a roving bug in Peluso's cellular telephone.² This order was renewed several times throughout 2004, as the government continued to identify locations where Peluso and Ardito discussed family matters and learned that the subjects were growing increasingly cautious of government surveillance.

In January 2005, Peluso agreed to cooperate with the government's investigation. At that point the government removed the listening device in his cellular telephone and Peluso began recording conversations with family members consensually by wearing a microphone. On July 7, 2005, Peluso pleaded guilty, pursuant to a cooperation agreement with the government, to a four-count information, charging him with, among other things, engaging in a pattern of racketeering activity.

3. This Motion

By the conclusion of the investigation, the government had intercepted hundreds of hours of Ardito's and Peluso's conversations with each other and with other defendants, including

Claudio Caponigro, Pasquale De Luca, Albert Faella, Albert Facciano, Gerald Fiorino, Walter Galiano, Salvatore Larca, Vincent Russo, and Albert Tranquillo, Jr.

On February 14, 2006, a grand jury returned a 42-count indictment charging 32 defendants with wide-ranging racketeering crimes and other offenses spanning more than a decade. On April 3, 2006, the grand jury returned a 45-count superceding indictment naming two additional defendants. Defendants now seek suppression of the conversations intercepted by the listening devices in the Ardito and Peluso cellular telephones.

Discussion

Title III of the Omnibus Crime Control and Safe Streets Act ("Title III")³ sets forth procedures for the interception of oral communications. Sections 2518(1)(b)(ii) and (3)(d) require, respectively, that an application for electronic surveillance include "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted"⁴ and be based on "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 about to be used, in connection with the commission of" an offense.⁵

In 1986, Congress amended Title III to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."⁶ One of the amendments was Section 2518(11), which permits "roving" electronic surveillance. It provides that

"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."⁷

Section 2518(12) further provides that an agent implementing a roving intercept under subsection 11 must ascertain the place of the communication in advance of interception.⁸

A. Constitutionality of Section 2518(11)

1. Facial Challenge

Defendants argue that the roving bug provision of Title III is unconstitutional because it fails to comport with the Fourth Amendment's requirement that a warrant "particularly describ[e] the place to be searched."⁹ In other words, by allowing the government to intercept communications without identifying the place of interception in advance, the statute authorizes general warrants.

In *United States v. Bianco*,¹⁰ the Second Circuit upheld Section 2518(11) against an identical constitutional challenge.¹¹ That holding is binding here. The facial challenge therefore is foreclosed.

2. As-Applied Challenge

Defendants argue that *Bianco* is distinguishable. The argument, however, is unpersuasive.

a. Mobile Interception Devices

Defendants point first to the fact that the order in *Bianco* authorized the placement of listening devices only in buildings whereas the order here authorized placement in mobile telephones. But the argument misses the point.

The essence of the motion to suppress is that the statute unconstitutionally permits interception in the absence of any specification of the place where communications are to be intercepted. In *Bianco*, the Second Circuit rejected precisely this argument. The fact that the unspecified location in *Bianco* happened to be in a building had nothing to do with the holding. Furthermore, while a mobile device makes interception easier and less costly to accomplish than a stationary one, this does not mean that it implicates new or different privacy concerns. It simply dispenses with the need for repeated installations and surreptitious entries into buildings. It does not invade zones of privacy that the government could not reach by more conventional means.

b. Particular Conversations

Defendants next seek to distinguish *Bianco* on the ground that the government in that case had a particular meeting in mind when it sought authorization to intercept. Again, the distinction is irrele-

According to the FlexiSpy Web site:

"You can listen in on calls and read SMS/MMS messages. What's more, even when the phone is not in use, you can remotely activate the microphone and listen in on non-call conversations. Of course, the legality of this falls in a grey area."

Actually, it is plainly illegal to use the tap on anyone except your minor children. FlexiSpy adds the limp caveat:

"If you are the owner of your spouse's (or child's) cell phone, you are merely monitoring your property, but if you use FlexiSpy Pro on an unsuspecting neighbor, that's a different story altogether."

FlexiSpy Products adamantly denies that FlexiSpy Pro tap is a Trojan, stating that it has to be consciously installed by a real live human. Yet the critics disagree. "This application installs itself without any kind of indication as to what it is. And when it is installed on the phone it completely hides itself from the user," says Jarno Niemela, a researcher for F-Secure.

This is a case in which both parties may be right — at least on the surface. A person has to consciously install the program, but that person does not have to be the cell phone owner. On the other hand, if it is sent as a Trojan, the person installing it may not know that it is spyware. The missing words are "effective legal consent of the cell phone user."

F-Secure warns consumers⁸

"When FlexiSpy Pro is installed on the phone it will hide from Symbian's built-in process menu and it does not have any visible user interface or icon. After FlexiSpy Pro is installed on the phone, the only indication that it is installed is that the application removal menu has an additional application named 'phones' in the list. This 'phones' application cannot be removed with the application manager.

FlexiSpy Pro has a hidden user interface that can only be accessed using a special code known to the person who has purchased the spying application and has installed it on the phone.

When FlexiSpy Pro is active on the device, it will record details of all voice call and SMS information, and then later send those details to the FlexiSpy Pro server."

Law enforcement has a cell phone

tap that is more limited but easier to install. When law enforcement officers get your cell phone number, they go to a Web site to find out the name of the service provider. They obtain a search warrant, call the service provider, and have the provider clone the phone on which they want to eavesdrop. The provider sends them a chip via overnight mail. Thereafter, each time the target uses the cell phone to make or receive calls or text messages, the police department receives the calls and records them. This technique is an updated version of the lease-line method of tapping land lines that was popular before cells phones came along.

Digital cell phone taps may be the newest technology available to the general public, but plenty of the old gear is still around and it works well. FM radio frequency transmitters that sell for \$20 in electronics stores make ideal drop bugs, i.e., disposables. Disposables are transmitter bugs that can be left somewhere to transmit until their battery runs dry, and then they can be forgotten. The eavesdropper does not have to make a second entry to recover the devices. These bugs are cheap and untraceable; nearly every law enforcement agency uses them. They are also used by private investigators, people getting divorced, partners terminating a business relationship, possessive spouses, and others.

Carrier current devices are also available at electronics stores. They are sold as baby monitor systems. Strip off the baby blue or pink plastic case and the device can be hidden anywhere in a house or building's electrical system, inside or out. It will transmit conversations from inside the house or office along the AC wiring to

a receiver down the line. Room to room plug-in intercom systems do the same thing and are used by eavesdroppers for the same purposes. They are also commonly available in electronics stores.⁹ More sophisticated devices include light switches and wall plugs that really work to turn on lights or run a vacuum, but also work as transmitters when there is a conversation in the room

Compromising Computers

Activity monitoring software, also known as key logger spyware, has been in circulation among amateur and professional eavesdroppers, mainly law enforcement, for at least a decade or more. The FBI was the first agency to acknowledge using it. There are two versions of key logger eavesdropping devices. The first is a hardware device that attaches to the back of the computer. It fits in line and looks like part of the cable in the back of the computer. Its disadvantage is that it requires a physical installation and has to be retrieved at some point. The other version of a key logger is software which can be sent by e-mail as a Trojan. It is the more insidious implant.

The key logger software programs sell in various stores for approximately \$100-200. The software is easily concealed in e-mail or as a Trojan and it installs within seconds. Once installed, it gives erroneous file name information and changes its name and position each time the computer boots. Forensic computer analysts are needed to find, identify, and remove the software, and to make a forensic copy of the hard drive for purposes of evidence and testifying in court.

Key loggers give a third-party access to every file and document on the target

United States v. Tomero, et al. (continued)

vant. Nothing in *Bianco* suggests that the constitutionality of the statute and the order hinged on the fact that the government knew that a particular meeting was to take place. The issue was whether it knew the location of the anticipated meeting when it obtained the order. It did not, but the order nevertheless was held constitutional.

c. Ten-Day Status Reports

Finally, defendants argue that *Bianco* is distinguishable because the order in that case required status reports every seven days instead of every ten. This difference is immaterial. A progress report every ten days was sufficient to keep the issuing court apprised of the status of the investigation and to alert it to any potential government overreaching. Like the issuing judge in *Bianco*, had Judge Jones suspected any government misconduct, she could have revoked or revised the order at any time.¹²

B. Section 2518 Requirements

1. Other Investigative Procedures

An application for electronic surveillance must include, among other things, "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."¹³ Defendants argue that the application failed adequately to do so.

As this Court has held, Section 2518(3)(c)'s exhaustion requirement "is far from an insurmountable hurdle. The government must demonstrate only that normal investigative techniques would prove difficult."¹⁴ All that is required is "a reasoned explanation, grounded in the facts of the case, and which squares with common sense."¹⁵ Moreover, as with the issuing judge's determination of probable cause, "a determination that the government has made this showing is entitled to substantial deference from a reviewing court."¹⁶

Defendants contend that there was no " 'genuine need' for either the Peluso or the Ardito roving bug."¹⁷ They suggest that the government could have relied on its confidential informants, preexisting warrants, or an undercover agent in order to obtain the information it sought.

The government addressed these possibilities in its applications. First, it stated that its confidential informants were unhelpful to the investigation because they were not privy to relevant conversations, in part because the defendants changed meeting locations frequently. In addition, one such informant was unwilling to wear a microphone or testify in court.¹⁸

Here's how the FlexiSpy Pro model works when it is installed:

Target Cell Phone ⁷	→ FlexiSpy Pro Server	→ Any designated computer
SMS messages	Holds for relay 24 hours a day 7 days a week	Any designated computer connected to the Web may retrieve the information
E-mail		
Telephone conversations		
Live voice		
Call history		

Second, the government explained that physical surveillance had been useful in “placing people with each other” and observing that meetings took place, but that it “provide[d] limited evidence of the purpose of the meetings or the content of [the subjects’] conversations.”¹⁹

Third, the government asserted that an undercover operation was “not feasible due, in part, to the unwillingness of the SUBJECTS to deal extensively with outsiders who are not members or associates of” the family or related organizations.²⁰

Finally, the government explained why more traditional methods of surveillance than roving intercepts were insufficient. It stated that wiretaps on the Ardito and Peluso cellular telephones were not successful because the subjects “were extremely careful and guarded on the cellphone, [and] recognize[d] the potential for electronic interception.”²¹ Further, the conversations intercepted at the four restaurants painted a limited picture of the subjects’ criminal activity because defendants were aware of the listening devices there and held meetings in other places, such as public streets, where the risk of surveillance was low.²²

The applications made a sufficient case for electronic surveillance. They indicated that alternative methods of investigation either had failed or were unlikely to produce results, in part because the subjects deliberately avoided government surveillance.

2. Identification of Interceptees

Defendants argue also that the order is invalid because the government failed to identify “the person . . . whose communications are to be intercepted.”²³ They point to the fact that the government’s applications named specific subjects, but referred also to “others as yet unknown.”

The statute limits interception to situations where “a particular identified individual or individuals can be expected to use numerous telephones or locations to discuss their crimes as a means of evading surveillance.”²⁴ It does not require the government to name every person whose voice it will capture, however. Rather, use of the singular “person” indicates that the government must identify a main subject whose communications it will intercept. It then may intercept conversations between the subject and interlocutors whose identities may not be known.²⁵ In other words, the statute prevents the interception of communications between two unknowns, not between a known subject and an unknown interlocutor.²⁶

3. Impracticality

Finally, defendants argue that it was practical to specify the locations of interceptions because Peluso had a propensity to frequent certain locations, and he and Ardito were not entirely successful in evading surveillance.

Title III does not require the government to show complete unpredictability in the movement of the subjects, that other methods of surveillance have failed or would fail, or that the subjects were successful in avoiding interception.²⁷ It was required to show only that the defendants moved often enough that the regular procedures for obtaining a warrant would inhibit the interception of some conversations needed for the investigation.²⁸

The government satisfied this burden. It determined that Ardito and Peluso met at dozens of locations and frequently were on the move because of their concern about surveillance. It stated in its application for the roving intercept that the subjects “conduct their meetings . . . in cars, at several different restaurants, on the street during ‘walks and talks’ . . . and in offices.”²⁹ Moreover, the government was conducting a wide-ranging investigation into a sprawling set of alleged conspiracies spanning more than a decade. Conversations relevant to the case potentially occurred numerous times daily. It would have been impractical for the government to predict their time and location in advance.³⁰

C. Good Faith

Finally, even if the order failed to comply with Title III’s requirements, nothing in the record suggests that the government implemented it in bad faith.

In *United States v. Leon*,³¹ the Supreme Court held that suppression is not proper where the government conducted a search in good faith reliance on a facially valid warrant.³² This good-faith exception to the exclusionary rule applies in Title III cases.³³

Conclusion

Defendants’ motions to suppress conversations intercepted pursuant to 18 U.S.C. § 2518 are denied.³⁴

Notes

1. The order prohibited interception unless “the agents and officers conducting the interception have reason to believe, through physical surveillance, source information, prior interceptions or conduct, or other facts revealed during the course of the investigation that Ardito and other SUBJECTS or other members and associates of [the family] are engaging in conversations

computer’s hard drive. Any strokes of the keys will be replicated on the eavesdropper’s computer screen. What the target says in e-mails, instant messaging, documents, and spreadsheets or anything else that comes up on screen will be revealed to the eavesdropper. Equally as disturbing, the eavesdropper can learn all of the target’s passwords, account numbers, and user names including bank accounts and credit cards used online.

One key logger software manufacturer advertises this way: “WebWatcher is the most trusted name in Activity Monitoring Software because we do what no one else can:

- ❖ Monitor in real-time from anywhere;
- ❖ Block ANY Web page based on content or Web address;
- ❖ Read instant message (IM or “Chat”) conversations;
- ❖ Read incoming and outgoing e-mail;
- ❖ Log every keystroke;
- ❖ Take screenshots;
- ❖ Record online and offline activities; and
- ❖ Quickly sift through data using unique keyword system.

You can watch over your target from anywhere. With Webwatcher’s Web-based monitor you can check your recorded data from any computer in the world.

- ❖ Watch your target’s activities in REAL-TIME.
- ❖ See what your targets are doing as they are doing it!
- ❖ Using our secure servers, your data is uploaded instantly, giving you the ability to react to situations before they become problems.
- ❖ It is completely invisible.

Designed to meet the exacting standards of intelligence agencies engaged in the war on terror, WebWatcher is completely invisible. Whether you are trying to monitor your computer savvy spouse or the head of your tech department, you won’t be detected. FlexiSpy Pro doesn’t appear in the Registry, the Process List, the System Tray, the Task Manager, on the Desktop, or in Add/Remove pro-

grams. There aren't even any visible files that can be detected!"¹⁰

Anyone who uses computers has to heed what the advertisements say and should keep in mind that the sales of spy equipment are of a magnitude sufficient to support an industry.

Wireless Connections Even More Vulnerable

Wireless computer systems are more vulnerable than the land line or phone line systems. Although weaker, a wireless computer is essentially a small broadcaster just like a commercial radio tower that broadcasts to car radios. The user's computer broadcasts to the receiver which then connects to the Internet.

The regular computer key logs will work on a wireless computer, but there is an easier way to capture every key stroke of the user. It is as simple as having another receiver in the area tuned to the same frequency. The broadcast frequency is easy to find with a frequency counter or other devices made for that purpose.

ISIS's Sk-05 Wireless Key Capture surveillance system is designed to offer an eavesdropper a covert means to record keystrokes originating from a computer

whose user is under surveillance. The information gathered can include typed documents, passwords, outgoing e-mails, Web sites, outgoing internet messaging, etc. The eavesdropper may be sitting in a car outside the building or in the café two floors below.¹¹

Conclusion

Eavesdropping is probably more common today than any time in history. The technology is sophisticated and difficult to detect without using equally sophisticated search equipment. The toys are available to law enforcement as well the public.

We used to say, "Just because you are paranoid doesn't mean that someone isn't following you." Now we can add the phrase "... or listening to every word you say and watching every word you type."

There is no room in this article to cover the multitude of micro video cameras that fit inside the button of a shirt, a tie tack, the frame of an ordinary pair of eyeglasses, a wall clock, or baseball cap. And when it comes to following people, well, that is usually done remotely by attaching a small GPS transmitter to their cars and tracking them via satellite.

United States v. Tomero, et al. (continued)

regarding the SUBJECT OFFENSES." *E.g.*, Application, Sept. 3, 2003 ¶ 8.

2. Like the one installed in Ardito's phone, the device operated whether or not the phone was in use.

3. 18 U.S.C. § 2510 *et seq.*

4. *Id.* § 2518(1)(b)(ii).

5. *Id.* § 2518(3)(d).

6. S.REP.NO. 541, 99th Cong., 2d Sess. 32, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

7. 18 U.S.C. § 2518(11).

8. *See id.* § 2518(12).

9. U.S. CONST. amend. IV.

10. 998 F.2d 1112 (2d Cir.1993).

11. *Id.* at 1124.

12. *See Bianco*, 998 F.2d at 1125.

13. *Id.* § 2518(1)(c).

14. *United States v. Bellomo*, 954 F.Supp. 630, 638-39 (S.D.N.Y.1997); *see also United States v. Torres*, 901 F.2d 205, 231 (2d Cir.1990) ("the purpose of the statutory requirements is not to preclude resort to electronic surveillance until after all other possible means of investigation have been exhausted by investigative agents; rather, they only require that the agents inform the authorizing judicial officer of the nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods.").

15. *Bellomo*, 954 F.Supp. at 639 (quoting *United States v. Ianniello*, 621 F.Supp. 1455, 1465 (S.D.N.Y.1985)).

16. *Id.* (citing *Ianniello*, 621 F.Supp. at 1465).

17. Fiorino Br. 14 (quoting *Dalia v. United States*, 441 U.S. 238, 250, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979)).

18. *See, e.g.*, Application, Sept. 3, 2003 ¶ 66(a).

19. *Id.* ¶ 66(b).

20. *Id.* ¶ 66(e).

21. *Id.* ¶ 66(g).

22. *Id.* ¶ 66(h). The defendants are incorrect to claim that the intercept order was unlawful merely because other investigative techniques had been helpful to the investigation. The government did not seek information it already had obtained through other means. Rather, it sought to "intercept conversations thought necessary to explore matters that the government had not succeeded in investigating through available means." *United States v. Scala*, 388 F.Supp.2d 396, 404 (S.D.N.Y.2005).

23. 18 U.S.C. § 2518(11)(a)(ii).

24. *United States v. Ferrara*, 771 F.Supp. 1266, 1318 (D. Mass.1991) (noting that § 2518(11)(a)(ii)'s requirement is more stringent than that of § 2518(1)(b)(iv), which requires identification of subjects, "if known").

25. *Id.* ("It is, however, permissible for the government to use a roving intercept order to capture criminal conversation between an anticipated participant who has been targeted by name in a roving order and another individual, whether or not the other person was previously known to the government.").

26. *Id.*

27. Defendants point to the language of § 2518(11)(b), which outlines procedures for roving wiretaps. That section is similar to § 2518(1)(a), but instead of requiring impracticality, requires a showing that the subject's "actions could have the effect of thwarting interception from a specified facility." 18 U.S.C. §

SENTENCING MITIGATION: WIN THE BATTLE AND THE WAR

*Successful Trial, Plea,
Sentencing, and Post
Conviction Mitigation.
Serving NACDL members
since 1981.*

*Make sure you have
what it takes to successfully
mitigate a sentence*

*A reasonable sentence
is more than the Guidelines*

- Don't give away more than you have to through a plea agreement
- Create a winning defense team
- Make the most beneficial objections to the PSR
- Develop reasonable psycho-social factors for departure
- Ask for everything you can support: creative legal and technical arguments to further your positions
- Persuasive and professional presentation
- Preservation of Appellate issues
- Appellate & 2255 representation also available

LAW OFFICE OF MARCIA G. SHEIN

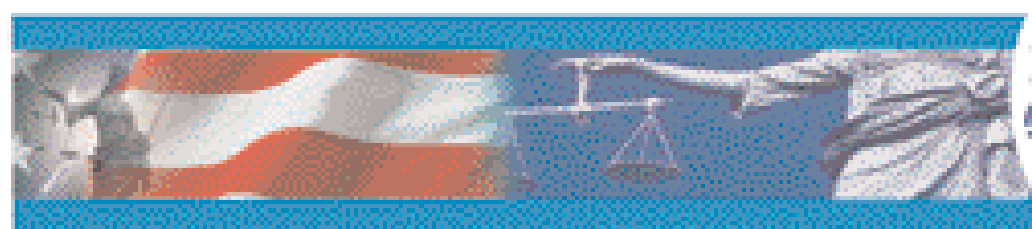
Phone: 404-633-3797 www.MsheinLaw.com Fax: 404-633-7980

Federal Criminal Law Center, 2392 North Decatur Road, Decatur, GA 30033

Success statistics and resume available on request

NOT ALL SENTENCES END IN A PERIOD

LISTEN & LEARN!



www.NACDLseminars.com

Your annual subscription gives you the entire year of NACDL Seminars — includes all sessions recorded and all the available handouts on a convenient CD-Rom, mailed to you after each quarterly meeting.

Subscribe today and receive these bonuses:

- ★ Bonus 1 - Annual Advanced Law Seminar, Aspen.
- ★ Bonus 2 - Annual DUI Seminar, Las Vegas.
- ★ Bonus 3 - Unlimited access to the entire NACDLseminars digital library. No more waiting. Download past programs, many with handouts, right from your computer. Learn from the experts. PRICELESS!

**As a Subscriber, You'll Receive
6 Complete Seminars for only \$249 a Year!**

PLUS Unlimited Downloads of Past Seminars!

Register online at www.NACDLseminars.com, or mail / fax your order to:

↓ NATIONAL MEDIA SERVICES • 613 NORTH COMMERCE AVENUE • FRONT ROYAL, VIRGINIA 22630 ↓
PHONE: (540) 635-4181 • FAX: (540) 635-4240

Name _____

Company _____

Street Address _____

City _____ State _____ Zip _____

Telephone Number _____ Ext. _____

Email _____

Payment: (Make Checks Payable to National Media Services, Inc.)

VISA/MC AMEX Check # _____ for \$ _____ Cash _____

Acct. No. _____ Exp. Date _____

Signature _____

Yes - I would like to become a NACDLseminars.com Subscriber for only \$249 a year



Notes

1. Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. § 3789d.
2. Electronic Surveillance Countermeasures, Jarvis International Academy.
3. Patricia Holt, *The Bug in the Martini Olive*, Random House Value Publishing (1993).
4. Electronic Surveillance Counter Measures, Texas A&M Extension Services.
5. FlexiSpy Products and FlexiSpy Pro are not the real names of the products being discussed. This author does not intend to advertise the products in any way.
6. WebWatcher Computer Monitoring Software, <http://www.awaresstech.com/employees/index.html?sid=30>.
7. F-Secure Trojan information pages, <http://www.f-secure.com>.
8. F-Secure Trojan information pages, <http://www.f-secure.com>.
9. Wiretapping and Electronic Surveillance, *National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance*, GPO, (1976).
10. WebWatcher Computer Monitoring Software, <http://www.awaresstech.com/employees/index.html?sid=30>.

11. ISIS's Sk-05 Wireless Key Capture surveillance system. <http://www.isis.com>. ■

About the Author

Louis L. Akin, LPI, is a writer and licensed professional investigator in Austin, Texas, with 23 years of experience in investigation. He has used his knowledge to catch illegal eavesdroppers. His forte, however, is criminal investigation and crime scene reconstruction. Akin has previously contributed articles to THE CHAMPION on blood spatter and fingerprints.



Louis L. Akin
Akin Investigations
316 W 12th Street, Suite 213
Austin, TX 78701
512-477-2546
E-MAIL ai@akininc.com
WEB SITE <http://akininc.com>

United States v. Tomero, et al. (continued)

2518(11)(b)(ii). Defendants claim that this additional requirement indicates a lower standard for obtaining a wiretap than an oral intercept. The standard, however, is not necessarily higher or lower; it simply is more specific. A roving wiretap may be obtained only on a showing of an attempt to thwart surveillance. A roving oral intercept, on the other hand, may be obtained on any showing of impracticality, which may include the subject's efforts to evade. Indeed, as the Second Circuit noted in *Bianco*, effort to evade is probative of impracticality. See *Bianco*, 998 F.2d at 1123 (quoting S.REP. NO. 54, 99th Cong., 2d Sess. 32, reprinted in 1986 U.S.C.C.A.N. 3555, 3586).

28. Defendants claim that the government "jump[ed] from interception order to interception order without meaningful and continual reassessment of necessity." Fiorino Br. 15. The Title III applications in this case, however, reveal the opposite. The government began with a traditional intercept order for Brunello Trattoria. When this proved insufficient, it sought to install listening devices in three additional restaurants. Only when this failed did it apply for the roving intercept order on Ardito and eventually Peluso. The government expanded the investigation slowly and deliberately, each time determining that its preexisting warrants were insufficient for intercepting all of Ardito's and Peluso's relevant conversations.

29. See, e.g., Application, Sept. 3, 2003 ¶ 66(h).

30. Defendants argue also that the order failed to comply with § 2518(12), which provides that no interception by a roving intercept may begin "until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." 18 U.S.C. § 2518(12). Defendants contend that this section was violated because the "[o]rders are [sic] boilerplate. It includes no such finding [of advance ascertainment]. It simply authorizes interceptions at locations 'that are impractical to specify.'" Fiorino Br. 12.

This argument is mistaken. § 2518(12) does not require the order to specify a location in advance, but requires the officer implementing the order to do so. Defendants do not argue, and the record does not indicate, that the officers implementing the order violated this provision.

31. 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

32. *Id.* at 922 ("We conclude that the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion.").


33. See, e.g., *Bellomo*, 954 F.Supp. at 638 (citing cases where courts applied the good-faith exception to Title III cases). See also *Scala*, 388 F.Supp.2d at 403.

34. Defendants assert in their brief, without explanation, that the government violated Judge Jones's intercept order and misled her about the extent of the surveillance. Fiorino Br. 2. They do not address these contentions, however, let alone provide support for them in the remainder of their brief. Nor does the record indicate that these assertions are true. Accordingly, the claims are disregarded. ■

When you need to impress someone with the truth...

POLYGRAPH

JACK TRIMARCO & ASSOCIATES
POLYGRAPH/INVESTIGATIONS, INC.



9454 Wilshire Blvd. 6th Floor
Beverly Hills, CA 90212
(310) 247-2637
email: jtrimarco@aol.com
www.jacktrimarco.com

Jack Trimarco, President
Former Polygraph Unit Chief
Los Angeles, FBI. (1990-1998)
C.A. PI. #20970

Member Society of Former Special Agents
Federal Bureau of Investigation

Former Inspector General Polygraph Program
Office of Counter Intelligence
U.S. Department of Energy