Electronic Surveillance Issues

November 2005

Stephen L. Harwood
Senior Counsel

Office of Enforcement Operations
Criminal Division
Department of Justice

Table of Contents

Legislation

Legislative History

OCCSTA

S. Rep. No. 1097, 90th Cong., 2d Sess., 1968, 1968 WL 4956 (Leg.Hist.)

ECPA

S. Rep. No. 541, 99th Cong., 2d Sess. 1986, 1986 WL 31929 (Leg.Hist.)

CALEA

S. Rep. No. 402, 103rd Cong., 2nd Sess. 1994, 1994 WL 562252 (Leg.Hist.)

H.R. Rep. No. 827(I), 103rd Cong., 2nd Sess. 1994, 1994 WL 557197 (Leg.Hist.)

Congressional Policy Role

"As new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature. Congress undertook in Title III to legislate comprehensively in this field and has shown no reluctance to revisit it." In re Askin, 47 F.3d 100 (4th Cir. 1995).

Interstate Commerce Standard

The federal wiretapping statute passes the interstate commerce standard because telecommunications are both channels and instrumentalities of interstate commerce. U.S. v. Carnes, 309 F.3d 950 (6th Cir. 2002); Spetalieri v. Kavanaugh, 36 F. Supp.2d 92, 115-16 (N.D.N.Y. 1998).

The legislative history of the Omnibus Crime Control and Safe Streets Act of 1968 pertaining to Section 2511 of Title 18 contains the following language concerning Congressional authority under the commerce clause:

> Since the facilities used to transmit wire communications form part of the interstate or foreign communications network, Congress has plenary power under the commerce clause to prohibit all interception of such communications, whether by wiretapping or otherwise. (Weiss v. United States, 60 S.Ct. 269, 308 U.S. 321 (1939)).
>
> The broad prohibition of subparagraph (a) is also applicable to the interception of oral communications. The interception of such communications, however, does not necessarily interfere with the interstate or foreign communications network, and the extent of the constitutional power of Congress to prohibit such interception is less clear than in the case of interception of wire communications. The Supreme Court has indicated that Congress has broad power to protect certain rights under the Equal Protection Clause of the 14th amendment against private interference. (United States v. Guest, 86 S.Ct. 1170, 383 U.S. 745 (1966) (concurring and dissenting opinions).) The right here at stake--the right of privacy--is a right arising under certain provisions of the Bill of Rights and the due process clause of the 14th amendment. Although the broad prohibitions of subparagraph (a) could, for example, be constitutionally applied to the

unlawful interception of oral communications by persons acting under color of State or Federal law, see Katzenbach v. Morgan, 86 S.Ct. 1717, 384 U.S. 641 (1966), the application of the paragraph to other circumstances could in some cases lead to a constitutional challenge that can be avoided by a clear statutory specification of an alternative constitutional basis for the prohibition.

Therefore, in addition to the broad prohibitions of subparagraph (a), the committee has included subparagraph (b), which relies on accepted jurisdictional bases under the commerce clause and other provisions of the Constitution to prohibit the interception of oral communications.

S. Rep. No. 1097, 90th Cong., 2d Sess. (1968) at 2180, 1968 WL 4956 (Leg.Hist.).

Justice Department Policy

Attorney General Guidelines

The Supreme Court has clearly held that a court need not exclude evidence obtained in violation of an agency's regulations or rules where neither the Constitution nor statute require adoption of any particular procedures. U.S. v. Caceres, 440 U.S. 741 (1979) (IRS consensual monitoring); U.S. v. Williamston, 1993 WL 527977 (4th Cir. December 21, 1993)(unpublished) (DEA deputations); U.S. v. Guzman, 2000 WL 276505 (U.S. Armed Forces) (consensual monitoring approval not in accord with procedures of DoD directive).

AG guidelines on criminal investigation of individuals and organizations did not create duty in favor of general public with regard to execution of investigations. Kugel v. United States, 947 F.2d 1504 (D.C. Cir. 1991).

Warrantless Access to Communications

Interception by Service Provider

Telephone company's warrantless recording, disclosure and use of the wire communications of a person suspected of using a "blue box" to evade toll charges was a reasonable exercise of the telephone company's authority under 2511(2)(a)(i) to protect its rights and property. U.S. v. Harvey, 540 F.2d 1345 (8th Cir. 1976) (citing U.S. v. Clegg, 509 F.2d 605 (5th Cir. 1975) for delineation of minimum privilege accorded telephone company under 2511(2)(a)(i)).

Under 2511(2)(a)(i), there must be some substantial nexus between the use of the telephone instrument to be monitored and the specific fraudulent activity being investigated so that the service provider can show that such monitoring is "necessary . . . to the protection of the rights or property of the provider." AT&T had right to monitor employee's communications on company-issued cellphone in furtherance of the employee's fraudulent cellphone cloning scheme where AT&T did not have the capability of intercepting the cloned instruments themselves. U.S. v. McLaren, 957 F. Supp. 215 (M.D. Fla. 1997).

Cellular One employees were not acting as government agents when, after being informed by the Secret Service that its customers were being defrauded by a clone phone operation, without the knowledge of the government exercised its right under 18 U.S.C. 2511(2)(a)(i) to conduct warrantless interceptions to detect fraudulent use of its services and located the residence from which the clone phone radio signal was being transmitted. Cellular One then provided that information to the Secret Service which then used that information to obtain a search warrant for the residence being used by the clone cell phone users. U.S. v. Pervaz, 118 F.3d 1 (1st Cir. 1997).

A jury could reasonably find that Cellular One was acting as an instrument or agent of the government when police officers conducting a kidnaping investigation, having been informed that Cellular One could conduct, under 18 U.S.C. 2511(2)(a)(i), a warrantless wiretap of a clone cellphone being used by the kidnaping suspect, asked Cellular One to relay to the police the contents of calls monitored by Cellular One. Cellular One appeared to be motivated by its desire to help the officers rather to protect its own property pursuant to the provisions of 18 U.S.C. 2511(2)(a)(i).(The intercepted message relayed to the police, that the caller wouldn't be at work that day, is irrelevant to a cloned phone investigation but very useful to a kidnaping investigation.) Officers are not entitled to qualified immunity because the wiretap statute clearly establishes the rights of someone using a telephone as against the police, and accordingly "it has been crystal clear in this circuit, at least since 1976, that in no situation may the Government direct the telephone company to intercept wire communications in order to circumvent the warrant requirements of a reasonable search." U.S. v. Auler, 539 F.2d 642 (7th Cir. 1976). "This is why the courts in Pervaz and McLaren . . . go to such lengths to determine whether the phone companies . . . were acting at the request or direction of police officers." McClelland v. McGrath, 31 F. Supp.2d 616 (N.D. Ill. 1998).

American Airlines, through their computerized reservation system, is a provider of wire or electronic communication service and American's Senior Security Representative was acting within the scope of her employment to protect the rights and property of her employer by monitoring defendant travel agents' apparent misuse of American's electronic communication service. See 18 U.S.C. 2511(2)(a)(i). Moreover, one of the parties to the communication (viz.,

American, as the security representative's employer) had consented to the monitoring. See 18 U.S.C. 2511(2)(d). U.S. v. Mullins, 992 F.2d 1472 (9th Cir. 1993).

There is no constitutional or statutory basis for suppression where, in the course of an investigation into a large fraud scheme being perpetrated against AT&T, security personnel of AT&T Wireless, without government involvement, and as authorized under 18 U.S.C. 2511(2)(a)(i), conducted warrantless interceptions and then disclosed to law enforcement officials the defendant's incriminating communications intercepted during such warrantless monitoring. U.S. v. Villanueva, 32 F. Supp.2d 635 (S.D.N.Y. 1998).

Switchboard Operator

Initial intercept by hotel operator or clerk was not "willful" (pre-ECPA mens rea), and continued eavesdropping when distress or possible crime was overheard was not intended by Congress to be unlawful. U.S. v. Savage, 564 F.2d 728 (5th Cir. 1977); Adams v. Sumner, 39 F.3d 933 (9th Cir. 1994).

Switchboard operator's exception (2511(2)(a)(i)) is limited only to that moment or so during which the operator must listen to be sure the call is placed. Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).

Access to Stored Communications by Service Provider

During the government's investigation of a kidnapping for ransom, a telecommunications service provider provided records to the government without a court order. The government's application for a nunc pro tunc 2703(d) order retroactively authorizing the disclosure of the records to the government was denied because there is no provision for the issuance of such an order, and furthermore, such an order would not provide the immunity set forth in 18 U.S.C. 2703(e) because the disclosure when made was not authorized by a court order. However, a kidnapping for ransom is the type of emergency situation which involves "immediate danger of death or serious physical injury to a person. . ." Thus, a provider who discloses records or other information pursuant to the statutory authorization in 18 U.S.C. 2702(c)(4) (added by the Patriot Act of 2001) in emergency circumstances has the same protection from lawsuits as a provider who discloses the records pursuant to a court order. The Homeland Security Act of 2002 added an authorization (18 U.S.C. 2702(b)(8)) to disclose the contents of telecommunications in the same circumstances. In the Matter of the Application of the United States for a Nunc Pro Tunc Order for Disclosure of Telecommunications Records, 352 F. Supp.2d 45 (D. Mass. 2005).

The Reno Police Department provided a computer messaging system from which contents of stored messages were retrieved that provided the basis for an internal affairs investigation of the plaintiff police officers who claimed that the storage and retrieval of their messages violated 18 U.S.C. 2510-22 and the Constitution. Title III does not apply because electronic communications in storage are not communications and therefore cannot be intercepted. The controlling statutory provisions are 2701-11 concerning access to electronic communications in storage. However, since the City is the provider of the electronic communications service, under 2701(c)(1) it and its employees are free to do as they wish when it comes to accessing communications in electronic storage. Even if the computer storage of the messages were deemed an intercept, consent would likely be implied under 2511(2)(c). A credible Fourth Amendment privacy claim is precluded by the nature and use of the messaging system (notice of message logging, banning of certain messages, limited users, routine recording by police

departments). Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996). See also U.S. v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) and Eagle Investment Systems Corporation v. Tamm, 146 F. Supp.2d 105 (D. Mass. 2001).

"Like the court in Bohach (see above), we read §2701(c) literally to except from Title II's protection all searches by communications service providers. Thus, we hold that, because Fraser's e-mail was stored on Nationwide's system (which Nationwide administered), its search of that e-mail falls within §2701(c)'s exception to Title II." Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3d Cir. 2003).

Smyth v. Pillsbury Company, 914 F. Supp. 97 (E.D. Pa. 1996) (wrongful discharge case):

> . . . we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.
>
> In the second instance, even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.

Note that 18 U.S.C. 2511(2)(a)(i) provides:

> 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.

Note also that 18 U.S.C. 2701(c) provides:

> 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;

Plaintiffs' employment by insurance company was terminated because they violated company e-mail policy by transmitting sexually explicit e-mails on the company's computers. There was no reasonable expectation of privacy in e-mail transmitted over the company's computer system (citing Smyth, see above) and there was no Title III "interception" violation because no e-mails were acquired during transmission (citing Eagle, see above). (No mention was made of 18 U.S.C. 2701(c)(1) provision permitting a service provider to authorize its own access to electronic communications stored on its system.) Garrity v. John Hancock Mutual Life Insurance Company, 2002 WL 974676 (D. Mass.).

Defendant business and it's law firm divulged contents of plaintiff's e-mail messages on defendant's e-mail system to the Wall Street Journal. Such disclosure was not a violation of 2702(a)(1) because the defendant business was not a provider of electronic communication service "to the public." Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998). See also Conner v. Tate, 130 F. Supp.2d 1370 (N.D. Ga. 2001).

Defining electronic communications service to include online merchants or service providers like Northwest [Airlines] stretches the ECPA too far. Northwest is not an internet service provider, and therefore cannot violate 18 U.S.C. 2702. Courts have concluded that "electronic communication service" encompasses internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online. In re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Minn.); Dyer v. Northwest Airlines Corporation, 334 F. Supp.2d 1196 (D. N.D. 2004); In re JetBlue Airways Corp. Privacy Litigation, 379 F. Supp.2d 299 (E.D.N.Y. 2005); Copeland v. Northwest Airlines Corporation, 2005 WL 2365255 (W.D. Tenn.).

Airline's alleged unauthorized disclosure of its passengers' personally identifiable travel information did not violate 18 U.S.C. 2701 absent an allegation that companies that accessed the information obtained it without authorization from the airline's facility. Even if airline was contractually bound by its privacy policy not to disclose such information, that obligation did not deprive it of its legal capacity under 18 U.S.C. 2702(b)(3) to consent to disclosure of its passenger information to TSA. In re American Airlines, Inc., Privacy Litigation, 370 F. Supp.2d 552 (N.D. Tex. 2005).

The Ninth Circuit interprets the 18 U.S.C. 2510(17)(B) definition of "electronic storage" to include backup storage regardless of whether it is intermediate or post-transmission:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again -- if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition. . . One district court reached a contrary conclusion, holding that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage." *See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, at 633-34, 636 (E.D. Pa. 2001).* We reject this view as contrary to the plain language of the Act. In contrast to [18 U.S.C. 2510(17)(A)], *[18 U.S.C. 2510(17)(B)]* does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser's* interpretation renders *subsection (B)* essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as "temporary, intermediate storage" within the meaning of *subsection (A).* By its plain terms, *subsection (B)* applies to backup storage regardless of whether it is intermediate or post-transmission.
>
> * * * * *
>
> We acknowledge that our interpretation of the Act differs from the government's and do not lightly conclude that the government's reading is erroneous. Nonetheless, for the reasons above, we think that prior access is irrelevant to whether the messages at issue were in electronic storage.

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

On December 10, 2003, the Third Circuit applied the 2701(c)(1) service provider exception to an insurance company that accessed employee's e-mail on the company server. The Court, however, had the following to say about the district court's holding regarding the applicability of the "backup protection" storage language of 2510(17)(B). It appears the Third Circuit would likely agree with the Ninth Circuit (see Theofel above) on the backup storage issue:

> The District Court granted summary judgment in favor of Nationwide, holding that Title II does not apply to the e-mail in question because the transmissions were neither in "temporary, intermediate storage" nor in "backup" storage. Rather, according to the District Court, the e-mail was in a state it described as "post-transmission storage." We agree that Fraser's e-mail was not in temporary, intermediate storage. But to us it seems questionable that the transmissions were not in

> backup storage - a term that neither the statute nor the legislative history defines. Therefore, while we affirm the District Court, we do so through a different analytical path, assuming without deciding that the e-mail in question was in backup storage.

Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3d Cir. 2003).

Company's access to contents of employee's company-issued computer hard drive and his communications over the Internet was lawful under 2701(c) and 2511(2)(d). Borninski v. Williamson, 2005 WL 1206872 (N.D. Tex.).

On March 22, 2004, the district court for the Central District of California, without citing the Ninth Circuit's Theofel opinion (see above), applied the Theofel view that prior access is irrelevant to whether messages are in "electronic storage" as defined in 18 U.S.C. 2510(17)(B). This application of the "backup protection" storage language of 2510(17)(B) was used to deny defendant's dismissal motion in police officers' suit against Arch Wireless for its release to police department of officers' text messages without warrant, subpoena or consent. Police officers qualified as "users" of the pager service. Contractual privity between service provider and user is not necessary under the statute to enable a claim by the user against the provider for violation of Section 2702. Quon v. Arch Wireless Operating Co, Inc., 309 F. Supp.2d (C.D. Cal. 2004).

The Air Force e-mail system carried a banner on the opening screen that said: "users logging on to this system consent to monitoring by the Hostadm." Under the provisions of 18 U.S.C. 2701(c), the Air Force, acting through its employees, was exempt from liability under 18 U.S.C. 2701 when it retrieved defendant's e-mail in the course of investigating a slowdown in the operation of the e-mail system. The Air Force was authorized by 18 U.S.C. 2702(b)(6) to divulge to law enforcement the defendant's apparently incriminating e-mail inadvertently obtained by the Air Force while conducting maintenance of its e-mail system. U.S. v. Monroe, 2000 WL 276509 (U.S. Armed Forces).

"MUD" Use by Service Provider

Ameritech used its records (message unit detail (MUD)) of an employee's telephone calls made from a calling card and from his home telephone to catch the employee violating the rules of his disability leave. The court dismissed all claims with prejudice. "One final difficulty with the 'use' claim is federal law which expressly permits telephone company employees to 'intercept, disclose or use [telephone communications] in the normal course of . . . employment while engaged in any activity which is a necessary incident to . . . the protection of the rights and property of [the telephone company].' 18 U.S.C. 2511(2)(a)(i). I do not think Illinois law would found a tort on the legally authorized conduct of defendants in the circumstances alleged here." Schmidt v. Ameritech Corporation, 1996 WL 153888 (N.D. Ill. 4/1/96).

Telephonic "Ordinary Course of Business" Exception

When an employee's supervisor has particular suspicions about confidential information being disclosed to a business competitor, has warned the employee not to disclose such information, has reason to believe that the employee is continuing to disclose the information, and knows that a particular phone call is with an agent of the competitor, it is within the ordinary course of business to listen in on an extension phone for at least so long as the call involves the type of information he fears is being disclosed. The court did not decide whether interception of a

personal call on a business extension telephone is authorized by 2510(5)(a) (see footnote 8); at what point continued monitoring would violate Title III had the conversation turned to personal matters; or whether a general practice of random monitoring of employee calls can ever be justified under 2510(5)(a) (see footnote 10 citing James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979) which held that the monitoring of employee phone calls by supervisory personnel fell within the extension telephone exception where the monitoring device had been installed by the Bell system and all affected personnel had been notified in writing about the monitoring device). Briggs v. American Air Filter Co., Inc., 630 F.2d 414 (5th Cir. 1980).

A telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business. U.S. v. Harpel, 493 F.2d 346 (10th Cir. 1974).

Consent cannot be implied from the mere fact that the Corporation's multi-line phone system permitted defendant to eavesdrop unless the privacy option was activated. See Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("knowledge of the capability of monitoring alone cannot be considered implied consent"). Sheinbrot, M.D. v. Pfeffer, M.D., 1995 WL 432608 (E.D.N.Y. 7/12/95).

Because plaintiff acted to protect her interests rather than those of the Corporation, her actions cannot be viewed as being conducted in the "ordinary course of business" of the Corporation. Sheinbrot, M.D. v. Pfeffer, M.D., 1995 WL 432608 (E.D.N.Y. 7/12/95).

"The ordinary course of business exception to Title III is a technical doctrine that lives and dies by the secretive nature of the interception." George v. Carusone, 849 F. Supp. 159 (D. Conn. 1994) (citing Harpel and Sababu); cf. Amati v. City of Woodstock, 176 F.3d 952 (7th Cir. 1999) (notion that ordinary-course defense does not extend to surreptitious taping is potentially misleading and should be avoided).

To construe the "ordinary course" provision (2510(5)(a)) as applying only where one of the parties to the intercepted conversation consented would render the exemption meaningless, since interceptions which have the consent of one of the parties to the conversation are already explicitly exempted under 2511(2)(c) and (d). Anonymous v. Anonymous, 558 F.2d 677 (2d Cir. 1997); Amati v. City of Woodstock, 176 F.3d 952 (7th Cir. 1999).

Central alarm service's covert monitoring of all incoming and outgoing telephone calls qualified under the "ordinary course of business" exemption. Arias v. Mutual Central Alarm Service, Inc., 202 F.3d 553 (2d Cir. 2000).

The evidence did not establish a business justification for the drastic measure of secret 24-hour a day, seven-day a week monitoring of a corporation's telephone lines because of a stated fear of bomb threats. Sanders v. Robert Bosch Corporation, 38 F.3d 736 (4th Cir. 1994).

If covert monitoring is to take place, it must itself be justified by a valid business purpose. Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).

A personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983). See also Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp.2d 914 (W.D. Wis. 2002)(citing Watkins); U.S. v. Devers, 2002 WL 75803 (M.D. Ala.) (citing Watkins); Rassoull v. Maximus, Inc., 2002 U.S. Dist. LEXIS 21866 (D. Md.) (citing Watkins);

Anderson v. City of Columbus, Georgia, 374 F. Supp.2d 1240 (M.D. Ga 2005)(distinguishing Watkins).

The recording of a telephone conversation during office hours, between co-employees, over a specialized extension which connected the principal office to a substation, concerning scurrilous remarks about supervisory employees in their capacities as supervisors, was a matter in which the employer had a legal interest, and therefore fell within the "telephone extension exception." Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986); Anderson v. City of Columbus, Georgia, 374 F. Supp.2d 1240 (M.D. Ga 2005)(distinguishing Epps).

Monitoring of a business or business-related call through use of a speaker phone qualifies as the use of "telephone equipment" in the "ordinary course of business" and is therefore excepted under section 2510(5)(a). T.B. Proprietary Corp. v. Sposato Builders, Inc., 1996 WL 290036 (E.D. Pa. 5/31/96)

In Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993) (followed in Sanders v. Robert Bosch Corporation, 38 F.3d 736 (4th Cir. 1994), the court did not accept a monitoring system consisting of alligator clips attached to a microphone cable at one end and an interface connecting a microphone cable to a VCR and a video camera on the other, as a "telephone or telegraph instrument, equipment or facility, or any component thereof." The court noted that this monitoring system is factually remote from the telephonic and telegraphic equipment courts have recognized as falling within the exception at 18 U.S.C. § 2510(5)(a). The court cited as examples, Epps (dispatch console installed by telephone company considered telephone equipment); Watkins (standard extension telephone implicitly considered telephone equipment); Briggs (same); and James (monitoring device installed by telephone company implicitly considered telephone equipment).

ISPs are included in Section 2510(5)(a)'s ordinary course of business exception. Hall v. Earthlink Network, Inc., 396 F.3d 500 (2d Cir. 2005).

Wife's secret, systematic recording of husband's telephonic communications by attaching automatic recorders to extension telephone lines in home next to business owned and operated by her and her husband was not activity exempted from Title III under 18 U.S.C. 2510(5)(a)(i) (use of extension telephone in ordinary course of business). The interception devices were the recording machines she attached to the telephone extensions, and the interceptions were not in the ordinary course of business. U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995), cert. denied 5/13/96.

Unrecorded eavesdropping on home extension telephone by family member concerned about the safety of her sister was not an "intercept" under Title III or Massachusetts law because such telephone extension use, in the residential context, qualifies as use within the ordinary course of business under 18 U.S.C. 2510(5)(a)(i). Commonwealth v. Vieux, 671 N.E.2d 989 (Mass. App. Ct. 1996) (comprehensive review of case law concerning residential telephone interceptions). [Affirming the federal district court's rejection of a habeas petition, the First Circuit held that the Massachusetts Appeals Court holding in Vieux was not "contrary to" or "an unreasonable application" of federal law in light of a healthy debate among a number of courts. Vieux v. Pepe, 184 F.3d 59 (1st Cir. 1999)]

A personal call may not be intercepted in the ordinary course of business under the exemption in 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. The "ordinary course of business" exemption applied here because the installation of recording equipment on extension phone was not

surreptitious, but with advance knowledge on the part of both management and its employees, and was for a legitimate business purpose. Ali v. Douglas Cable Communications, 929 F. Supp. 1362 (D. Kan. 1996) (thorough analysis of case law on 2510(5)(a)).

Telephonic "Ordinary Course" of Law Enforcement Duties Exception

Police department's cloning and monitoring of alphanumeric pager issued to police officer (pager was provided to city by telephone company) for 10-14 days to confirm or disprove suspicions that officer was disclosing confidential investigative information to drug traffickers is not covered by the "ordinary course of business" and "law enforcement" exemptions provided by 18 U.S.C. 2510(5)(a). The court did not analyze the "business use" and "law enforcement" exemptions separately. "Although we do not find that the statute requires actual consent for the exception to apply, we do hold that monitoring in the ordinary course of business requires notice to the person or persons being monitored. Because it is undisputed here that plaintiff was not given any notice that his pager was being monitored, the exceptions cannot apply." The court also stated that the business use and law enforcement exceptions both require that the equipment used be provided by a communications carrier as part of the communications network. (A careful reading of 18 U.S.C. 2510 would not yield such a requirement for the law enforcement exception under 2510(5)(a)(ii)). The dissenting opinion noted this fact and also criticized the majority's holding that notice is a requirement of the ordinary course of business exception.) Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001). See also U.S. v. Friedman, 300 F.3d 111 (2d Cir. 2002)(agreeing with Adams that notice sufficient to support a finding of implied consent under 2511(2)(c) is not required for a recording to fall within the "ordinary course" exception, and assuming arguendo that some notice is required, holding that the defendant's jailhouse notice was sufficient for the application of the "ordinary course" exception and to dispose of Fourth Amendment claims related to his taped calls).

To record all calls to and from a police department is a routine police practice. If "ordinary course" of law enforcement includes anything, it includes that. Jandak v. Village of Brookfield, 520 F. Supp. 815 (N.D. Ill. 1981); cf. U.S. v. Daniels, 902 F.2d 1238 (7th Cir. 1990); See also, Norwood v. City of Hammond, 2000 WL 158455 (E.D. La.). What would not be routine would be if the police, in order to trick people into making damaging admissions over the phone, announced that calls to and from the police department were not being recorded, and then recorded them anyway. Such a scheme would not be in the "ordinary" course of law enforcement. The boundary is between routine noninvestigative uses of electronic eavesdropping and its use either as a tool of investigation (which requires a warrant) or as a device for intimidation, suppression of criticism, blackmail, embarrassment, or other improper purposes. See U.S. v. Harpel, 493 F.2d 346, (10th Cir. 1974).

If all the lines are taped, as is the ordinary practice of police departments, then the recording of personal as well as official calls is within the ordinary course. Amati v. City of Woodstock, 176 F.3d 952 (7th Cir. 1999).

County Detention Center's telephone monitoring system (attached to a single trunk line that included the telephones that served the Judicial Corridor of the detention center) recorded the telephone conversations of judges using the offices and courtroom facilities located in a separate section of the detention facility. The County never notified the judges that their calls were being recorded until it was confirmed by the jail administrator four years later when a judge began to suspect such interception. The ordinary course of law enforcement's duties does not include recording the conversations of state judicial officers. The County's conduct therefore was not

excused by the “law enforcement exception” of 18 U.S.C. § 2510(5)(a)(ii). Abraham v. County of Greenville, South Carolina, 237 F.3d 386 (4th Cir. 2001)(citing Amati).

The government's jailhouse nonconsensual taping of a prisoner's "confession" to a priest was a violation of the Religious Freedom Restoration Act (RFRA) (held unconstitutional by Supreme Court on 6/25/97) and the Fourth Amendment. Since the taping was done in the ordinary course of duty of the law enforcement officer (jailor) (18 U.S.C. 2510(5)(a)), the mens rea required for a violation of 2511 was not present and therefore the prosecutor's retention of the intercepted confession was not a violation of 2511. This case was remanded for appropriate injunctive relief barring any future interception of confidential communications between a prisoner and a member of the clergy in the member's professional capacity. Mockaitis v. Harcleroad, 104 F.3d 1522 (9th Cir. 1997).

The law enforcement exception does not exempt from liability the recording of private or privileged conversations where neither caller consented to the recording. In re State Police Litigation, 888 F. Supp. 1235 (D. Conn. 1995).

Routine, nonsurreptitious recording of a police investigative line which results in the recording of a conversation of an officer misusing the line for private purposes, where the officer should have known that the line was monitored, was in the ordinary course of the police chief's duties as a law enforcement officer, and is exempted from the statute by Section 2510(5)(a)(ii). Jandak v. Village of Brookfield, 520 F. Supp. 815 (N.D. Ill. 1981).

It should be noted that unlike the business extension exception contained in 18 U.S.C. § 2510(5)(a)(i), which requires both that the equipment be used in the ordinary course of business and that the equipment be furnished by, or connected to the facilities of, a provider of wire or electronic services, the law enforcement exception contained in § 2510(5)(a)(ii) requires only that the equipment be used in the ordinary course of law enforcement duties. The pertinent question under the Act is whether the equipment itself is being used in the ordinary course of the law enforcement agency's duties; not whether the conversation recorded by the equipment relates to the law enforcement agency's duties. First v. Stark County Board of Commissioners, 2000 WL 1478389 (6th Cir. 10/4/00)(unpublished).

Prison authorities did not "intercept," consensually or otherwise, any communication within meaning of Title III when they routinely monitored and recorded inmate's conversation with his attorney, in case in which inmate chose not to use available unmonitored line. The communications were obtained by “law enforcement officers” who “used,” “in the ordinary course of [their] duties,” some telephone “instrument, equipment or facility, or [a] component thereof,” and therefore, under the provisions of 18 U.S.C. 2510(5)(a)(ii), the recordings were excluded entirely from the coverage of the statute. Exclusion from coverage of Title III of communications so obtained by “law enforcement officers” is not limited to use of a telephone to listen, as opposed to use of a tape recorder to record. 18 U.S.C. 2510(5)(a)(ii). Smith v. U.S. Department of Justice, 251 F.3d 1047 (D.C. Cir. 2001); U.S. v. Lewis, 406 F.3d 11 (1st Cir. 2005) (citing Smith, and footnoting to In re High Fructose, 216 F.3d 621 (7th Cir. 2000) and U.S. v. Hammond, 286 F.3d 189 (4th Cir. 2002)).

The ordinary course of the Police Department's business is law enforcement, and, in the circumstances here, the detective’s use of the extension phone to listen in on the conversation of a suspect who could not have reasonably expected privacy was not inconsistent with the ordinary course of the Police Department's business. 18 U.S.C. 2510(5)(a)(i). Kirby v. Senkowski, 141 F. Supp.2d 383 (S.D.N.Y. 2001).

Police chief's secret taping of police telephone line used for personal calls was not protected by ordinary course of business exception of 2510(5)(a)(ii). Abbott v. The Village of Winthrop Harbor, 1998 U.S. Dist. LEXIS 11897 (N.D. Ill. 7/29/98).

Workplace Searches

College's warrantless use of CCTV to monitor locker area of storage room for thefts and weapons was constitutional. There was no reasonable expectation of privacy in an unenclosed locker area located on a storage room wall within view of numerous persons who had unfettered access to the unlocked storage room. Even if there was a reasonable expectation of privacy, the warrantless video surveillance was reasonable under the Fourth Amendment because employer was investigating work-related misconduct. Citing O'Connor v. Ortega, 480 U.S. 709 (1987) (balancing test for reasonableness of searches conducted to investigate work-related misconduct; whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis) and U.S. v. Taketa, 923 F.2d 665 (9th Cir. 1991) (warrant required to conduct criminal investigation through video surveillance of office reserved for employee's exclusive use). Thompson v. Johnson County Community College, 930 F. Supp. 501 (D. Kan. 1996). See also Gross v. Taylor, 1997 WL 535872 (E.D. Pa. 8/5/97) (police officers on duty in patrol car do not have reasonable expectation of privacy or non-interception). See also U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000) (warrantless search of CIA computer network for Internet use in violation of office policy) (quoting O'Connor: "Ordinarily, a search of an employee's office by a supervisor will be justified at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct"); see also U.S. v. Slanina, 283 F.3d 670 (5th Cir. 2002)(applying O'Connor to uphold warrantless search of government employee's computer equipment for work-related misconduct even though the search might also yield evidence of criminal acts and the supervisor conducting the search is a law enforcement officer; Simons and Taketa distinguished); see also Haynes v. Office of the Attorney General, 298 F. Supp. 2d 1154 (D. Kan. 2003)(preliminary injunction issued to protect former assistant attorney general's private information on office computer).

Marine corporal whose e-mails sent and received over a Government computer network were seized with the aid of the network administrator (not pursuant to authorized system monitoring activity) acting solely at the behest of law enforcement officials, without a warrant, had a limited expectation of privacy in her e-mail communications via the Government network server. "Specifically, while the e-mails [of Marine corporal] may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a result of monitoring or when a search was conducted in accordance with the principles enunciated in the 4th Amendment. Under the circumstances presented in this case, the appellant had a subjective expectation of privacy in the e-mails sent and received on her Government computer vis-à-vis law enforcement and this expectation of privacy was reasonable." U.S. v. Long, 61 M.J. 539 (N.M.Ct.Crim.App. 2005) (citing O'Connor, Simons, Slanina (see above)).

In the present case, the frank nature of the employees' conversations makes it obvious that they had a subjective expectation of privacy. After all, no reasonable employee would harshly criticize the boss if the employee thought that the boss was listening. The essential question, therefore, is whether this expectation of privacy was objectively reasonable. We believe that the facts of this case make clear that it was. The conversations took place only when no one else was present, and stopped when the telephone was being used or anyone turned onto the gravel road that was the only entrance to the office. The record thus indicates that the employees took great care to ensure that their conversations remained private. Moreover, the office was a small,

relatively isolated space. The employees could be sure that no one was in the building without their knowledge. The Abshers rely on Kemp v. Block, 607 F. Supp. 1262 (D. Nev. 1985), a case in which the employee-plaintiffs, who worked in a single room, were found to have had no reasonable expectation of privacy. In that case, however, the single room was part of a larger office complex, meaning that others could easily overhear their conversations. In contrast, the entire office in the present case consisted of a single room that could not be accessed without the employees' knowledge. We therefore conclude that the employees had a reasonable expectation of privacy in their workplace. Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999).

Consensual Monitoring

USAM 9-7.300

18 U.S.C. 2511(2)(c) and (d)

If by virtue of sections 2511(2)(c) or (d) an interception is not prohibited by Title III, there are no Title III restrictions on its use. Section 2517(3) does not come into play and such questions as whether the section authorizes disclosure only in government proceedings and only at trial drop out; the meaning of "oral communications" also becomes moot. In re High Fructose Corn Syrup Antitrust Litigation, 216 F.3d 621 (7th Cir. 2000)(Judge Posner provides a clarifying and insightful analysis of the structure of Title III). See also U.S. v. Hammond, 286 F.3d 189 (4th Cir. 2002)(followed Seventh Circuit's reasoning in In re High Fructose and extended the rationale to the "law enforcement" exception (2510(5)(a)(ii)) as well as the "consent" exception).

With regard to the language of 18 U.S.C. 2511(2)(c) and (d), Judge Posner noted in In re High Fructose Corn Syrup Antitrust Litigation, 216 F.3d 621 (7th Cir. 2000) that:

> One might wonder why, if the statute tracks the Fourth Amendment, the statute's drafters bothered to carve an express exception for oral communications intercepted by one of the parties to the communication, given that such interceptions do not violate the Fourth Amendment. Some cases in other circuits suggest, in conformity with the statutory language, that there can be a reasonable expectation that one's conversations even if not private will not be intercepted electronically. See, e.g., Angel v. Williams, 12 F.3d 786, 790 n. 6 (8th Cir. 1993); Walker v. Darby, 911 F.2d 1573, 1578-79 (11th Cir. 1990); Boddie v. American Broadcasting Companies, Inc., 731 F.2d 333, 338-39 and n. 5 (6th Cir. 1984). None of the cases, however, involves recording one's own conversations, as in this case.

To subject interceptions made lawful by sections 2511(2)(c) and (d) to section 2517(3) would have absurd consequences. It would mean that Whitacre had violated the statute by turning his recordings over to the FBI, since on the district court's reading of that section the only permissible disclosure of the contents of an interception made lawful by sections 2511(2)(c) or (d) is to play a tape of, or testify to, those contents in court. Section 2517(3) reflects a traditional sensitivity about wiretapping and related methods of electronically eavesdropping on other people's conversations. As is implicit (and sometimes explicit) in the cases that hold that such eavesdropping violates the Fourth Amendment but that recording your own conversations does not, there just is not the same sensitivity about the latter practice. Title III does not require a warrant for such recording or regulate its use in any way. The matter has been left to the states, except for the flat prohibition of consensual recording for improper purposes. If FBI informant's recordings were made lawful by either 2511(2)(c) or (d), Title III does not restrict their use by the plaintiffs in private civil litigation. Informant would not be within the exception under 2511(2)(d) for recording for a criminal or tortious purpose, because a purpose of gathering evidence of a violation of law is not criminal or tortious. "True, his motive in making the

recordings may have been criminal or tortious (or more likely both)--to elude detection of his fraud against ADM by becoming a valued FBI informant and good-guy whistleblower. But when the law speaks of recording conversations with a criminal or tortious purpose, it has, we think, regard for the intended use of the recordings." The intent was to collect evidence of antitrust violations, not evidence that might be used for an improper purpose. "The recordings were no more unlawful than an arrest would be by a police officer who wanted to demonstrate zeal in the performance of his duties in the hope that it would shield him from prosecution for embezzling funds of the police department." In re High Fructose Corn Syrup Antitrust Litigation, 216 F.3d 621 (7th Cir. 2000).

Plaintiff's tape recording of conversation and events surrounding his arrest is, by virtue of 2511(2)(d), not prohibited by Title III and therefore there are no Title III restrictions on its use and it is admissible with respect to the federal claims against the defendant. A purpose of gathering evidence of a violation of law is not criminal or tortious. Even if the act of recording the conversation was a violation of the Illinois law, this does not constitute a criminal or tortious purpose for its use. Glinski v. City of Chicago, 2002 WL 113884 (N.D. Ill.)(citing High Fructose (see above), Sussman and Roberts (see below)).

Title III does not apply to the use of body wires because the informant who wears the wire is a party to the communication and consents to its interception. 18 U.S.C. § 2511(2)(c). Martinez v. U.S., 2001 U.S. Dist. LEXIS 2457 (S.D.N.Y.).

Consent under Title III need not be explicit; instead, it can be implied. Gilday v. Dubois, 124 F.3d 277 (1st Cir. 1997) (prisoner had to consent in writing before using monitored prison telephone system and parties were not connected unless call recipient responded appropriately to automatic recorded message advising that call would be recorded). Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993) (subject was not told of the manner in which the monitoring was conducted and that he himself would be monitored.); Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (defendant was informed that all incoming calls on a particular line would be recorded); Laughlin v. Maust, 1997 WL 436224 (N.D. Ill. 8/1/97) (restaurant manager was told that main telephone line at restaurant would be monitored); Rassoull v. Maximus, Inc., 2002 U.S. Dist. LEXIS 21866 (D. Md.) (citing Griggs-Ryan). (See PRISONER MONITORING)

Record amply supported the court's determination that woman voluntarily consented to the government's recording of her conversations with defendants. U.S. v. Cruz, 1997 WL 196035 (4th Cir. 4/23/97).

Recorded telephone call to defendant was suppressed because Government failed to prove by a preponderance of the evidence that pregnant common law wife of co-defendant voluntarily consented to police recording her telephone call with defendant. A reasonable person in the woman's position, subjected to the coercive effect of police conduct, may well have had her free will overborne and believed that she could not refuse to participate in the telephone call to the defendant. U.S. v. Moore, 96 F. Supp.2d 1154 (D. Col. 2000).

Consent can be shown where one of the parties knew that the call would be monitored. U.S. v. Davis, 799 F.2d 1490 (11th Cir. 1986); O'Ferrell v. U.S., 968 F. Supp. 1519 (M.D. Ala. 1997).

Suspect implicitly consented to the monitoring of his telephone conversations conducted on an extension telephone at the police station after a detective first dialed the number from another extension and told the person answering the phone that the suspect was on the line. In view of the circumstances, he could not have expected the calls to be private or confidential. More importantly, he believed that the detective was listening and even addressed the detective

directly, mocking him. He chose to speak to his mother and girlfriend nonetheless. Kirby v. Senkowski, 141 F. Supp.2d 383 (S.D.N.Y. 2001).

Warrantless audio and video monitoring of bribe transactions in hotel suite with the consent of a participating informant did not violate the Constitution or statutory law. The opinion includes a good review of the Supreme Court's jurisprudence in Hoffa, White and Caceres regarding consensual monitoring. The Supreme Court has not drawn any distinction between audio and video surveillance, and similarly the court in the instant case does not see any constitutionally relevant distinction between the two types of evidence. The court rejects the First Circuit's decision in U.S. v. Padilla, 520 F.2d 526 (1st Cir. 1975) (a quarter century old and not followed in any other circuit) suppressing, based on a fear of potential law enforcement abuse, consensual recordings made on a device placed in the room rather than on the person of the consenting party. The Court favorably cites the Second and Eleventh Circuit cases of U.S. v. Myers, 692 F.2d 823 (2d Cir. 1982) (surveillance of congressman's meeting with undercover agents at townhouse maintained by FBI), and U.S. v. Yonn, 702 F.2d 1341 (11th Cir. 1983) (motel room consensual monitoring; also specifically rejected Padilla reasoning). The monitoring devices in the instant case were installed at a time when the defendant had no expectation of privacy in the hotel suite. U.S. v. Lee, 359 F.3d 194 (3d Cir. 2004).

"The government met its burden to demonstrate consent when it established that [informant] knew what the government agents were about when they set up the recording equipment and provided him with a body wire." U.S. v. Bates, 2005 WL 3050278 (N.D. Ind.).

Consensual video and audio recordings in hotel room do not have to be suppressed in their entirety because they contain brief periods when the consenting party was not in the room. The record established that the technicians taping the meeting were expressly instructed to tape only while the consenting party was in the room. The technicians erred. The record established that the prosecutors learned of this error and, without reviewing the tape, arranged for the unauthorized time periods to be redacted. The unredacted version was made available to the Defendants, but nothing from the unauthorized time period was ever utilized in the prosecution. Further, the district court, after an evidentiary hearing, concluded that the Government had not acted in bad faith. U.S. v. Yang, 281 F.3d 534 (6th Cir. 2002).

District court suppressed consensual audio and video recordings because the interception devices were hidden in a hotel room obtained by the consenting informant as a temporary home for the subject woman and her minor child. The court determined that the woman had a justifiable expectation of privacy in her surroundings. Following the reasoning in U.S. v. Padilla, 520 F.2d 526 (1st Cir. 1975), the court suppressed the recordings notwithstanding the fact that the government remotely controlled the recording devices so that monitoring occurred only when the consenting informant was in the room. The court found that the informant had no right to consent to placement of recording devices in the subject's hotel room, and that the government's placement of the recording devices in the defendant's room without a warrant or judicial supervision was an intrusion so massive as to be fatal under the Fourth Amendment. The government opposed suppression, citing U.S. v. Yonn, 702 F.2d 1341 (11th Cir. 1983) (rejecting Padilla analysis), U.S. v. Laetividal-Gonzalez, 939 F.2d 1455 (11th Cir. 1991), and U.S. v. Cox, 836 F. Supp. 1189 (D. Md. 1993). U.S. v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995).

A judge in the Eastern District of New York followed the analysis in U.S. v. Yonn, 702 F.2d 1341 (11th Cir. 1983) to hold that defendants had no constitutional right to exclude recordings of conversations they had with a cooperating witness. To conduct the consensual interceptions the government activated a Title III room "bug" awaiting renewal of its Title III authorization. The cooperating witness did not know about the room "bug." The ineffectiveness of a microphone

on the body of the cooperating witness caused the government to resort to the Title III microphone to accomplish the consensual recordings. U.S. v. Yeung, 1996 WL 31235 (E.D.N.Y.).

As long as a guardian has a good faith, objectively reasonable belief that it is necessary to consent on behalf of his or her minor child to the taping of telephone conversations, the guardian may vicariously consent on behalf of the child to the recording. Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998) (child aged fourteen); Thompson v. Dulaney, 838 F. Supp. 1535 (D. Utah 1993) (children aged three and five); Wagner v. Wagner, 64 F. Supp.2d 895 (D. Minn. 1999).

Courts have repeatedly held that informants who tape-record private conversations at the direction of government investigators are "acting under color of law" within the meaning of subsection 2511(2)(c). Obron Atlantic Corporation v. Barr, 990 F.2d 861 (6th Cir. 1993) (continuous but irregular contact with DOJ attorneys following their request for assistance and their instructions on how to conduct the calls); U.S. v. Haimowitz, 725 F.2d 1561 (11th Cir. 1984) (FBI "supervised" taping); U.S. v. Shields, 675 F.2d 1152 (11th Cir. 1982) (cooperating detective controlled the recording process); U.S. v. Tousant, 619 F.2d 810 (9th Cir. 1980); U.S. v. McKneely, 69 F.3d 1067 (10th Cir. 1995) (cooperating defendant consented to audio and video surveillance of her hotel room); U.S. v. Andreas, 216 F.3d 645 (7th Cir. 2000) (CW's taping of coconspirators was very loosely supervised by FBI); U.S. v. Schulze, 2005 WL 3150267 (9th Cir.)(unpublished)(FBI supplied informant with equipment to record his conversations); U.S. v. Cowhig, 2004 WL 3088652 (D. Mass.)(that CW may have made the recordings when the FBI was not present, had ulterior motives for cooperating with the federal investigation, or exercised discretion in deciding which conversations to record neither undermines nor alters the fact that CW made the audio tapes under the direction of a federal investigation); U.S. v. Cannon, 2003 WL 21406180 (E.D. La.); U.S. v. Cox, 836 F. Supp. 1189 (D. Md. 1993) (cooperating defendant consented to audio and video surveillance of his motel room); Debose-Parent v. Hyatt, 2001 WL 709291 (E.D. La.)(applying Obron; state bar counsel was acting under color of law (2511(2)(c)) when he advised lawyer there would be no ethics violation if the lawyer, with his client's consent, recorded opposing counsel's attempted ex parte communication with the lawyer's client; the lawyer and his client were not acting under color of law because they were not acting at the behest of the state or under its direction, but the lawyer and client were protected under the consensual interception exception found in 2511(2)(d) because the plaintiff failed to allege that they recorded the conversation with the intent to commit a criminal or tortious act).

The FBI's failure to comply with its own internal guidelines, or failure to record every conversation between alleged conspirators, is not grounds for a constitutional challenge to the admissibility of evidence. U.S. v. Caceres, 440 U.S. 741 (1979); U.S. v. Feekes, 879 F.2d 1562 (7th Cir. 1989) (stating that failure to record conversations is a credibility issue to be determined by the jury). U.S. v. Andreas, 216 F.3d 645 (7th Cir. 2000). See also U.S. v. Loehr, 2003 U.S. Dist. LEXIS 24934 (N.D. Ill.)(citing Andreas).

Media employees' interception, for broadcast, of federal agent's conversation with owner of premises being searched pursuant to warrant was protected under 2511(2)(c). Berger v. Hanlon, 129 F.3d 505 (9th Cir. 1997).

An Ohio Arts Council representative tape recorded a meeting the representative held with a grant applicant to discuss his claim of racial discrimination in the denial of his application. The district court properly dismissed the applicant's civil suit alleging that the recording of his meeting violated his civil rights. Both Ohio and federal law provide exceptions for one party

consensual monitoring of communications. Paasewe v. Ohio Arts Council, 2003 U.S. App. LEXIS 17934 (6th Cir.)(unpublished).

Assistant basketball coach who recorded telephone conversation with potential recruit was protected under the "consent" provisions of 2511(2)(d). Thomas v. Pearl, 998 F.2d 447 (7th Cir. 1993).

"Because the party tape recording the meeting was present, nothing illegal occurred." 18 U.S.C. 2511(2)(d). U.S. v. McAfee, 8 F.3d 1010 (5th cir. 1993).

The person receiving a fax is a party to the communication for purposes of consent under 2511(2)(d). Before he received the fax, the recipient of the fax had already completed the fraudulent act of impersonating the plaintiff and therefore the fax transmission was not undertaken for the purpose of committing fraud. The conduct may be a violation of other statutes or common law, but it is not a violation of the ECPA. Clemons v. Waller, 2003 U.S. App. LEXIS 23547 (6th Cir.) (unpublished).

A defendant seeking to suppress a consensual tape recording bears the burden of proving by a preponderance of the evidence, either (1) that the primary motivation, or (2) that a determinative factor in the actor's motivation for intercepting the conversation was to commit a criminal, tortious, or other injurious act. U.S. v. Cassiere, 4 F.3d 1006 (1st Cir. 1993) (citing U.S. v. Vest, 639 F. Supp. 899 (D. Mass. 1986)); U.S. v. Zarnes, 33 F.3d 1454 (7th Cir. 1994) (husband did not prove that wife made tape to blackmail him); U.S. v. Farrah, 2000 WL 92349 (D. Conn.)(consensual taping by fraud victim); U.S. v. Kovolas, 1998 U.S. Dist. LEXIS 12044 (D. Mass.)(consensual taping of arsonist); CFTC v. Rosenberg, 85 F. Supp.2d 424 (D. N.J. 2000) (consensual taping by victim of broker fraud).

Magistrate judge allowed defendant to have an evidentiary hearing on suppression motion raising the issue of whether, under 2511(2)(d), consensually intercepted conversation was intercepted "for the purpose of committing any criminal or tortious act." U.S. v. Mavroules, 813 F. Supp. 115 (D. Mass. 1993).

In suit brought under Section 2520, a genuine issue of fact existed as to whether defendant ex-husband's recording of certain telephone conversations with plaintiff wife (Wayne County Circuit Judge) was done for the purpose of committing a crime (blackmail of wife) and therefore not protected under 2511(2)(d). Ferrara v. Detroit Free Press, Inc., 1998 U.S. Dist. LEXIS 8635 (E.D. Mich.). [Jury later rendered a verdict in defendant's favor]

Plaintiff sued radio station and its reporter because they taped a telephone interview with plaintiff for later radio broadcast, without plaintiff's knowledge. Defendants' summary judgment motion was granted because plaintiff did not establish that recording was made for any reason other than to gain information for the radio broadcast. Plaintiff failed to establish that the defendants taped the conversation for the purpose of committing a crime or a tort. 18 U.S.C. 2511(2)(d). Vazquez-Santos v. El Mundo Broadcasting Corporation, 283 F. Supp.2d 561 (D. P.R. 2003).

Tape recordings made by Cisneros' former mistress (Medlar) were lawful under 18 U.S.C. 2511(2)(d).(See Dale infra). The defendant failed to produce any evidence to rebut Medlar's testimony that her purposes in recording the conversations were to preserve a record of the financial agreement between herself and Cisneros and to maintain a record of his statements to her in the event she needed to correct inaccurate public accounts of their relationship. Neither of these interception purposes qualifies as criminal or tortious and therefore the consensual

recordings are not prohibited by Title III. The use of the tapes is not the critical factor for Title III purposes. Rather, it is the party's intent in making the recording that is determinative. U.S. v. Cisneros, 59 F. Supp.2d 58 (D. D.C. 1999).

Husband's recording of his telephone conversation with his wife was legal under 18 U.S.C. 2511(2)(c) or (d), and therefore the submission and use of the transcript of the conversation in Delaware Family Court was authorized under 18 U.S.C. 2517(3). Goode v. Goode, 2000 WL 291541 (D. Del.). See also Hurst v. Phillips, 2005 WL 2436712 (W.D. Tenn.).

Saving of an AOL Instant Messenger conversation on a computer by a party to the conversation was lawful under 18 U.S.C. 2511(2)(d) and therefore use of the transcript of the conversation by the defendants was lawful. S.L. v. Friends Central School, 2000 WL 352367 (E.D. Pa.).

U.S. v. Dale, 991 F.2d 819 (D.C. Cir. 1993) upheld district court's refusal to suppress tape recorded calls. District court found that section 2511(2)(d) was not violated when a recording party who was originally a willing participant in criminal scheme began taping conversations to protect his interests, and another party recorded conversations to keep a record of his employment dispute and not for purposes of extortion. The defendants did not meet their burden of proving that the tape recordings were done for criminal or tortious purposes. Taping phone calls to make an accurate record of a conversation to prevent future distortions by a participant is not illegal, see U.S. v. Underhill, 813 F.2d 105 (6th Cir. 1987), U.S. v. Miller, 1996 WL 426135 (6th Cir.); even when the recording is made in the hopes of producing evidence of an illegal conspiracy, see By-Prod. Corp. v. Armen-Berry Co., 668 F.2d 956 (7th Cir. 1982). A person may even tape confederates in the hope of obtaining evidence to reduce his own sentence. See U.S. v. Ruppel, 666 F.2d 261 (5th Cir. 1982).

The fact that the consenting party may have violated Massachusetts' law requiring consent by all parties does not by itself establish that the consenting party intercepted the conversations for the purpose of committing any criminal or tortious act in violation of the state law. U.S. v. DiFelice, 837 F. Supp. 81 (S.D.N.Y. 1993).

Federal court need not decide whether one party consensual recording (lawful under 18 U.S.C. 2511(2)(d)) of defendant's call violated California law because federal law governs the admissibility of evidence in a federal criminal trial. "Evidence admissible under federal law cannot be excluded because it would be inadmissible under state law." U.S. v. Pforzheimer, 826 F.2d 200 (2d Cir. 1987) (quoting U.S. v. Quinones, 758 F.2d 40 (1st Cir. 1985); U.S. v. Adams, 694 F.2d 200 (9th Cir. 1982). U.S. v. Morrison, 153 F.3d 34 (2d Cir. 1998); Manning v. Buchan, 357 F. Supp.2d 1036 (N.D. Ill. 2004)(Illinois statute requiring all party consent does not control admissibility in federal court, at least as to claims made under law).

On Indian reservation in the State of Washington, the federal law at 18 U.S.C. 2511(2)(d), protecting one-party consensual monitoring, cannot be overridden by assimilation, under the ACA, of the state law that requires all-party consent. U.S. v. Aripa, 1997 WL 787487 (9th Cir. 12/22/97) (unpublished).

"Thus, the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception--its intended use-was criminal or tortious. To hold otherwise would result in the imposition of liability under the federal statute for something that is not prohibited by the federal statute (i.e., recording a conversation with the consent of only one party), simply because the same act is prohibited by a state statute. Surely this is not the result intended by Congress." Payne v. Norwest Corporation, 911 F. Supp. 1299 (D. Mont.

1995). See also Sussman v. American Broadcasting Company, Inc., 186 F.3d 1200 (9th Cir. 1999); Glinski v. City of Chicago, 2002 WL 113884 (N.D. Ill.)(citing Sussman).

Plaintiff in federal sexual harassment suit had secretly recorded her oral communications with her supervisor and others. Although plaintiff's secret recordings probably violated California state law, federal courts have applied federal law on conversation recording to the exclusion of state law when the issue of tape recording impropriety has been raised in actions based on federal law. Thus, the 'tortious purpose' referenced by 2511(2)(d) must be a tortious purpose other than the mere intent to surreptitiously record an oral conversation. The Ninth Circuit has consistently held that such evidence is admissible in federal court proceedings when obtained in conformance with federal law and without regard to state law. This holding is applicable to civil as well as criminal proceedings. Roberts v. Americable Intern. Inc., 883 F. Supp. 499 (E.D. Cal. 1995); Glinski v. City of Chicago, 2002 WL 113884 (N.D. Ill.)(citing Roberts). See also U.S. v. Kovolas, 1998 U.S. Dist. LEXIS 12044 (D. Mass.) (private party taped conversation with arsonist for her own protection).

California statute criminalizing the taping of a confidential conversation and limiting the admissibility of illegally intercepted conversations, is an exception to the general rule that the Federal Rules govern the admissibility of evidence in diversity cases. The statute embodies a state substantive interest in the privacy of California citizens from exposure of their confidential conversations to third parties. The California Constitution expressly guarantees a right to privacy. Penal Code § 632 is an integral component of California's substantive state policy of protecting the privacy of its citizens, and is properly characterized as substantive law within the meaning of Erie R.R. v. Tompkins, 304 U.S. 64 (1938). Feldman v. Allstate Insurance Company, 322 F.3d 660 (9th Cir. 2003). See also Zhou v. Pittsburg State University, 252 F. Supp.2d 1194 (D. Kan. 2003)(noting Feldman diversity case but holding that in employment discrimination action based on federal question, tape recorded conversation between employee and employer's counsel was admissible, although tape was likely made in contravention of California statute).

". . . consent cannot be implied from the mere fact that the Corporation's multi-line phone system permitted defendant to eavesdrop unless the privacy option were activated. See Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("knowledge of the capability of monitoring alone cannot be considered implied consent" (emphasis in original)). Sheinbrot, M.D. v. Pfeffer, M.D., 1995 WL 432608 (E.D.N.Y. 7/12/95).

Title III prohibits monitoring cloned cellphones without a court order. Foreseeability of monitoring is insufficient to infer consent. Rather, the circumstances must indicate that a party to the communication knew that interception was likely and agreed to the monitoring. U.S. v. Staves, 383 F.3d 977 (9th Cir. 2004).

Tapes of telephone calls are admissible under the consent exception of Title III (2511(2)(d)) where defendant knew the telephone lines in the securities lending area were continuously taped and the company reserved the right to listen to those tapes, and the employee handbooks made it clear that the company had the right to review the recordings. Despite those warnings, defendant chose to continue to use those phones. U.S. v. Rittweger, 258 F. Supp.2d 345 (S.D.N.Y. 2003). See also U.S. v. Capriotti, 2004 U.S. Dist. LEXIS 5666 (N.D. Ill.)(calls recorded on corporate telephone monitoring system had a consenting party per the 2511(2)(d) exception).

Section 2511(2)(d) protects ABC's undercover consensual recordings because the recordings were not made for the purpose of committing a crime or tortious act. Desnick v. American Broadcasting Companies, Inc., 44 F.3d 1345 (7th Cir. 1995) (eye clinic examinations). See also

Deteresa v. American Broadcasting Companies, Inc., 121 F.3d 460 (9th Cir. 1997) (airline stewardess who worked O.J. Simpson's Chicago flight); Sussman v. American Broadcasting Companies, Inc., 186 F.3d 1200 (9th Cir. 1999) ("Prime Time Live" investigation of company providing psychic advice by telephone); Medical Laboratory Management Consultants v. American Broadcasting Companies, Inc., 30 F. Supp.2d 1182 (D. Az. 1998).

An Internet website was a party to communications with plaintiffs, consented to third party monitoring of such communications, and was not shown to have had a criminal or tortious purpose, and therefore is within the exemption provided by 18 U.S.C. 2511(2)(d). In re DoubleClick Inc. Privacy Litigation, 154 F. Supp.2d 497 (S.D.N.Y. 2001). See also: Chance v. Avenue A, Inc., 165 F. Supp.2d 1153 (W.D. Wash. 2001); Crowley v. Cybersource Corporation, 166 F. Supp.2d 1263 (N.D. Cal. 2001); In re Toys R US, Inc., Privacy Litigation, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal.).

Conflicting State Laws

The state law cannot preempt the federal unless the federal act itself sanctions the application of state standards. Warrantless interceptions where one party consents are specifically permitted under 18 U.S.C. 2511(2)(c) and (d). Where one party consented and no state court order or warrant was obtained, the requirement of 18 U.S.C. 2516(2) that the applicable state law must be complied with, does not come into play. It is only wiretapping by state officers under § 2516(2) which requires further authorization by state statute. State law is simply irrelevant in a federal prosecution if the investigating officers, even state officers acting alone, are not acting under the authorization of a state court. The legislative intent that federal law is to prevail in case of conflict is further indicated by 18 U.S.C. 2520, which provides that a good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under Chapter 119 "or under any other law." U.S. v. Glasco, 917 F.2d 797 (4th Cir. 1990); U.S. v. Masko, 2000 U.S. App. LEXIS 19057 (4th Cir.)(unpublished)(following Glasco); U.S. v. D'Antoni, 874 F.2d 1214 (7th Cir. 1989); U.S. v. McNulty, 729 F.2d 1243 (10th Cir. 1984) (en banc); U.S. v. Nelligan, 573 F.2d 251 (5th Cir. 1978); U.S. v. Workman, 80 F.3d 688 (2d Cir. 1996); U.S. v. Mathis, 96 F.3d 1577 (11th Cir. 1996).

Plaintiff may use one-party consensual recording to advance its federal law claim even though the recording violated Illinois state law. Century Consultants, Ltd. v. Miller Group, Inc., 2005 WL 3108455 (C.D. Ill.) (unpublished).

If in the course of assisting undercover federal operations private parties acted in good faith by reasonably relying upon the authority of government agents, state law claims against the private parties are barred by the supremacy clause. Brown v. Nationsbank Corporation, 188 F.3d 579 (5th Cir. 1999).

"Party to the Communication" under 18 U.S.C. 2511(2)(c) and (d)

A “party to the communication” under 2511(2)(d) is one who is present when the oral communication is uttered and need not directly participate in the conversation. Inside Edition producer, working undercover as a sales agent for a magazine sales company, wore a hidden camera and microphone and recorded the day to day activities of the company that he observed first hand. Pitts Sales, Inc. v. King World Productions, Inc., 383 F. Supp.2d 1354 (S.D. Fla 2005).

"The courts that have addressed the issue have held that a defendant has no reasonable expectation of privacy in statements made in the presence of a government agent, even though the agent was not participating in the conversation. See U.S. v. Coven, 662 F.2d 162 (2d Cir. 1981), cert. denied, 456 U.S. 916 (1982). The court finds that a conversation conducted in Spanish in the presence of a third person does not carry any expectation of privacy 'that society is prepared to recognize as 'reasonable," Katz v. U.S., 389 U.S. 347 (1967). Such a holding would imply that someone speaking Spanish is entitled to a greater expectation of privacy than someone who only speaks English." U.S. v. Torres, 983 F. Supp. 1346 (D. Kan. 1997).

American Airlines, as one of the parties to the communication (as the employer of the security representative who monitored defendants' apparent misuse of American's computerized reservation system) had consented to the monitoring. See 18 U.S.C. 2511(2)(d). U.S. v. Mullins, 992 F.2d 1472 (9th Cir. 1993).

DEA agent who answered two calls to a cellular telephone more than two days after the government seized it pursuant to federal forfeiture law (not for any investigatory purpose), was not a party to the communications for the purposes of consent under 2511(2)(c) and therefore the calls must be suppressed. U.S. v. Kim, 803 F. Supp. 352 (D. Hawaii 1992).

Where an accomplice who, in cooperation with police, recorded three-way conference call was known by codefendant to be listening in on his conversation with defendant, and defendant was told that the codefendant had the accomplice "on the line," the recording of the phone conversation violated neither Fourth Amendment nor federal eavesdropping law. U.S. v. Miller, 720 F.2d 227 (1st Cir. 1983). See also U.S. v. Moncivais, 401 F.3d 751 (6th Cir. 2005)(citing Miller).

In U.S. v. Foundas, 610 F.2d 298 (5th Cir. 1980), the defendant claimed that some of the conversation in the agent's hotel room was not directed at the agent and, therefore, the agent (and the hidden microphone) could not testify regarding those portions of the conversation. There was no indication in the stipulated facts or the transcript that there were sotto voce remarks or whispered asides. At any rate, the court said that if secret conversations were recorded, the burden of proof was on the party seeking to suppress the tapes. Id. at footnote 2.

"A conversation belongs equally to all participants . . . no one can have an expectation of privacy about the use of a conversation by a participant." U.S. v. Baldwin, 632 F.2d 1, 3 (6th Cir. 1980) (Jones, J., dissenting from denial of petition for rehearing).

The Supreme Court has always sanctioned a certain degree of deception or subterfuge on the part of law enforcement authorities as a necessary incident to the investigation of unlawful activities, which are, by their nature, covert and secretive. U.S. v. Passarella, 788 F.2d 377 (6th Cir. 1986) (agent answered telephone call to house where he was executing a search warrant, but did not identify himself to defendant caller) (citing Lewis v. U.S., 385 U.S. 206 (1966); On Lee v. U.S., 343 U.S. 747 (1952); U.S. v. Guidry, 534 F.2d 1220 (6th Cir. 1976)).

"The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak." Lopez v. U.S., 373 U.S. 427 (1963) (dissenting opinion).

The Fourth Amendment does not protect a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it. Hoffa v. U.S., 385 U.S. 293 (1966).

The Government's use of agents who themselves may reveal the contents of conversations with an accused does not violate the Fourth Amendment. U.S. v. White, 401 U.S. 745 (1971). In re Askin, 47 F.3d 100 (4th Cir. 1995) (endorsing unitary view of an intercepted communication).

Prisoner Monitoring

"[W]e hold that society is not prepared to recognize as legitimate any subjective expectation of privacy that a prisoner might have in his prison cell and that, accordingly, the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell." Hudson v. Palmer, 468 U.S. 517 (1984).

Prison officials are "investigative or law enforcement officers" within the meaning of the statute, and monitoring pursuant to an established and posted prison policy is in the officers' "ordinary course of duty" within the purview of 2510(5)(a)(ii). U.S. v. Lewis, 406 F.3d 11 (1st Cir. 2005) (Mass. state corrections system inmate telephone system administrator); U.S. v. Gangi, 2003 WL 190822 (10th Cir.); U.S. v. Hammond, 286 F.3d 189 (4th Cir. 2002); Smith v. U.S. Department of Justice, 251 F.3d 1047 (D.C. Cir. 2001); U.S. v. Van Poyck, 77 F.3d 285 (9th Cir. 1996); U.S. v. Sababu, 891 F.2d 1308 (7th Cir. 1989); U.S. v. Feekes, 879 F.2d 1562 (7th Cir. 1989); U.S. v. Paul, 614 F.2d 115 (6th Cir. 1980); U.S. v. Levy, 2005 WL 2179650 (E.D.N.Y.); Jennings v. U.S., 2003 U.S. Dist. LEXIS 22264 (N.D. Ill.); U.S. v. Rivera, 292 F. Supp.2d 838 (E.D. Va. 2003)(applying Hammond; recognizes the absence of circuit case law squarely addressing whether private phone contractors who provide telephone monitoring services to the prison qualify as investigative or law enforcement officers under 2510(7), but finds that the language of 2518 permitting contractors to conduct interceptions under the supervision of an investigative or law enforcement officer brings the contractually arranged provision of the means and equipment for recording (no monitoring and no discretion concerning which calls to record; all monitoring conducted by prison officials) within the law enforcement exception); U.S. v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991); U.S. v. Cheely, 814 F. Supp. 1430 (D. Alaska 1992); U.S. v. Vasta, 649 F. Supp. 974 (S.D.N.Y. 1986); See also U.S. v. Friedman, 300 F.3d 111 (2d Cir. 2002)(agreeing with Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001) that notice sufficient to support a finding of implied consent under 2511(2)(c) is not required for a recording to fall within the "ordinary course" exception, and assuming arguendo that some notice is required, holding that the defendant's jailhouse notice was sufficient for the application of the "ordinary course" exception and to dispose of Fourth Amendment claims related to his taped calls).

In Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979), the First Circuit expressly reserved decision as to whether monitoring in accordance with an established prison policy of which the prisoners were informed could qualify as part of the ordinary course of business of a law enforcement officer. "The issue in this circuit was in 1984, and still is, reasonably debatable." Langton v. Hogan, 71 F.3d 930 (1st Cir. 1995). See also U.S. v. Lanoue, 71 F.3d 966 (1st Cir. 1995).

Employees of a private corporation operating a detention facility in Rhode Island are not "investigative or law enforcement officers" for purposes of 2510(5)(a)(ii). Huguenin v. Ponte, 29 F. Supp.2d 57 (D. R.I. 1998); U.S. v. Faulkner, 323 F. Supp.2d 1111 (D. Kan. 2004)(citing Huguenin).

Prison inmates impliedly consent to the interception of their telephone calls when the inmates are fully informed of the monitoring and recording system, and notices posted above phones explicitly state that use of the institutional phones constitutes consent to monitoring. U.S. v. Footman, 215 F.3d 145 (1st Cir. 2000)(prisoners have no per se constitutional right to use a

telephone; there is little reason to believe that Congress was concerned with the privacy interests of prison inmates); U.S. v. Workman, 80 F.3d 688 (2d Cir. 1996) (prisoner's telephone calls were recorded on cassette from the start of his incarceration, and sent to law enforcement officials for use in an ongoing criminal investigation. Between March 1991 and July 1992, prison officials recorded approximately 1,000 separate conversations.); Gilday v. Dubois, 124 F.3d 277 (1st Cir. 1997) (prisoner had to consent in writing before using monitored prison telephone system and parties were not connected unless call recipient responded appropriately to automatic recorded message advising that call would be recorded). U.S. v. Van Poyck, 77 F.3d 285 (9th Cir. 1996); U.S. v. Jones, 2003 WL 463444 (9th Cir.)(unpublished) (following Van Poyck; pretrial detainees); U.S. v. Gangi, 2003 WL 190822 (10th Cir.)(following reasoning in Van Poyck); U.S. v. Willoughby, 860 F.2d 15 (2d Cir. 1988); U.S. v. Amen, 831 F.2d 373 (2d Cir. 1987); U.S. v. Hammond, 286 F.3d 189 (4th Cir. 2002); U.S. v. Apostolopuos, 2005 WL 2482525 (S.D.N.Y.); U.S. v. Sutton, 2004 U.S. Dist. LEXIS 27743 (W.D. Ky.); U.S. v. Faulkner, 323 F. Supp.2d 1111 (D. Kan. 2004); U.S. v. Rivera, 292 F. Supp.2d 838 (E.D. Va. 2003) (applying Hammond; not unreasonable for prison to compel defendant to make the choice between monitoring and no phone use; the distinction between acquiescence and consent would only be persuasive if defendant had a right to unmonitored telephone calls); U.S. v. Lombardo, 1999 U.S. Dist. LEXIS 7078 (S.D.N.Y.); U.S. v. Gotti, 42 F. Supp.2d 252 (S.D.N.Y. 1999); U.S. v. Rohlsen, 968 F. Supp. 1049 (D. V.I. 1997); U.S. v. Perez, 940 F. Supp. 540 (S.D.N.Y. 1996); U.S. v. Escobar, 842 F. Supp. 1519 (E.D.N.Y. 1994); U.S. v. Heatly, 994 F. Supp. 483 (S.D.N.Y. 1998); U.S. v. Kee, 2000 WL 760098 (S.D.N.Y.); U.S. v. Kaczowski, 114 F. Supp.2d 143 (W.D.N.Y. 2000).

In U.S. v. Horr, 963 F.2d 1124 (8th Cir. 1992), the Eighth Circuit affirmed the district court's denial of a prisoner defendant's motion to suppress tapes of monitored prison telephone calls. The district court based its decision on 2510(5)(a)(ii). The appellate court, however, based its affirmance on implied consent, 2511(2)(c), rather than 2510(5)(a)(ii).

The BOP's warrantless recording of an inmate's telephonic communications was permissible under both the "law enforcement" (2510(5)(a)(ii)) and "consent" (2511(2)(c)) exceptions to Title III, and the FBI was free to use these intercepted conversations once they were excepted under the provisions of Title III. The FBI obtained the tapes from the BOP by means of a subpoena. U.S. v. Hammond, 286 F.3d 189 (4th Cir. 2002)(included "law enforcement" exception as well as "consent" exception under the Seventh Circuit's reasoning in In re High Fructose that Title III exemption is for the entirety of Title III). See also U.S. v. Acklin, 2003 U.S. App. LEXIS 15437 (4th Cir.)(unpublished)(citing Hammond); U.S. v. Rivera, 292 F. Supp.2d 838 (E.D. Va. 2003) (citing Hammond).

The issue of what constitutes "implied consent" in the context of the prison telephone monitoring system has not yet been directly addressed by the First Circuit. It may reasonably be argued that "implied consent" in this sense is not a free and voluntary consent. Langton v. Hogan, 71 F.3d 930 (1st Cir. 1995). See also, U.S. v. Lanoue, 71 F.3d 966 (1st Cir. 1995).

Recordings focused on a particular inmate, made to gather evidence in a criminal investigation rather to advance prison security; made on separate cassettes, rather than on the reel-to-reel containing all inmate calls; conducted for more than a year; and sent to the Buffalo Police and the FBI for use in an ongoing criminal investigation was not monitoring by "a law enforcement officer in the ordinary course of his duties" under 2510(5)(a)(ii). U.S. v. Green, 842 F. Supp. 68 (W.D.N.Y. 1994) (tapes nevertheless held to be admissible under theory of implied consent; affirmed on appeal in U.S. v. Workman, 80 F.3d 688 (2d Cir. 1996)). See also U.S. v. Lanoue, 71 F.3d 966 (1st Cir. 1995).

The law enforcement exception does not exempt from liability the recording of private or privileged conversations where neither caller consented to the recording. In re State Police Litigation, 888 F. Supp. 1235 (D. Conn. 1995).

The government's jailhouse nonconsensual taping of a prisoner's "confession" to a priest was a violation of the Religious Freedom Restoration Act (RFRA) (held unconstitutional by Supreme Court on 6/25/97) and the Fourth Amendment. Since the taping was done in the ordinary course of duty of the law enforcement officer (jailor) (18 U.S.C. 2510(5)(a)), the mens rea required for a violation of 2511 was not present and therefore the prosecutor's retention of the intercepted confession was not a violation of 2511. This case was remanded for appropriate injunctive relief barring any future interception of confidential communications between a prisoner and a member of the clergy in the member's professional capacity. Mockaitis v. Harcleroad, 104 F.3d 1522 (9th Cir. 1997).

In U.S. v. Moody, 977 F.2d 1425 (11th Cir. 1992), the court denied Moody's contention that Title III monitoring of his oral communications in his prison cell violated his Fifth Amendment rights against self-incrimination and to due process.

A person seated in a police car does not have a reasonable expectation of privacy under 18 U.S.C. 2510, et seq., nor the Fourth Amendment. U.S. v. McKinnon, 985 F.2d 525 (11th Cir. 1993); U.S. v. Clark, 22 F.3d 799 (8th Cir. 1994); U.S. v. Turner, 209 F.3d 1198 (10th Cir. 2000)(whether person is in custody does not materially affect an expectation of privacy in a police car); U.S. v. Zuniga-Perez, 2003 WL 21386434 (10th Cir.)(unpublished)(applying Turner; defendants in custody and Mirandized; no interrogation); Gross v. Taylor, 1997 WL 535872 (E.D. Pa. 8/5/97) (police officers on duty in patrol car do not have reasonable expectation of privacy or non-interception); U.S. v. Fabian, 2005 WL 2043008 (D. Vt.) (citing Clark and Turner; police car unmarked but defendant was informed that he was sitting in a police vehicle).

Suspect's words spoken into mouthpiece of phone during call from police station were oral communications as recorded by police on hidden tape recorder at the police station. That the suspect believed his conversation in Thai would not be understandable to nearby police officer was of no help to the suspect because the statute [2518(2)] protects an oral communication only if there is a justifiable expectation that the communication is "not subject to interception." Police officer was standing three feet away. A television camera was suspended from the ceiling about eight feet from the telephone and pointed toward the phone. Siripongs v. Calderon, 35 F.3d 1308 (9th Cir. 1994).

Suspect implicitly consented to the monitoring of his telephone conversations conducted on an extension telephone at the police station after a detective first dialed the number from another extension and told the person answering the phone that the suspect was on the line. In view of the circumstances, he could not have expected the calls to be private or confidential. More importantly, he believed that the detective was listening and even addressed the detective directly, mocking him. He chose to speak to his mother and girlfriend nonetheless. In addition, the ordinary course of the Police Department's business is law enforcement, and, in the circumstances here, the detective's use of the extension phone to listen in on the conversation of a suspect who could not have reasonably expected privacy was not inconsistent with the ordinary course of the Police Department's business. 18 U.S.C. 2510(5)(a)(i). Kirby v. Senkowski, 141 F. Supp.2d 383 (S.D.N.Y. 2001).

Prisoner's telephonic and holding cell conversations overheard by guarding officer who was within earshot were not "oral communications" as defined in 2510(2). In any event, because the officer used no electronic or mechanical device when he overheard defendant's conversations,

there was no interception as defined in 2510(4). U.S. v. Veilleux, 846 F. Supp. 149 (D.N.H. 1994).

Police officers whose utterances were tape-recorded during their use of excessive force against a prisoner in a public jail had no objectively reasonable expectation that their communications would not be intercepted and therefore their intercepted words were not "oral communications" as defined in 18 U.S.C. 2510(2). Angel v. Williams, 12 F.3d 786 (8th Cir. 1993); See also U.S. v. Harrelson, 754 F.2d 1153 (5th Cir. 1985) (wife visiting husband in prison).

Because the marital communications privilege protects only communications made in confidence, the privilege does not apply with regard to communications between husband and wife when one of the spouses is incarcerated. U.S. v. Madoch, 149 F.3d 596 (7th Cir. 1998) (telephone calls on prison phone); See also U.S. v. Harrelson, 754 F.2d 1153 (5th Cir. 1985) (wife visiting husband in prison).

During "no-contact" visits at a private pretrial detention facility (CCA), inmates and visitors sit in different rooms, separated from each other by clear glass. Each visiting station is separated from the adjacent ones by cement block partitions. Visitors communicate with prisoners through an internal communication device that physically resembles a telephone handset. The device, however, is an entirely internal system connecting only the two visiting rooms. It is not connected to any facility capable of transmitting interstate or foreign communications. 18 U.S.C. 2510(1). Accordingly, the visitation conversations are not “wire communications” protected by the federal wiretap law. Although the inmate and his visitor at a private pretrial detention facility claim to have believed that their conversations were private and could not be overheard, any expectation of privacy was objectively unreasonable under the circumstances.

> Prison inmates necessarily have reduced privacy rights because of the nature of incarceration and the myriad of institutional needs and objectives of prison facilities. Hudson v. Palmer, 468 U.S. 517, 524, 82 L. Ed. 2d 393, 104 S. Ct. 3194 (1984); Wolff v. McDonnell, 418 U.S. 539, 555, 41 L. Ed. 2d 935, 94 S. Ct. 2963 (1974). We agree with the district court's conclusion that CCA had legitimate security reasons for monitoring the conversations and that the recordings were not made in an attempt to gather evidence about the robberies or the murder. Because CCA's practice of monitoring and recording prisoner-visitor conversations was a reasonable means of achieving the legitimate institutional goal of maintaining prison security and because those conversing in a prison setting are deemed to be aware of the necessity for and the existence of such security measures, we agree with the district court that the defendants' rights were not violated by the introduction of the recordings. . .
>
> The practice of monitoring conversations reflects CCA's efforts to ensure a high level of security in its facility, and there is no reason to believe that a visitor who converses with an incarcerated person has any more reasonable basis for his expectation that the conversation will remain private than has the inmate.

U.S. v. Peoples, 250 F.3d 630 (8th Cir. 2001).

The prosecutor does not have an obligation under Brady or the Jencks Act to retrieve, review, or disclose information (BOP telephone tape recordings) possessed by other government agencies that have no involvement in the investigation or prosecution at issue. The prosecutor need not conduct open-ended fishing expeditions of unrelated files. The defense did not make a sufficient materiality showing regarding the BOP tapes. Under the Jencks Act, the phrase “in the possession of the United States” refers to possession by the prosecutorial arm of the federal government. In this case, even if the BOP recorded communications related to the witnesses’ testimony, the BOP was not part of the prosecutorial arm of the federal government as it was not involved in either the investigation or the prosecution of the defendants. U.S. v. Merlino, 2003 WL 22664513 (3d Cir.).

Cellular Phones Seized Incident to Arrest

An arrestee has a legitimate expectation of privacy in the fact that calls were received and in the identity of callers to his cellular telephone that has been lawfully seized as evidence incident to his arrest, but government agent's answering of the arrestee's cellular telephone without a warrant in the period before arraignment--so long as the arraignment itself is not unreasonably delayed--is presumptively reasonable and does not violate the Fourth Amendment. U.S. v. De La Paz, 43 F. Supp.2d 370 (S.D.N.Y. 1999) (contains good analysis of jurisprudence regarding pager searches and telephones answered by police during execution of search warrants). But cf. U.S. v. Kim, 803 F. Supp. 352 (D. Hawaii 1992) (holding that a DEA agent who answered two calls to a cellular telephone more than two days after the phone had been seized pursuant to federal forfeiture law (not for any investigatory purpose), was not a party to the communications for the purposes of consent under 2511(2)(c) and therefore the calls and derivative evidence must be suppressed).

"Because the cell phone was seized incident to the arrest of the defendants, it is properly within the scope of an inventory search. The separate question is whether it was permissible for officers to note the numbers of incoming phone calls stored in the cell phone memory. In this case, the evidence indicated that exigent circumstances justified retrieval of the phone numbers." Subsequent incoming calls can cause the deletion or overwriting of earlier stored numbers. "This can occur whether the phone is on or off, so it is irrelevant whether the defendant or the officers turned on the phone. The Court concludes that under these circumstances, the agent had the authority to immediately search or retrieve, as a matter of exigency, the cell phone's memory of stored numbers of incoming phone calls, in order to prevent the destruction of this evidence. . . The Court further concludes that the phone numbers stored in the memory of the cell phone are not a "communication" subject to the requirements of the ECPA. . . Recorded phone numbers in a cell phone's memory are not the contents of a communication." U.S. v. Parada, 289 F. Supp.2d 1291 (D. Kan. 2003)(citing Meriwether and Reyes (see below)).

Pagers Seized Incident to Arrest

Seizure of defendant's telephone number from pager was within scope of search warrant for telephone numbers of suppliers, customers, and couriers; (2) defendant failed to show that he had a subjective expectation of privacy in a telephone number he sent blindly to whomever happened to be in possession of the pager; (3) there was no "interception" by the law enforcement agent within the meaning of The Electronic Communications Privacy Act. U.S. v. Meriwether, 917 F.2d 955 (6th Cir. 1990).

Regarding Meriwether, the following appears at footnote 20 of a January 3, 1996 Southern District of New York opinion denying suppression of "searches" of digital paging devices seized pursuant to arrest and consensual search, and suppressing a "search" of a pager seized pursuant to a defective search warrant:

> Reyes correctly points out what may be perceived as flaws in the reasoning of the Meriwether court. For one thing, the court enumerates several rationales for deciding that pressing a pager button is not an interception under the ECPA, but does not specify which rationale it adopts. The reasons the court gives include that: (i) retrieval of a number from a pager's memory is not an interception because the transmission of the number to the pager had ceased; (ii) the agent who pressed the pager button became a party to the communication, and there can be no interception when a party to a communication records that communication; and (iii) the agent did not acquire the contents of the communication by a proscribed method, that is, by electronic, mechanical or other device as proscribed by the definition of "intercept" (simply pressing the digital display button and then visually observing the telephone numbers, the court stated, did not constitute the use of an electronic,

> mechanical or other device). Meriwether, 917 F.2d at 960. With regard to the third rationale, this Court agrees with Reyes that in fact pressing a button on the pager does constitute the use of an electronic or mechanical device. However, the Court is constrained by the use of the word 'transfer' in the definition of 'electronic communication,' and is persuaded by the reasoning of the Steve Jackson court on this issue."

U.S. v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996)(footnote 20). See also U.S. v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997).

In U.S. v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993), a DEA agent seized a pager from the person of the defendant incident to arrest. The agent then activated the pager's memory, retrieving certain telephone numbers that tied the defendant to an undercover heroin sale that had just been completed by a codefendant. No heroin was found on the defendant and no warrant was obtained to seize the pager or activate the pager's memory. Judge Jensen noted that an officer's authority to possess a package is distinct from his authority to examine its contents. U.S. v. David, 756 F. Supp. 1385 (D. Nev. 1991) (exigent circumstances that justified government agent's warrantless seizure of defendant's computer memo book during interview with defendant did not also justify agent's search of book's contents; agent seized book after he observed defendant attempt to delete information and had ample opportunity to obtain search warrant following seizure.) The judge declined to apply the reasoning of U.S. v. Meriwether, 917 F.2d 955 (6th Cir. 1990) because the instant case, unlike Meriwether, deals with the privacy rights of the person in possession of the pager. "In contrast to the transmitter of a message to a pager, the possessor of the pager has control over the electronically stored information. The expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information." The court cited U.S. v. Blas, 1990 WL 265179 (E.D. Wis.) as the only federal case which addresses the privacy rights of a person in possession of a pager. In Blas, the court suppressed telephone numbers a government agent obtained from defendant's pager, ruling that the defendant's consent to "look at" the pager did not extend to the contents of the pager. The judge in Chan said that the defendant's expectation of privacy in the seized pager is analogous to that of the defendant in Blas. "While the instant case does not revolve around a consent issue, the court concurs with the reasoning in Blas and finds that Chan had a reasonable expectation of privacy in the contents of the pager's memory." The court said that although there was no danger that Chan would in any way produce a weapon from the pager, and probably no threat that he would access the pager to destroy evidence, the court is unwilling to characterize a search conducted within minutes of arrest as "remote in time and space," and therefore, U.S. v. Chadwick, 433 U.S. 1 (1977) is not controlling. Finally, the court stated that Chan's expectation of privacy was destroyed as the result of a valid search incident to an arrest; that the general requirement for a warrant prior to the search of a container does not apply when the container is seized incident to arrest, New York v. Belton, 453 U.S. 454 (1981); and therefore, the search conducted by activating the pager's memory is valid. "As the valid search of the pager incident to Chan's arrest destroyed Chan's privacy interest in the pager's contents, the Court need not address the government's arguments concerning exigent circumstances."

U.S. v. Ortiz, 84 F.3d 977 (7th Cir. 1996):

> Chan found that the retrieval of telephone numbers from a pager's memory immediately upon arrest is not so "remote" from the arrest that it falls within the exception of Chadwick . . . . We agree with this analysis . . . . Because of the finite nature of a pager's electronic memory, incoming pages may destroy currently stored telephone numbers in a pager's memory. The contents of some pagers also can be destroyed merely by turning off the power or touching a button . . . . See, e.g., United States v. Meriwether, 917 F.2d 955, 957 (6th Cir.1990). Thus, it is imperative that law enforcement officers have the authority to immediately "search" or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence. The motion to suppress was properly denied.

The warrantless search and retrieval of telephone numbers from a pager found on defendant's person at the time of his arrest was justified as incident to a valid arrest. U.S. v. Lynch, 908 F. Supp. 284 (D. V.I. 1995). See also U.S. v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996).

A police officer does not need a warrant to "search" a lawfully seized electronic pager by activating the display mechanism to reveal incoming telephone numbers that he has probable cause to believe belong to drug customers. The possibility that the numbers would be lost or become useless to investigators created exigent circumstances sufficient to justify the warrantless intrusion into what the court recognized as legitimate privacy interests surrounding the device. People v. Bullock, 277 Cal. Rptr. 63 (1990).

Police Department's use of "clone pagers" to intercept numeric transmissions to suspect's digital display pagers pursuant to state court "pen register" order cannot be considered the use of a "pen register" within the meaning of the ECPA, but was an unauthorized interception of electronic communications under 18 U.S.C. 2511. Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995). (". . . the Brown holding reinforces this Court's conclusion that for purposes of the ECPA, an "interception" must acquire data simultaneously with the transmission of the data. [A] search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication." The same exceptions to the warrant requirement apply to this section (2703(a)) as apply to any other warrantless search. U.S. v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996).) See also U.S. v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997).

Beepers

Fourth amendment not implicated. U.S. v. Knotts, 460 U.S. 276 (1983). However, warrantless monitoring of a beeper located in a private residence may violate the fourth amendment rights of persons having a reasonable expectation of privacy in the residence. U.S. v. Karo, 468 U.S. 705 (1984).

Tracking device was placed in international shipment of heroin while at Customs area field office at Dulles Airport in Northern Virginia pursuant to a warrant issued by a federal magistrate judge in the District of Columbia. Government, at oral argument, agreed that 3117 does not empower the court to authorize installation of the tracking device outside its jurisdiction. The court noted:

> In fact, the statute does not appear to authorize installation of a tracking device at all. On its face, the statute is addressed to a court already "empowered" by some other authority to issue an order for the installation of such a device. The statute merely permits such an otherwise-empowered court to authorize the use of that device both inside the jurisdiction and outside the jurisdiction if the installation is made inside. See also SEN. REP. NO. 99-541, at 33-34 (1986). Before section 3117 was enacted in 1986, courts relied on Federal Rule of Criminal Procedure 41 for the power to issue search warrants authorizing the installation and use of tracking devices. See *In re Application of the United States ("White Truck"), 155 F.R.D. 401, 402-03 (D. Mass. 1994)* (discussing historical practice); cf. *United States v. New York Tel. Co., 434 U.S. 159, 169-70, 54 L. Ed. 2d 376, 98 S. Ct. 364 (1977)* (holding Rule 41 broad enough to authorize installation and use of pen registers). At the time, however, Rule 41 only authorized warrants issued by "a federal magistrate ... within the district wherein the property or person sought is located," thus rendering uncertain a court's power to issue a warrant permitting the continued use of a mobile tracking device after it (and the container in which it had been placed) left the district. FED. R. CRIM. P. 41(a) (1986); see Clifford Fishman, Electronic Tracking Devices and The Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered, *34 CATH. U. L. REV. 277, 375 (1985).* Section 3117 resolved that uncertainty by providing the necessary authority. See *White Truck, 155 F.R.D. at 403.* In 1990, Rule 41 itself was amended to permit a magistrate to issue a search warrant not only for property within the judicial district, but also for property "either within or outside the district if the property ... is within the district when the warrant is sought but might move outside

> the district before the warrant is executed." FED. R. CRIM. P. 41(a); see also id. Advisory Committee's note on 1990 amendment (suggesting that amendment provides authority for issuance of warrant to follow beeper across state lines).

The government, however, did not require a warrant to authorize its conduct in this case because there was no privacy interest in the shipment once government officers legally opened the international shipment and identified the illegal contents. The tracking of the container on the public roads does not violate the Fourth Amendment when it reveals no information that could not have been obtained through visual surveillance. In this case the defendant was observed as he picked up the heroin shipment at a Mail Boxes Etc. in Washington, D.C. U.S. v. Gbemisola, 225 F.3d 753 (D.C. Cir. 2000).

DEA's capture of defendant's cell-site data did not violate the defendant's Fourth Amendment or Title III rights. Assuming without deciding that cell-site data fits within the definition of "electronic communication," the Court points out that suppression is not a permissible statutory remedy under Title III for the illegal interception of an electronic communication. 18 U.S.C. 2510(1)(c). (The Court finds that a strong argument exists that cell-site data is not a form of communication at all, in that it is not a message and it is not exchanged between individuals, but is just data sent from a cellular phone tower to the provider's computers.) Under the rationale of U.S. v. Knotts, 460 U.S. 276 (1983), the defendant has no legitimate expectation of privacy in the cell-site data because a person has no reasonable expectation of privacy regarding his travel on public thoroughfares, and the surveillance agents could have obtained the same information by following the defendant's car on the public highways. DEA simply used the cell-site data to "augment" sensory faculties, which is permissible under Knotts. Defendant's argument that DEA's use of the defendant's cell-site data effectively turned his cell phone into a tracking device within the meaning of 18 U.S.C. 3117, undermines the defendant's contention that suppression is appropriate under Title III. The definition of "electronic communication," 18 U.S.C. 2510(12)(C), excludes "any communication from a tracking device (as defined in section 3117 of this Title)" and thereby removes such tracking device communications from Title III coverage. Assuming, moreover, that the defendant is correct in his assertion that his phone was used as a tracking device, § 3117 does not provide a suppression remedy. See U.S. v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000), where the court observed that, in contrast to other statutes governing electronic surveillance, § 3117 "does not *prohibit* the use of a tracking device in the absence of conformity with the section.... Nor does it bar the use of evidence acquired without a section 3117 order." (Emphasis in original.) The Court finds Gbemisola to be persuasive and likewise concludes that § 3117 does not provide a basis for suppressing the cell-site data. Defendant attempted to distinguish his case from Smith v. Maryland, 442 U.S. 735 (1979) in that he did not voluntarily convey his cell-site data to anyone, and did not in fact use his cell phone. The agent dialed defendant's cell phone and the dialing caused the phone to send signals to the nearest cell tower. The Court, however, finds that the distinction between the cell-site data and the defendant's location is not legally significant under the particular facts of this case. The cell-site data is simply a proxy for the defendant's visually observable location as to which the defendant has no legitimate expectation of privacy. The Supreme Court's decision in Knotts is controlling. The DEA agents did not conduct a search within the meaning of the Fourth Amendment when they obtained the defendant's cell-site data. U.S. v. Forest, 355 F.3d 942 (6th Cir. 2004).

The Government's placement of two magnetized electronic tracking devices (gps device and Birddog beeper) on the undercarriage of defendant's vehicle parked in defendant's driveway outside the curtilage of his residence did not violate the Fourth Amendment. Assuming the officers committed a trespass by walking into the open driveway, there was no demonstration of a legitimate expectation of privacy cognizable under the Fourth Amendment in this portion of the defendant's property. "The existence of a physical trespass is only marginally relevant to the

question of whether the Fourth Amendment has been violated, however, for an actual trespass is neither necessary nor sufficient to establish a constitutional violation." U.S. v. Karo, 468 U.S. 705 (1984). No seizure occurred because the officers did not meaningfully interfere with the defendant's possessory interest in the vehicle. U.S. v. McIver, 186 F.3d 1119 (9th Cir. 1999).

Postal Inspectors' use of an electronic tracking device to monitor movement of a stolen mail pouch that defendant placed in his van did not constitute a search within the ambit of the Fourth Amendment. "We believe it would be a mistake, and a misreading of the Supreme Court's guidance in Knotts and Karo, to analyze this question solely in terms of the defendant's privacy expectation in the interior of his own van." The beeper was concealed in a mail pouch that belonged to the government and in which the defendant had no expectation of privacy whatsoever. The defendant stole the mail pouch and hid it in his van. U.S. v. Jones, 31 F.3d 1304 (4th Cir. 1994).

18 U.S.C. 3117 provides that court order may authorize use of beeper within and without the jurisdiction of the court if beeper is installed within the jurisdiction of the court.

Cordless Telephones

The radio portion of a cordless telephone communication is a protected wire or electronic communication under Title III. Pub.L. No. 103-414 (10/25/94), amending 18 U.S.C. 2510(1) & (12).

Exception for "radio portion" of cordless telephone communication applies to both sides of the conversation, because only the radio portion was intercepted. In re Askin, 47 F.3d 100 (4th Cir. 1995); McKamey v. Roach, 55 F.3d 1236 (6th Cir. 1995); See also Price v. Turner, 260 F.3d 1144 (9th Cir. 2001)(agreeing with McKamey that prior to 1994, the Wiretap Act permitted, without exception the interception of the radio portion of cordless phone communications).

Section 2520 applies to all cordless telephones regardless of their sophistication. Spetalieri v. Kavanaugh, 36 F. Supp.2d 92 (N.D.N.Y. 1998) (calls by head of police narcotics unit to cordless user intercepted by scanner); Tapley v. Collins, 41 F. Supp.2d 1366 (S.D. Ga. 1999) (police chief intercepted cordless calls on scanner).

Although defendant police officer's interception of the cordless telephone communications of plaintiff during a drug investigation in 2000 violated federal law (cordless telephone exemption removed from Title III in 1994), the good faith defense in 18 U.S.C. 2520(d) excuses the defendant from liability because he relied in good faith on a Tennessee court order issued in accordance with state law, and he received verification of its propriety from a local assistant district attorney. Because the law regarding Fourth Amendment applicability to cordless telephone communications is not "clearly established" (neither the Supreme Court nor the Sixth Circuit has specifically addressed the issue), and because he was acting pursuant to a court order under state law, and with the endorsement of an assistant district attorney, the defendant has qualified immunity from liability if there was a Fourth Amendment violation. Frierson v. Goetz, 2004 U.S. App. LEXIS 10037 (6th Cir.) (unpublished).

A cordless telephone communication between two men conspiring to commit murder was reported to the police by a neighbor who illegally intercepted the cordless communication. The conspirators were convicted in state court. One pleaded guilty and testified against the other. The one who stood trial was unsuccessful in his attempt to exclude all testimony by his coconspirator as derivative of the illegal interception. The Ninth Circuit affirmed the district court's denial of

the defendant's habeas petition. "Assuming that the interception of the cordless telephone conversation between Rogers and Lord violated Title III and that Rogers' testimony at trial was sufficiently connected to the illegal interception to constitute a "fruit of the poisonous tree" (issues we do not decide in this case), Lord's Title III claim is not cognizable under the standards for federal habeas review, because the claim does not involve an "error of the character or magnitude" to justify habeas relief. Lord v. Lambert, 347 F.3d 1091 (9th Cir. 2003).

Illegal interception of the radio portion of a cordless telephone communication is penalized under the same scheme as that applied to the illegal interception of the radio portion of a cellular telephone communication. The offense is considered to be an "infraction" (subject to a fine of not more than $5000; 18 U.S.C. 3559(a)(9) and 3571(b)(7)) if it is a first offense not for a tortious or illegal purpose, not for commercial advantage or private commercial gain, and the intercepted radio communication was not encrypted, scrambled 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. 18 U.S.C. 2511(4)(b).

Thermal Imaging

In a case involving the government's warrantless use of infra red imaging to detect unusual amounts of heat emitted from a house believed to contain a marijuana growing operation, the Supreme Court protected traditional Fourth Amendment notions of privacy in the home from encroachment by the government's warrantless use of high tech surveillance devices. The ruling is limited to private homes and to surveillance devices "not in general public use," so there will be opportunities for the Court to generate additional permutations to the complex field of Fourth Amendment jurisprudence. Held: "Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant." Kyllo v. U.S., 533 U.S. 27 (2001) (Scalia writing for the majority, joined by Thomas, Breyer, Ginsburg and Souter).

Seizures by Rule 41 Warrant

"Sneak and Peek" Warrant

Warrant providing for notice within seven days satisfies constitutional standards. U.S. v. Freitas, 800 F.2d 1451 (9th Cir. 1986)(house-methamphetamine operation)(Freitas I). The constitutional infirmity did not emanate from the surreptitious nature of the entry, or even from the fact that the warrant failed to provide for contemporaneous notice. Rather, it was based on a distinction between post-search notice and no notice. U.S. v. Freitas, 856 F.2d 1425 (9th Cir. 1988) (Freitas II).

Warrants should require seven-day notice absent a strong showing of necessity. U.S. v. Johns, 948 F.2d 599 (9th Cir. 1991)(storage locker-methamphetamine precursors).

Covert entry searches for intangibles are permissible if police officers have made showing of reasonable necessity for dispensing with advance or contemporaneous notice of search and if officers give appropriate person notice of search within reasonable time after covert entry; as an initial matter, the issuing court should not authorize a notice delay of longer than seven days. Each extension of the notice delay period should be based on a fresh showing of need for further delay. (Two month delay in seven-day increments.) U.S. v. Villegas, 899 F.2d 1324 (2d Cir. 1990)(farm-cocaine lab); U.S. v. Ludwig, 902 F. Supp. 121 (W.D. Tex. 1995)(storage locker-cocaine)(reasonable necessity shown for notice delay).

A sneak and peek warrant to examine defendant's incoming and outgoing mail at the MCC was granted pursuant to Villegas and related cases, and the delay notice was limited to the maximum period of seven days specified in Villegas. The government mistakenly failed to request an extension of the original order when it applied eight times (before eight different magistrate judges) to obtain additional seven day delays of notice. The lack of authorization to continue the search cannot have operated to the defendant's prejudice because each application for delay of notice contained enough evidence to have justified continued authorization. This case is a good candidate for not applying the exclusionary rule because the government appears to have believed that it was complying with the requirements of the Fourth Amendment, and did comply with the important requirement of presenting evidence of probable cause to a neutral magistrate. "Mistakes were made, as the morally anemic like to say; but that is all they were -- mistakes. The evidence should not be suppressed merely because, in Judge Cardozo's craftily quaint phrase, 'the constable has blundered.'" To remedy excessive copying of the defendant's mail, the court required the government to forward to the court for sealing all correspondence copied other than those letters proffered to the magistrate judges, and to keep no additional copies of any such correspondence. U.S. v. Heatley, 41 F. Supp.2d 284 (S.D.N.Y. 1999).

The good faith exception to the exclusionary rule applies to sneak and peek search warrants. U.S. v. Ludwig, 902 F. Supp. 121 (W.D. Tex. 1995).

U.S. v. Pangburn, 983 F.2d 449 (2d Cir. 1993)(storage locker-methamphetamine precursors) held: "We prefer to root our notice requirement in the provisions of Rule 41 rather than in the somewhat amorphous Fourth Amendment 'interests' concept developed by the Freitas I court. The Fourth Amendment does not deal with notice of any kind, but Rule 41 does. It is from the Rule's requirements for service of a copy of the warrant and for provision of an inventory that we derive the requirement of notice in cases where a search warrant authorizes covert entry to

search and to seize intangibles." This Rule 41 violation should not call forth the application of the exclusionary rule because there was no prejudice to the defendant and the executing officers did not intentionally disregard the notice requirement.

During the execution of a "sneak and peek warrant" at a storage locker, the officers briefly removed weapons from a duffel bag found within the locker, tested them for operability and took them out to the street and photographed them. This behavior did not constitute a "seizure" in violation of 18 U.S.C. 3103a(b)(2) or the sneak and peek warrant's prohibition of the seizure of any tangible property. There was no "meaningful interference with" the defendant's "possessory interests" in the weapons. Even if the complained of activity constituted a "seizure" in violation of the warrant, the evidence need not be suppressed under the "independent source doctrine." A conventional search warrant was obtained later the same day. Once the weapons were found during the initial sneak and peek, the second warrant was inevitable and would have occurred whether or not the weapons were removed to the street and tested and photographed. U.S. v. Mikos, 2003 WL 22462560 (N.D. Ill.)(storage locker-evidence relevant to health fraud and murder).

Video Surveillance

USAM 9-7.200

Seven circuits, recognizing that video surveillance does not fall within the letter of Title III, have applied certain of the higher constitutional standards of Title III (e.g., necessity and minimization) to video surveillance warrants. U.S. v. Williams, 124 F.3d 411 (3d Cir. 1997); U.S. v. Falls, 34 F.3d 674 (8th Cir. 1994); U.S. v. Koyomejian, 970 F.2d 536 (9th Cir. 1992) (en banc); U.S. v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987) (quoting George Orwell's 1984) (in defendant's home); U.S. v. Biasucci, 786 F.2d 504 (2d Cir. 1986) (in business office); U.S. v. Torres, 751 F.2d 875 (7th Cir. 1984) (in terrorist safe houses); U.S. v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990) (in warehouse).

Title III has no application to video surveillance. U.S. v. Westberry, 2000 U.S. App. LEXIS 15064 (6th Cir.) (unpublished) (citing Torres).

The Fourth Amendment protects citizens from secret video surveillance in another person's hotel room without a warrant or the consent of a participant in the monitored activity. The Ninth Circuit affirmed the lower court's suppression of that part of the government's hidden video surveillance of motel room drug activities that occurred after consenting informants left the room. The severity of the governmental intrusion is important in determining the legitimacy of a citizen's expectation of privacy in a particular place. The court declined to apply Minnesota v. Carter, 525 U.S. 83 (1998) because the intrusion there was merely a police officer's visual observation through a ground floor apartment window. In support of its position that the nature of the intrusion may affect the legitimacy of an expectation of privacy, the court cites various cases before and after Carter, including the Supreme Court's recent opinion in Bond v. U.S., 529 U.S. 334 (2000) wherein the Court held that an agent's warrantless manipulation of a bus passenger's bag in an overhead compartment violated the Fourth Amendment, because the defendant had a reasonable expectation that he would not be subjected to such a severe intrusion (tactile observation) into his privacy. U.S. v. Nerber, 222 F.3d 597 (9th Cir. 2000).

Consensual audio/video recordings conducted only during the consenting informant's presence in a hotel room rented by the informant were admissible because the audio recordings were within the 18 U.S.C. 2511(2)(c) exception for consensual monitoring and the consensual video

monitoring did not offend the Constitution. Applying Nerber (see above) to the video recordings, the Court did not decide (because if error it was harmless) the issue left open in dicta in a footnote in Nerber as to whether the defendant would have an objectively reasonable expectation of privacy where the informant consented to the video recording, but the hotel room was rented by the defendant). U.S. v. Shryock, 342 F.3d 948 (9th Cir. 2003).

Warrantless audio and video monitoring of bribe transactions in hotel suite with the consent of a participating informant did not violate the Constitution or statutory law. The opinion includes a good review of the Supreme Court's jurisprudence in Hoffa, White and Caceres regarding consensual monitoring. The Supreme Court has not drawn any distinction between audio and video surveillance, and similarly the court in the instant case does not see any constitutionally relevant distinction between the two types of evidence. The court rejects the First Circuit's decision in U.S. v. Padilla, 520 F.2d 526 (1st Cir. 1975) (a quarter century old and not followed in any other circuit) suppressing, based on a fear of potential law enforcement abuse, consensual recordings made on a device placed in the room rather than on the person of the consenting party. The Court favorably cites the Second and Eleventh Circuit cases of U.S. v. Myers, 692 F.2d 823 (2d Cir. 1982) (surveillance of congressman's meeting with undercover agents at townhouse maintained by FBI), and U.S. v. Yonn, 702 F.2d 1341 (11th Cir. 1983) (motel room consensual monitoring; also specifically rejected Padilla reasoning). The monitoring devices in the instant case were installed at a time when the defendant had no expectation of privacy in the hotel suite. U.S. v. Lee, 359 F.3d 194 (3d Cir. 2004).

Hotel room audio and video consensual surveillance did not violate defendant's constitutional or statutory rights. U.S. v. Corona-Chavez, 2003 U.S. App. LEXIS 9350 (8th Cir.)(Nerber distinguished).

The U.S. Forest Service's use of an unattended, motion-activated video camera to record activity near a marijuana patch located in a wooded section in a remote area of Clay, County, Kentucky did not violate the Fourth Amendment rights of the defendant who was videotaped cultivating marijuana plants on the land. The Forest Service officers were unaware of who owned the land and the defendant admitted he was not the owner. Under the open fields doctrine the defendant lacked an objectively reasonable expectation of privacy in the open field where he cultivated his marijuana plants. U.S. v. Westberry, 2000 U.S. App. LEXIS 15064 (6th Cir.)(unpublished).

Consensual video surveillance is not violative of the Fourth Amendment. U.S. v. Cox, 836 F. Supp. 1189 (D. Md. 1993) (cooperating defendant consented to video and audio monitoring of motel room, was in the room at all times, and the surveillance did not pick up any words or actions that were outside the consenting party's hearing and sight) (citing U.S. v. Myers, 692 F.2d 823 (2d Cir. 1982) (video surveillance of congressman's meeting with undercover agents); U.S. v. Echeverri, 1992 WL 302907 (E.D.N.Y.); U.S. v. Napolitano, 552 F. Supp. 465 (S.D.N.Y. 1982)).

Consensual video and audio recordings in hotel room do not have to be suppressed in their entirety because they contain brief periods when the consenting party was not in the room. The record established that the technicians taping the meeting were expressly instructed to tape only while the consenting party was in the room. The technicians erred. The record established that the prosecutors learned of this error and, without reviewing the tape, arranged for the unauthorized time periods to be redacted. The unredacted version was made available to the Defendants, but nothing from the unauthorized time period was ever utilized in the prosecution. Further, the district court, after an evidentiary hearing, concluded that the Government had not acted in bad faith. U.S. v. Yang, 281 F.3d 534 (6th Cir. 2002).

College's warrantless use of CCTV to monitor locker area of storage room for thefts and weapons was constitutional. There was no reasonable expectation of privacy in an unenclosed locker area located on a storage room wall within view of numerous persons who had unfettered access to the unlocked storage room. Even if there was a reasonable expectation of privacy, the warrantless video surveillance was reasonable under the Fourth Amendment because employer was investigating work-related misconduct. Thompson v. Johnson County Community College, 930 F. Supp. 501 (D. Kan. 1996) (Citing O'Connor v. Ortega, 480 U.S. 709 (1987) (balancing test for reasonableness of searches conducted to investigate work-related misconduct; whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis) and U.S. v. Taketa, 923 F.2d 665 (9th Cir. 1991) (warrant required to conduct criminal investigation through video surveillance of office reserved for employee's exclusive use)). See also Gross v. Taylor, 1997 WL 535872 (E.D. Pa. 8/5/97) (police officers on duty in patrol car do not have reasonable expectation of privacy or non-interception). See also U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000)(warrantless search of CIA computer network for Internet use in violation of office policy) (quoting O'Connor: "Ordinarily, a search of an employee's office by a supervisor will be justified at its inception when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."); U.S. v. Slanina, 283 F.3d 670 (5th Cir. 2002)(applying O'Connor to uphold warrantless search of government employee's computer equipment for work-related misconduct even though the search might also yield evidence of criminal acts and the supervisor conducting the search is a law enforcement officer; Simons and Taketa distinguished).

(Pole Cameras)

FBI installed video cameras (could be adjusted from police station and zoom in to read a license plate) on the tops of telephone poles overlooking the residences of two defendants. The pole cameras were incapable of viewing inside the houses. No warrant was necessary for installation and use of the pole cameras because they only observed what any passerby would easily have been able to observe. Defendant resident of house had no reasonable expectation of privacy that was intruded upon by the video cameras. Agents also used a "video car" equipped with three hidden cameras, two VCRs and a transmitter to record and listen to conversations in and around the car with the consent of an informant who was a party to those communications. 18 U.S.C. 2511(2)(c). U.S. v. Jackson, 213 F.3d 1269 (10th Cir. 2000).

"[I]t is beyond dispute that the government, even in the investigation stage, may request court approval for third party assistance in installing surveillance measures like the pole camera." U.S. v. Bullock, 1999 WL 81526 (E.D. Pa.) and U.S. v. Turner, 1999 WL 88937 (E.D. Pa.) (Bullock and Turner are co-defendants; both cases cite U.S. v. New York Telephone Co., 434 U.S. 159 (1977) (district court had authority under the All Writs Act (28 U.S.C. 1651) to direct utility to assist federal law enforcement officials in setting up pen register, with reimbursement at prevailing rates, to investigate offenses which there was probable cause to believe were being committed by means of telephone. Power conferred by All Writs Act extends, under appropriate circumstances, to persons who though not parties to original action or engaged in wrongdoing are in a position to frustrate implementation of court order or proper administration of justice and encompasses even those who have not taken any affirmative action to hinder justice)).

Search Warrant Access to Computers, Disks, and Cassettes

U.S. v. Ross, 456 U.S. 798 (1982) (lawful search not limited by the possibility that separate acts of entry or opening may be required to complete the search); U.S. v. Crouch, 648 F.2d 932 (4th Cir. 1981) (removal of documents from an envelope); U.S. v. Gray, 814 F.2d 49 (1st Cir. 1987)

(from the breast pocket of a nylon jacket); U.S. v. Gentry, 642 F.2d 385 (10th Cir. 1981) (from a locked briefcase found on the premises); U.S. v. Gomez Soto, 723 F.2d 649 (9th Cir. 1984) (from a locked briefcase and a micro cassette found on the premises). In each case the court rejected the defendant's contention that a second warrant was required before police could open the container in which the documents were found.

Government's use of "Key Logger System" (KLS) on defendant's computer to capture encryption passphrase did not record keystrokes when the modem was operating. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated. CIPA requirements were met and the government's proposed unclassified summary of the specific classified data concerning the KLS technique is sufficient for purposes of litigating the suppression motion. U.S. v. Scarfo, 180 F. Supp.2d 572 (D. N.J. 2001).

The transmission of keystrokes from a keyboard to a computer's processing unit is not the transmission of an electronic signal by a system that "affects interstate or foreign commerce," and therefore does not constitute an "electronic communication" as defined in 18 U.S.C. 2510(12). The "system" involved in this case is the local computer hardware and one or more software programs, and either an e-mail or other communications program to compose messages. Although the system is connected to a larger system--the network–which affects interstate or foreign commerce, the transmission in issue did not involve that system. Therefore, defendant's installation of a Keykatcher device on the cable between the keyboard and the CPU of an insurance company employee's desktop computer is not a violation under 18 U.S.C. 2511. U.S. v. Ropp, 347 F. Supp.2d 831 (C.D. Cal. 2004) (citing U.S. v. Scarfo, 180 F. Supp.2d 572 (D. N.J. 2001)).

Computer searches are not per se overbroad. During search of computers and records from law office, seizure of items outside the warrant was inevitable, but not unconstitutional. If computer and related hardware must be removed from search scene to perform particularized search for records, copies should be made and the computer equipment returned as soon as possible. There is no justification for favoring those who are capable of storing their records on computers over those who keep hard copies of their records. U.S. v. Hunter, 13 F. Supp.2d 574 (D. Vt. 1998) (citing Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F.Supp. 432, 437 (W.D. Tex. 1993) and U.S. v. Abbell, 963 F. Supp. 1178 (S.D. Fla. 1997)). See also U.S. v. Lloyd, 1998 WL 846822 (E.D.N.Y.).

Because of the technical difficulties of conducting a computer search in a suspect's home (on-line obscenity bulletin board system), the seizure of the computers, including their content, for off-site examination, was reasonable to allow police to locate the offending files. Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

In U.S. v. Lucas, 932 F.2d 1210 (8th Cir. 1991), police seized an answering machine and its tape while executing a warrant that provided for the search and seizure of books, records and other papers relating to the distribution of controlled substances. The court found that the language in the warrant providing for the seizure of 'records' supported the seizure of the answering machine and its tape. The court rejected defendant's contention that the government needed a second search warrant to listen to the tape.

Warrant to search for and seize "any records or documents associated with cocaine distribution" justified police listening to three unmarked audio cassettes and then seizing the tapes after determining that they related to the investigation. U.S. v. Peters, 92 F.3d 768 (8th Cir. 1996).

Unpublished decisions in which courts have concluded that police may seize information from computer disks without obtaining a second warrant: U.S. v. Sprewell, 1991 WL 113647 (9th Cir. Cal.) (search warrant authorized search for any tally sheets or pay and owe sheets tending to establish narcotics transactions. Personal computer, programs and disks taken to police headquarters where a computer specialist helped find files in the computer's electronic memory that purportedly contained evidence of narcotics sales.); U.S. v. Sissler, 1991 WL 239000 (W.D. Mich.) (warrant authorized seizure of records of drug transactions. Police seized hundreds of computer disks and a personal computer. Citing Ross, the court held that the police were permitted to examine the computer's internal memory and the disks.)

Computer hardware was seized as an instrumentality of the crime of obscenity distribution over a computer bulletin board service. Warrant was not overbroad under the Fourth Amendment. Concomitant and incidental seizure of e-mail and software stored therein did not invalidate the hardware seizure. The fact that a given object may be used for multiple purposes, one licit and one illicit, does not invalidate the seizure of the object when supported by probable cause and a valid warrant. This is not approval of any subsequent efforts by the police to search or retain the stored files without a warrant (police did not access the stored files). Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997).

Police officer's search of computer files he had probable cause to believe contained child pornography exceeded scope of warrant to search computer for drug related documents. "His seizure of the evidence upon which the charge of conviction was based was a consequence of an unconstitutional general search, and the district court erred by refusing to suppress it. Having reached that conclusion, however, we are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result." U.S. v. Carey, 172 F.3d 1268 (10th Cir. 1999) (contains analysis of several other computer search cases).

(Scope of Consent)

The First Circuit affirmed suppression of child pornography seized from suspect's computer during a consent search. The consent to search was given in the context of a police search for evidence of the presence of an assault suspect who had attacked a woman in the next door apartment. The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of "objective" reasonableness--what would the typical reasonable person have understood by the exchange between the officer and the suspect? Florida v. Jimeno, 500 U.S. 248 (1991). U.S. v. Turner, 169 F.3d 84 (1st Cir. 1999).

Applicability of Title III

"Oral Communication"

18 U.S.C. 2510(2)

Burglars and others not legitimately on the premises do not have a reasonable expectation of privacy as to their conversations while so situated. Rakas v. Illinois, 439 U.S. 128 (1979); U.S. v. Pui Kan Lam, 483 F.2d 1202 (2d Cir. 1973).

Government's placement of an electronic surveillance microphone at an outdoor grave site memorial service, which intercepted plaintiffs' communications, did not violate constitutional or statutory rights. Plaintiffs failed to demonstrate that they possessed a reasonable expectation of privacy regarding their oral communications at the grave site memorial service. Plaintiffs provided no evidence of the context and circumstances of the conversations or of any steps taken to maintain their privacy. Court did not reach the question whether individuals such as the plaintiffs could have an objectively reasonable expectation of privacy at a grave site burial service under different facts or whether the individual defendants would have qualified immunity in such a situation. Further, because the court's holding rests on the plaintiffs' failure to demonstrate their subjective expectation of privacy, it did not reach the question whether, in other circumstances, officers would be required to obtain judicial approval for the intercept. Kee v. City of Rowlett, 247 F.3d 206 (5th Cir. 2001); Cressman v. Ellis, 2003 U.S. App. LEXIS 20807 (5th Cir.)(unpublished)(citing Kee and its mention of the many factors that affect a finding of a subjective expectation of privacy).

The overhear of conversations through the common walls and doors of hotel rooms by agents' unaided ears violates neither the Fourth Amendment nor Title III. See U.S. v. Hessling, 845 F.2d 617 (6th Cir. 1988); U.S. v. Mankani, 738 F.2d 538 (2d Cir. 1984); U.S. v. Agapito, 620 F.2d 324 (2d Cir. 1980); U.S. v. Burnett, 493 F. Supp. 948 (N.D.N.Y. 1980).

A federal district judge in Boston held that in the light of Minnesota v. Carter, 525 U.S. 83 (1998), the utterances of a defendant during his participation in an LCN making ceremony at another person's house are not protected by the Fourth Amendment. The defendant did not have an expectation of privacy that society would today deem to be justified because he was not an overnight guest and engaged only in business discussions (making ceremony). In addition, the court finds that when Title III was enacted it was intended that evolving, contemporary conceptions of reasonable expectations of privacy be applied in deciding whether an intercepted conversation constitutes an "oral communication" as defined in 2510(2). In view of the decision in Carter, the court is compelled to find that the defendant did not at the making ceremony in the house have a justified expectation that he would not be intercepted and, therefore, did not engage in what the statute defines as an "oral communication." Thus, the defendant is not an "aggrieved person" as defined in § 2510(11). Accordingly, he does not have standing, under § 2518(10)(a), to seek suppression for an alleged violation of Title III concerning the electronic surveillance conducted at the house where the making ceremony was held. Therefore, his motion to suppress must be denied. U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999).

Government's warrantless use of hidden video cameras to observe defendants in hotel room after consenting informants left the room is a privacy intrusion sufficiently serious to support a finding that the defendants had a reasonable expectation of privacy under the Fourth Amendment

that their activities while alone in a hotel room would not be subject to surveillance by hidden cameras. Minnesota v. Carter, 525 U.S. 83 (1998) is distinguishable because the privacy intrusion in Carter was a police officer looking through a ground floor apartment window. The nature of the intrusion may affect the legitimacy of an expectation of privacy, as the Supreme Court recently opined in Bond v. U.S., 529 U.S. 334 (2000), wherein the Court held that an agent's warrantless manipulation of a bus passenger's bag in an overhead compartment violates the Fourth Amendment because the passenger has a reasonable expectation that he will not be subjected to such a severe intrusion (tactile observation) into his privacy. U.S. v. Nerber, 222 F.3d 597 (9th Cir. 2000).

Hotel room audio and video consensual surveillance did not violate defendant's constitutional or statutory rights. U.S. v. Corona-Chavez, 2003 U.S. App. LEXIS 9350 (8th Cir.)(Nerber distinguished).

U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999):

> It might also be reasoned that Title III recognizes that there are circumstances in which a person knows that he is being overheard, but justifiably expects that he will not be recorded, because 18 U.S.C. §§ 2511(2)(c) and (2)(d), which authorize the consensual recording of conversations in certain circumstances, would otherwise be superfluous with regard to oral communications because when Title III was enacted the Supreme Court had held that an individual did not for Fourth Amendment purposes have a legitimate expectation that someone to whom he was speaking in person would not record his statements. See United States v. White, 401 U.S. 745 (1971); Hoffa v. United States, 385 U.S. 293 (1966). See also In re High Fructose Corn Syrup Antitrust Litig., 46 F. Supp. 2d at 825-26. As has been noted in rejecting this reasoning, however, §§ 2511(2)(c) and (2)(d) also apply to "wire and electronic types of communication, which, at least in the case of wire communications, are protected against interception regardless of the speaker's reasonable expectation of privacy." In re High Fructose Corn Syrup Antitrust Litig., 46 F. Supp. 2d at 827. Absent § 2511(2)(c) and (2)(d), consensual monitoring of telephone conversations would not be permitted. It appears to this court that although redundant in view of the definition of "oral communication" in § 2510(2), oral communications were included in §§ 2511(2)(c) and (2)(d) to make clear that the statute authorized consensual monitoring of person to person discussions as well as telephone conversations. The failure to include oral communications in those provisions could have given the mistaken impression that consensual monitoring of such discussions was not permitted.

Regarding the use of the term "oral communication" in the language of 18 U.S.C. 2511(2)(c) and (d), Judge Posner noted in In re High Fructose Corn Syrup Antitrust Litigation, 216 F.3d 621 (7th Cir. 2000) that:

> One might wonder why, if the statute tracks the Fourth Amendment, the statute's drafters bothered to carve an express exception for oral communications intercepted by one of the parties to the communication, given that such interceptions do not violate the Fourth Amendment. Some cases in other circuits suggest, in conformity with the statutory language, that there can be a reasonable expectation that one's conversations even if not private will not be intercepted electronically. See, e.g., Angel v. Williams, 12 F.3d 786, 790 n. 6 (8th Cir. 1993); Walker v. Darby, 911 F.2d 1573, 1578-79 (11th Cir. 1990); Boddie v. American Broadcasting Companies, Inc., 731 F.2d 333, 338-39 and n. 5 (6th Cir. 1984). None of the cases, however, involves recording one's own conversations, as in this case.

Prisoner's telephonic and holding cell conversations overheard by guarding officer who was within earshot were not "oral communications" as defined in 2510(2). In any event, because the officer used no electronic or mechanical device when he overheard defendant's conversations, there was no interception as defined in 2510(4). U.S. v. Veilleux, 846 F. Supp. 149 (D.N.H. 1994).

Suspect's words spoken into mouthpiece of phone during call from police station were oral communications as recorded by police on hidden tape recorder at the police station. That the suspect believed his conversation in Thai would not be understandable to nearby police officer was of no help to the suspect because the statute [2510(2)] protects an oral communication only if there is a justifiable expectation that the communication is "not subject to interception." Police officer was standing three feet away. A television camera was suspended from the ceiling about eight feet from the telephone and pointed toward the phone. Siripongs v. Calderon, 35 F.3d 1308 (9th Cir. 1994); See also U.S. v. Longoria, 117 F.3d 1179 (10th Cir. 1999) (defendant who conversed in Spanish in presence of informant who the defendant knew did not understand Spanish did not have a reasonable expectation that his conversation would not be subject to interception).

A person's utterance is "subject to interception" if it is "readily or practicably capable of being intercepted." That is, if a person should know that the person's comments could be artificially detected without too much trouble, or that the means of artificial detection might actually be in place, the person's expectation of noninterception is not reasonable. Wesley v. WISN Division-Hearst Corporation, 806 F. Supp. 812 (E.D. Wis. 1992) (comments made near a radio station microphone). Gross v. Taylor, 1997 WL 535872 (E.D. Pa. 8-5-97) (police officers on duty in patrol car had no reasonable expectation of privacy or non-interception).

Police officers unsuccessfully sought suppression of non-consensual tape-recording of their use of excessive force against a prisoner in a public jail. There was no objectively reasonable expectation that their conversations would not be intercepted, and therefore there was no statutory "oral communication" [18 U.S.C. 2510(2)]. Angel v. Williams, 12 F.3d 786 (8th Cir. 1993); See also U.S. v. Harrelson, 754 F.2d 1153 (5th Cir. 1985) (wife visiting husband in prison).

The conversations of an inmate and his visitor were recorded by a private pretrial detention facility (CCA). Although the prisoner and his visitor claim to have believed that their conversations were private and could not be overheard, any expectation of privacy was objectively unreasonable under the circumstances and therefore their conversations were not protected as “oral communications” as defined in 18 U.S.C. 2510(2).

> Prison inmates necessarily have reduced privacy rights because of the nature of incarceration and the myriad of institutional needs and objectives of prison facilities. Hudson v. Palmer, 468 U.S. 517, 524, 82 L. Ed. 2d 393, 104 S. Ct. 3194 (1984); Wolff v. McDonnell, 418 U.S. 539, 555, 41 L. Ed. 2d 935, 94 S. Ct. 2963 (1974). We agree with the district court's conclusion that CCA had legitimate security reasons for monitoring the conversations and that the recordings were not made in an attempt to gather evidence about the robberies or the murder. Because CCA's practice of monitoring and recording prisoner-visitor conversations was a reasonable means of achieving the legitimate institutional goal of maintaining prison security and because those conversing in a prison setting are deemed to be aware of the necessity for and the existence of such security measures, we agree with the district court that the defendants' rights were not violated by the introduction of the recordings. . .
>
> The practice of monitoring conversations reflects CCA's efforts to ensure a high level of security in its facility, and there is no reason to believe that a visitor who converses with an incarcerated person has any more reasonable basis for his expectation that the conversation will remain private than has the inmate.

U.S. v. Peoples, 250 F.3d 630 (8th Cir. 2001).

The frank nature of the employees' conversations make it obvious that they had a subjective expectation of privacy because no reasonable employee would harshly criticize the boss if the employee thought that the boss was listening. The essential question is whether this expectation of privacy was objectively reasonable. The court finds that the facts of this case make clear that

it was. The conversations took place only when no one else was present, and stopped when the telephone was being used or anyone turned onto the gravel road that was the only entrance to the office. The record indicates that the employees took great care to ensure that their conversations remained private. Moreover, the office was a small, relatively isolated space. The employees could be sure that no one was in the building without their knowledge. The defendants rely on Kemp v. Block, 607 F. Supp. 1262 (D. Nev. 1985), a case in which the employee-plaintiffs, who worked in a single room, were found to have had no reasonable expectation of privacy. In that case, however, the single room was part of a larger office complex, meaning that others could easily overhear their conversations. In contrast, the entire office in the present case consisted of a single room that could not be accessed without the employees' knowledge. The court therefore concludes that the employees had a reasonable expectation of privacy in their workplace. Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999).

"Wire Communication"

Private networks and intra-company communications systems are within the protection of the statute. S. Rep. No. 541, p. 12.

"[T]he phrase 'in whole or in part . . . by the aid of wire . . .' is intended to refer to wire that carries the communication to a significant extent from the point of origin to the point of reception, even in the same building. It does not refer to wire that is found inside the terminal equipment at either end of the communication." S. Rep. No. 541, p. 12.

As of 10/25/94, the radio portion of a cordless telephone communication is a protected wire communication or electronic communication under Title III. 18 U.S.C. 2510(1) & (12)

As of 10/25/94, illegal interception of the radio portion of a cordless telephone communication is penalized under the same scheme as that applied to the illegal interception of the radio portion of a cellular telephone communication. The offense is considered to be an "infraction" (subject to a fine of not more than $5000; 18 U.S.C. 3559(a)(9) and 3571(b)(7)) if it is a first offense not for a tortious or illegal purpose, not for commercial advantage or private commercial gain, and the intercepted radio communication was not encrypted, scrambled 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. 18 U.S.C. 2511(4)(b).

During "no-contact" visits at a private pretrial detention facility, inmates and visitors sit in different rooms, separated from each other by clear glass. Each visiting station is separated from the adjacent ones by cement block partitions. Visitors communicate with prisoners through an internal communication device that physically resembles a telephone handset. The device, however, is an entirely internal system connecting only the two visiting rooms. It is not connected to any facility capable of transmitting interstate or foreign communications. 18 U.S.C. 2510(1). Accordingly, the visitation conversations are not “wire communications” protected by the federal wiretap law. U.S. v. Peoples, 250 F.3d 630 (8th Cir. 2001).

Government Access to Voice Mail and Answering Machine Messages

The USA Patriot Act (10/26/01) amended the 18 U.S.C. 2510(1) definition of “wire communication” by deleting “electronic storage” of same and adding “wire communications” to the stored communications provisions of 18 U.S.C. 2703. This change permits law enforcement to obtain stored wire communications (voice mail) as well as stored electronic communications

(e-mail) using the procedures set out in 2703 (such as a search warrant). Answering machine messages are seizable by search warrant, but are not communications "in electronic storage," as that term is defined in 18 U.S.C. 2510(17), and therefore are not covered by the stored communications law.

"Electronic Communication"

Definition: 18 U.S.C. 2510(12)

Interception order: 18 U.S.C. 2516(3)

The Ninth Circuit interprets the 18 U.S.C. 2510(17)(B) definition of "electronic storage" to include backup storage regardless of whether it is intermediate or post-transmission:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again -- if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition. . . One district court reached a contrary conclusion, holding that "backup protection" includes only temporary backup storage pending delivery, and not any form of "post-transmission storage." *See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, at 633-34, 636 (E.D. Pa. 2001).* We reject this view as contrary to the plain language of the Act. In contrast to [18 U.S.C. 2510(17)(A)], *[18 U.S.C. 2510(17)(B)]* does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser's* interpretation renders *subsection (B)* essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as "temporary, intermediate storage" within the meaning of *subsection (A).* By its plain terms, *subsection (B)* applies to backup storage regardless of whether it is intermediate or post-transmission.
>
> * * * * *
>
> We acknowledge that our interpretation of the Act differs from the government's and do not lightly conclude that the government's reading is erroneous. Nonetheless, for the reasons above, we think that prior access is irrelevant to whether the messages at issue were in electronic storage.

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

"We therefore conclude that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act." Defendant bookseller acted as an e-mail service provider to his customers and copied all their incoming e-mails from Amazon.com. At all times that the defendant's software programs performed these operations, the e-mail messages were in "temporary electronic storage" in random access memory or on hard disks, or both. U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc).

"By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of 'intercept'--acquisition contemporaneous with transmission-with respect to wire communications. . .The purpose of the recent amendment was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications. *See* H.R. Rep. 107-236(I), at 158-59 (2001). When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term 'intercept' with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable

to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (applying Konop); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994); Eagle Investment Systems Corporation v. Tamm, 146 F. Supp.2d 105 (D. Mass. 2001). See also Thompson v. Thompson, 2002 WL 1072342 (D. N.H.) (unpublished) (citing Steve Jackson Games and Eagle Investment and dismissing suit alleging "interception" through downloading of post-transmission e-mail and other files stored on plaintiff's computer). See also U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003)(citing Konop and Steve Jackson Games) and Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3d Cir. 2003)) (adopting the reasoning of Steiger, Konop, and Steve Jackson Games).

The transmission of keystrokes from a keyboard to a computer's processing unit is not the transmission of an electronic signal by a system that "affects interstate or foreign commerce," and therefore does not constitute an "electronic communication" as defined in 18 U.S.C. 2510(12). The "system" involved in this case is the local computer hardware and one or more software programs, and either an e-mail or other communications program to compose messages. Although the system is connected to a larger system--the network–which affects interstate or foreign commerce, the transmission in issue did not involve that system. Therefore, defendant's installation of a Keykatcher device on the cable between the keyboard and the CPU of an insurance company employee's desktop computer cannot be indicted as an attempt to intercept electronic communications in violation of 18 U.S.C. 2511. U.S. v. Ropp, 347 F. Supp.2d 831 (C.D. Cal. 2004) (citing U.S. v. Scarfo, 180 F. Supp.2d 572 (D. N.J. 2001)).

Electronic Communications "Readily Accessible to the General Public"

18 U.S.C. 2511(2)(g); 2510(16)

Plaintiff claimed that Defendant intercepted the Plaintiff's taxi cab radio messages and appropriated them for the Defendant's own use in violation of § 605 of the Federal Communications Act. To the extent that 18 U.S.C. § 2511(2)(g)(ii)(II) is silent as to the "use" of intercepted radio messages, thereby not authorizing the "use" of the same, the FCC's interpretation of § 605 of the Federal Communications Act, as it applies to the Plaintiff's claim, is based upon a permissible construction of the interplay between the Wiretap Act and the Communications Act, and the FCC's determination (use of intercepted messages prohibited by § 605) should be given deference. "Because we cannot locate, nor has Defendant proffered, any other section of the Wiretap Act which would authorize the use of these types of radio messages, § 605 (a)'s prohibition against using these intercepted messages for one's own benefit is applicable here." Cafarelli v. Yancy, 226 F.3d 492 (6th Cir. 2000).

(trunked radios)

Look at U.S. v. Gass, 936 F. Supp. 810 (N.D. Okl. 1996) and E.F. Johnson Co. v. Uniden, 623 F. Supp. 1485 (D. Minn. 1985) for possible insight into the lawfulness of intercepting trunked radio communications. Neither case provides an interpretation of the phrase "readily accessible to the general public," but Gass clearly recognizes the exceptions in 18 U.S.C. 2511(2)(g), and Uniden provides a description of the nature of trunked radio systems. OEO had some discussions with the Southern District of California in February/March 1997 regarding trunked radios and opined, based upon the submitted factual situation, that no Title III order was required to intercept the trunked radio communications described.

"Intercept"

The ECPA defines "intercept" as "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." 18 U.S.C. 2510(4).

"We therefore conclude that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act." Defendant bookseller acted as an e-mail service provider to his customers and copied all their incoming e-mails from Amazon.com. At all times that the defendant's software programs performed these operations, the e-mail messages were in "temporary electronic storage" in random access memory or on hard disks, or both. U.S. v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc).

"By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of 'intercept'--acquisition contemporaneous with transmission-with respect to wire communications. . .The purpose of the recent amendment was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications. *See* H.R. Rep. 107-236(I), at 158-59 (2001). When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term 'intercept' with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). See also U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003)(citing Konop); Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3d Cir. 2003)(adopting the reasoning of Steiger, Konop, and Steve Jackson Games).

The law is established that the taping of a telephone conversation is an "interception." However, courts have found that the act of listening to a taped conversation is not, in and of itself, an "interception." See U.S. v. Turk, 526 F.2d 654 (5th Cir. 1976) ("The argument that a new and different 'aural acquisition' occurs each time a recording of an oral communication is replayed is unpersuasive."); Reynolds v. Spears, 93 F.3d 428 (8th Cir. 1996); Amati v. The City of Woodstock, 829 F. Supp. 998 (N.D. Ill. 1993) ("Whether the communication is heard by the human ear is irrelevant" to determination of whether communication was intercepted); cf. U.S. v. Nelson, 837 F.2d 1519 (11th Cir. 1988) ("Term 'intercept' as it relates to 'aural acquisition' refers to the place where a communication is initially obtained regardless of where the communication is ultimately heard"). "This interpretation of §2510(4) is persuasive."

In 1992, the Second Circuit held that an interception must be deemed to have occurred "when the contents of wire communications are captured or redirected in any way." U.S. v. Rodriguez, 968 F.2d 130 (2d Cir. 1992) (holding both location where conversation was redirected and where it was overheard sufficed as situs of "interception" for jurisdictional purposes). Rodriguez followed in U.S. v. Denman, 100 F.3d 399 (5th Cir. 1996); U.S. v. Giampa, 904 F. Supp. 235 (D. N.J. 1995).

Due to a defect in the design of a telephone line voice recorder, when the recorder was deactivated, the handset microphone continued to pick up ambient noise and transmit it to a security control room. Officials were unaware of the defect until it was brought to their attention by a security supervisor, and there was no evidence that any employee ever listened to, recorded, or otherwise acquired any conversations through the open microphone. Therefore, the "contents" of the conversations were never "acquired." Sanders v. Robert Bosch Corporation, 38 F.3d 736

(4th Cir. 1994). See also Directv, Inc. v. Pluskhat, 2004 U.S. Dist. LEXIS 2231 (W.D. Mich.) (citing Sanders).

To the extent that there is some conflict over the proper interpretation of the term "interception," we note that clarification of the language and definitions of Title III may merit congressional attention. Arias v. Mutual Central Alarm Service, Inc., 202 F.3d 553 (2d Cir. 2000).

The Fifth Circuit, in U.S. v. Turk, 526 F.2d 654 (5th Cir. 1976), concluded that no new and distinct "interception" occurs when the contents of a communication are revealed through the replaying of a previous recording, and that the definition of "intercept" requires, at minimum, some involvement in the initial use of a "device" contemporaneous with the communication being intercepted. Accord Steve Jackson Games, Incorporated v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994); Forsyth v. Barr, 19 F.3d 1527 (5th Cir. 1994); Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997); U.S. v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997); U.S. v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996); Eagle Investment Systems Corporation v. Tamm, 146 F. Supp.2d 105 (D. Mass. 2001). The Turk court believes that an interpretation that "would exclude from the definition of 'intercept' the replaying of a previously recorded conversation has a firm basis in the language of 2510(4) and in logic, and corresponds closely to the policies reflected in the legislative history." The court rejected the argument that a different "aural acquisition" occurs each time a recording of an oral communication is replayed. Furthermore, the court concluded that the inclusion of sanctions under 18 U.S.C. 2511(1)(c) concerning disclosure of illegally intercepted communications means that such derivative "aural acquisitions" are not "interceptions," otherwise such sanctions would be redundant with the sanctions provided in 18 U.S.C. 2511(a) and (b) pertaining to interception.

U.S. v. Daccarett, 6 F.3d 37 (2d Cir. 1993), held (3-0) that no "interception" occurred because the government did not use any type of "device" to obtain EFTs and information from intermediary banks through oral orders and arrest warrants in rem. The court pointed out that because the ECPA defines "intercept" as "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," 18 U.S.C. 2510(4), "liability under the ECPA is therefore predicated on the use of a 'device.' See United States v. Turk, 526 F.2d 654, 658 (5th Cir.) (act requires 'contemporaneous acquisition of the communication through the use of the device'), cert. denied, 429 U.S. 823 (1976)."

When party to conversation wore a tape recorder as well as a radio transmitter, each communication was intercepted twice. One "aural acquisition" occurred when the agents heard the conversation being transmitted by radio. The other involved the tape recording and occurred at the time the recording was made, not when persons listened to the tape. U.S. v. Shields, 675 F.2d 1152 (11th Cir. 1982) (citing Turk).

Turk's interpretation of the term "intercept" was applied in the Southern District of Ohio in January, 1991 when it held that officers did not "intercept" any wire, oral or electronic communication when they replayed and transcribed the contents of tapes they seized from a telephone answering machine during the execution of a search warrant. U.S. v. Upton, 763 F. Supp. 232 (S.D. Ohio 1991).

On May 16, 1995, a judge in the District of Connecticut followed Turk, Shields, Nelson, and Rodriguez in holding: "If Congress had intended the phrase 'aural or other acquisition' to mean 'overheard,' it certainly could have employed the simpler term. The section's [2510(4)] additional requirement that a conversation be acquired 'through the use of any electronic,

mechanical, or other device' suggests that it is the act of diverting, and not the act of listening, that constitutes an 'interception.'" In re State Police Litigation, 888 F. Supp. 1235 (D. Conn. 1995).

U.S. v. Cheely, 814 F. Supp. 1430 (D. Alaska 1992) contains the following discussion:

There is substantial authority supporting the proposition that if monitoring is lawful, recording of the monitored conversations is lawful. U.S. v. Miller, 720 F.2d 227, 228 (1st Cir. 1983) (Title III only proscribes unlawful interceptions defined as listening to or monitoring of telephone conversations, not the recording of monitored conversations, hence if monitoring is lawful, recording is always lawful); see U.S. v. Harpel, 493 F.2d 346, 350 (10th Cir. 1974); cf. U.S. v. Suarez, 906 F.2d 977, 982 (4th Cir. 1990) (Title III clearly distinguishes between interception defined as oral monitoring and recording), U.S. v. White, 401 U.S. 745 (1971) (if conversation is legally overheard, then recording standing alone cannot violate the Fourth Amendment), Lopez v. U.S., 373 U.S. 427 (1963) (to same effect). These cases turn on the definition of intercept, which means to listen to someone's conversation through the use of a mechanical device. Recording devices do not accomplish the interception, they merely record a conversation that has already been intercepted. Consequently, if the initial interception, i.e., monitoring, is legal, subsequent recording is also legal. Katz v. U.S., 389 U.S. 347 (1967), does not contradict this conclusion. In Katz, the Supreme Court invalidated a recording on Fourth Amendment grounds, but only because the circumstances established that the police would not have lawfully overheard the conversations they recorded. Id. at 363 (White, J., concurring). Thus a recording of a telephone conversation could be an interception under 2510(4), but only if the conversation could not be heard by the human ear listening to the same telephone. See In the Matter of John Doe Trader No. One, 722 F. Supp. 419, 421-23 (N.D. Ill. 1989).

The First Circuit held that Pharmatrak, Inc., a firm providing data collection software to various pharmaceutical internet sites, "intercepted," without the consent of its pharmaceutical client web sites, personal and identifying data of the pharmaceutical sites' web users. (This holding appears to be based on a misunderstanding of the technology of web browsers that caused the court to believe that Pharmatrak was wiretapping communications between web users and the pharmaceutical sites. In fact, the information collected by Pharmatrak was sent by the users' own browsers directly to Pharmatrak. The users' browsers were simply operating per the standard for HTTP code. When the users clicked on a link in the pharmaceutical webpage they communicated simultaneously with the pharmaceutical sites and with Pharmatrak and then both the pharmaceutical client's server and Pharmatrak's server contributed content for the succeeding webpage. The pharmaceutical sites had configured their systems so as to expose the users' data in the URLs of the sites' dynamically generated pages.) The case was remanded to determine if Pharmatrak's actions were "intentional" within the meaning of the ECPA. In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).

"Electronic, Mechanical or Other Device"

Detective's overhearing a telephone conversation by listening on the same earpiece being used by a participating party did not violate Title III. When only two telephones are used, one to place the call and one to receive the call, the call has not been intercepted within the definition of Section 2510. U.S. v. Chiavola, 744 F.2d 1271 (7th Cir. 1984).

Dispatch console, not recording equipment, was the intercepting device within purview of 2510(4) & (5). Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986). See also U.S. v. Devers, 2002 WL 75803 (M.D. Ala.) (citing Epps).

When recording made by connecting telephone receiver to tape recorder, telephone receiver is the intercepting mechanism, not the recorder. U.S. v. Harpel, 493 F.2d 346 (10th Cir. 1974); Ali v. Douglas Cable Communications, 929 F. Supp. 1362 (D. Kan. 1996); U.S. v. Devers, 2002 WL 75803 (M.D. Ala.) (citing Harpel).

Speaker phone is "telephone equipment" within exception language of section 2510(5)(a). T.B. Proprietary Corp. v. Sposato Builders, Inc., 1996 WL 290036 (E.D. Pa. 5/31/96).

The recording device, not the extension phone, was the instrument used to intercept the calls and does not fall within the statutory exemption. U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995), cert. denied 5/13/96; Sanders v. Robert Bosch Corporation, 38 F.3d 736 (4th Cir. 1994); Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993); Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); Amati v. City of Woodstock, 1997 WL 587493 (N.D. Ill. 8/7/97); Laughlin v. Maust, 1997 WL 436224 (N.D. Ill. 8/1/97); Pascale v. Carolina Freight Carriers Corp., 898 F. Supp. 276 (D. N.J. 1995)).

In Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993) (followed in Sanders v. Robert Bosch Corporation, 38 F.3d 736 (4th Cir. 1994), the court did not accept a monitoring system consisting of alligator clips attached to a microphone cable at one end and an interface connecting a microphone cable to a VCR and a video camera on the other, as a "telephone or telegraph instrument, equipment or facility, or any component thereof." The court noted that this monitoring system is factually remote from the telephonic and telegraphic equipment courts have recognized as falling within the exception at 18 U.S.C. § 2510(5)(a). The court cited as examples, Epps (dispatch console installed by telephone company considered telephone equipment); Watkins (standard extension telephone implicitly considered telephone equipment); Briggs (same); and James (monitoring device installed by telephone company implicitly considered telephone equipment). (Dissenting judge in Bosch considered the round-the-clock telephone monitoring for bomb threats to be within the business use exception.) [See "ORDINARY COURSE OF BUSINESS" EXCEPTION]

The statute defines "intercept" as "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." 18 U.S.C. Sec. 2510(4). Liability under the ECPA is therefore predicated on the use of a "device." See United States v. Turk, 526 F.2d 654, 658 (5th Cir.) (act requires "contemporaneous acquisition of the communication through the use of the device"), cert. denied, 429 U.S. 823 (1976). Because the government did not use any type of "device" to obtain the EFTs and information from intermediary banks (the banks complied with instructions contained in oral orders and arrest warrants in rem to freeze specified funds) no "interception" occurred. U.S. v. Daccarett, 6 F.3d 37 (2d Cir. 1993).

In U.S. v Meriwether, 917 F.2d 955 at 960 (6th Cir. 1990), the Sixth Circuit opined that simply pressing the retrieval button on a digital display pager and then visually observing the telephone numbers did not constitute the use of an electronic, mechanical or other device. However, in U.S. v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996), in a footnote regarding Meriwether, the judge opined that, in fact, pressing a button on a digital pager does constitute the use of an electronic or mechanical device.

Roving Interception

The Ninth Circuit held that the provision for roving wiretaps [18 U.S.C. 2518(11)(b)] is constitutional. The court stated that the conditions imposed by the statute satisfy the purposes of

the particularity requirement of the Fourth Amendment. A wide-ranging exploratory search is not permitted and there is virtually no possibility of abuse or mistake. The court noted that actual use by an identified speaker is required before interception is permitted, and that standard minimization procedures are required. The court further noted that the statute excuses identification of particular facilities to be surveilled only if the government establishes to the court's satisfaction the suspect's purpose to thwart interception by changing facilities. The court also based its holding on the fact that it has previously determined that the many safeguards mandated by the statute for both roving and fixed interceptions satisfy the Fourth Amendment requirement, as characterized in Katz v. U.S., 389 U.S. 347 (1967), that the intrusion into privacy be no greater than is necessary to meet the legitimate needs of law enforcement. U.S. v. Petti, 973 F.2d 1441 (9th Cir. 1992).

In U.S. v. Gaytan, 74 F.3d 545 (5th Cir. 1996), the Fifth Circuit held: "We find Petti persuasive and join the Ninth Circuit in finding the roving wiretap provision constitutional.
The defendants argued that conversations between parties not specifically named in the order were intercepted on the roving tap. The Court said that the order allowed the interception of telephone conversations that did not involve a person specifically named in the order by virtue of the words ". . . and others yet unknown." The government contended that "this was a mere clerical error and that the order should have read 'with others yet unknown.'" The Court found that the government intercepted many phone calls that did not involve any of the parties specifically named in the order, though it maintains that it properly screened calls and terminated interception when it became apparent that none of the named parties was involved in the conversation. The Court said that "even assuming the order to be overly broad and some of the interceptions to have been improper, the district court corrected the matter by excluding from evidence 'interceptions from the cellular telephones not involving at least one of these individuals [named in the wiretap order] as a party to the conversation.'" The Court said it was proper to restrict the suppression to those conversations that were improperly intercepted. The Court also found that the affidavit indicated that the defendants had engaged in a pattern of changing cellular phone numbers in an effort to avoid surveillance.

In its application for a roving oral interception order Government's failure to inform issuing judge of information regarding particular address as possible site for Mafia induction ceremony did not warrant suppression; affiant acted in complete good faith, her error was not made in reckless disregard for truth or for Government's other obligations to court, and fully informed, reasonable judge would nevertheless have authorized electronic surveillance at that address. U.S. v. Ferrara, 771 F. Supp. 1266 (D. Mass. 1991).

In U.S. v. McKinney, 785 F. Supp. 1214 (D. Md. 1992) the court found sufficient the affidavit supporting a 24 hour roving wire interception order.

On July 20, 1993, the Second Circuit held that 18 U.S.C. 2518(11)(a) satisfies the particularity requirement of the fourth amendment; that the order permitting roving oral surveillance in that case was constitutional and valid; that under Franks v. Delaware, 438 U.S. 154 (1978) the government's failure to disclose to the issuing judge recently obtained information indicating that a specific address would be the site for a Mafia induction ceremony does not require suppression; that the failure of the government to include prior electronic surveillance applications among the various alternative investigative procedures was not a violation of 2518(1)(c); that the failure of the government to disclose prior electronic surveillance applications was a violation of 2518(1)(e), but 2518(1)(e) is not central to Title III, and the government's nondisclosure was a good faith error, therefore suppression is not appropriate. U.S. v. Bianco, 998 F.2d 1112 (2d Cir. 1993).

Roving surveillance order permitting the interception of calls to and from any cellular telephones that named member of the Gangster Disciples might use, satisfied the particularity standard of the Fourth Amendment. Favorably citing Petti, Bianco and Gaytan, the Seventh Circuit said "we have nothing to add to their analysis of the issue." U.S. v. Jackson, 207 F.3d 910 (7th Cir. 2000); U.S. v. Wilson, 237 F.3d 827 (7th Cir. 2001) (reiterating holding in Jackson); U.S. v. Hoover, 246 F.3d 1054 (7th Cir. 2001)(reiterating holding in Jackson).

Roving wiretap was reasonable under Fourth Amendment and minimization requirement was not flagrantly disregarded. U.S. v. Parks, 1997 WL 136761 (N.D. Ill.) and U.S. v. Johnson, 1997 U.S. Dist. LEXIS 9573 (N.D. Ill. 7/3/97) (both citing Petti, Gaytan, and Bianco).

Affidavit sufficiently demonstrated, as required by 2518(11)(b)(ii), the targeted person's purpose to thwart interception by changing facilities. U.S. v. Villegas, 1993 WL 535013 (S.D.N.Y.).

Section 2518(11)(a) does not require a showing that the impracticality of specifying a single place at which oral communications are to be intercepted stems from a target's intent to avoid interception. The government provided a sufficient basis to find that it was not practical to identify a specific automobile in which the conversations sought to be intercepted would occur. U.S. v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995).

Wiretap order applying to a target cellular telephone number and to any changed number subsequently assigned to the same ESN utilized by the target telephone and to any ESN subsequently assigned to the same telephone number utilized by the target cellular telephone, was not a "roving wiretap." A telephone number and ESN were specified with particularity and, therefore, there was no need to resort to 18 U.S.C. 2518(11)(b). U.S. v. Lutcher, 2004 WL 1274457 (E.D. La.).

"spot monitoring" for "ascertainment"

OEO takes the position that if physical surveillance is not possible, spot monitoring may be employed to meet the ascertainment requirement of 2518(12) before "actual interception" begins under a roving interception order.

Electronic Pocket Notebook

The data stored in these devices are not "electronic communications" because the data is not "transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. 2510(12).

Electronic Funds Transfers

(On April 24, 1996, 18 U.S.C. 2510(12) was amended to exclude "electronic funds transfer information" from the definition of "electronic communication.")

Application/Order/Affidavit

Authorized Attorney

Application may be made by any attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in Chapter 119 of Title 18. 18 U.S.C. 2510(7) and 2518(1)(a). An assistant United States attorney is authorized by statute to "prosecute all offenses against the United States." 28 U.S.C. 547(1). The Justice Department does not permit attorneys who are not licensed members of the bar in at least one state or the District of Columbia to practice law without supervision. An attorney does not lose his status as an assistant United States attorney when he voluntarily chooses to become an inactive member of his bar. Even if he were "unlicensed," he could still function within the Justice Department, albeit with supervision, and therefore could still "participate in the prosecution of offenses." Tyree v. Dance, 1990 WL 40298 (9th Cir.). An assistant United States attorney prosecuting a crime that occurred within his jurisdiction has the authority to submit a wiretap application in another district in furtherance of such prosecution. U.S. v. Ishola, 1996 WL 197461 (N.D. Ill. 4/19/96).

A Title III application must be authorized by certain high-ranking Justice Department officials, 18 U.S.C. 2516(1), but 18 U.S.C. 2518(1)(a) does not require that a government attorney, rather than a law enforcement officer, execute the affidavit (attached as part of the application) used to establish probable cause and the inadequacy of alternative investigative techniques. Per 2518(1)(a), each application shall include the identity of the "investigative or law enforcement officer" making the application, and the officer authorizing the application. U.S. v. Williams, 124 F.3d 411 (3d Cir. 1997).

Non-Enumerated Offenses

“18 U.S.C. § 371 was an enumerated offense for the purposes of 18 U.S.C. § 2516, where the wiretap order concurrently authorized investigation of two other offenses specifically listed in § 2516. However, this case presents no opportunity to determine whether a wiretap order including only 18 U.S.C. § 371, without additional explicitly enumerated offenses, would survive appellate review.” Mere references to non-enumerated offenses will not invalidate wiretap application documents or orders. “[T]he incorrect description of suspected non-enumerated offenses as enumerated in application materials and findings in a wiretap order does not invalidate that order where the authorization to wiretap itself was limited to only enumerated offenses. The question of whether an order authorizing wiretapping in investigation of both enumerated and non-enumerated offenses would survive review is saved for another day.” U.S. v. Smart, 278 F.3d 1168 (10th Cir. 2002).

"The reference to additional statutory violations was irrelevant; once the acts of taping were justified under 18 U.S.C. § 2518 by any adequate evidence, that reference furnishes no basis of suppression." U.S. v. Mongelli, 799 F. Supp. 21 (S.D.N.Y. 1992).

Probable Cause

The existence of probable cause is determined by looking at the "totality of the circumstances." This determination is a practical, common sense decision whether, given all the circumstances

set forth in the affidavit there is a fair probability that evidence of a crime will be found in a particular place. Illinois v. Gates, 462 U.S. 213 (1983).

For the issuance of a wiretap order, probable cause is present if the totality of the circumstances reveals that there is a fair probability that a wiretap will uncover evidence of a crime. U.S. v. Fairchild, 189 F.3d 769 (8th Cir. 1999).

The standard for probable cause under Title III is identical to that under the Fourth Amendment. U.S. v. Zambrana, 841 F.3d 1320 (7th Cir. 1988); U.S. v. Gotti, 2005 WL 859244 (S.D.N.Y.); U.S. v. Caldwell, 2005 WL 818412 (N.D. Ill.)(citing Zambrana); U.S. v. Garcia, 2005 WL 589627 (S.D.N.Y.); United States v. Mares- Martinez, 240 F. Supp.2d 803 (N.D. Ill. 2002); U.S. v. Santana, 218 F. Supp.2d 53 (D. N.H. 2002); U.S. v. Aparo, 2002 WL 2022329 (E.D.N.Y.)(citing U.S. v. Fury, 554 F.2d 522 (2d Cir. 1977)).

Title 18 U.S.C. 2518(3)(d) establishes three alternative bases for establishing probable cause: (1) that the target facilities are being used or are about to be used in connection with an enumerated offense; or (2) that the target facilities are leased to or listed in the name of an individual believed to have committed an enumerated offense; or (3) that the target facilities are commonly used by an individual believed to have committed an enumerated offense. The only limitation on such interceptions is whether there is probable cause to believe that communications concerning the offense will be obtained through the interception. U.S. v. Diguglielmo, 1985 U.S. Dist. LEXIS 19385 (E.D. Pa.).

It was error for magistrate to use bank records that were not submitted to the issuing court as a basis for second guessing that court's probable cause determination. Additional facts about the loan transactions that the magistrate thought the FBI recklessly failed to pursue were not essential to the showing of probable cause as to a possible kickback conspiracy. Thus, there was no Franks v. Delaware violation. Beyond misperceiving the government's probable cause showing, the magistrate judge erred in focusing his Franks v. Delaware analysis on what the FBI could have learned with more investigation-which is relevant only to the statutory necessity issue-rather than on what the FBI actually knew when it prepared the instant affidavit. Staleness was an issue in this case, but where recent information corroborates otherwise stale information, probable cause may be found. Stripped of its erroneous Franks v. Delaware underlay, the district court's contrary conclusion reflects a de novo probable cause determination that is inconsistent with the deferential standard of review that must be accorded the issuing judge. In view of the complex nature of the investigation (bank fraud conspiracy) and the issuing judge's continuing supervision, the government's minimization procedures did not violate 18 U.S.C. 2518(5). The agents submitted their minimizing procedures to the issuing judge and reported minimizing problems to the judge as surveillance progressed. "The agents used the 'two minutes up/one minute down' minimization technique recommended in the Department of Justice Manual, a procedure we reviewed favorably . . . ." This technique provided intermittent spot-checking of minimized conversations, a procedure expressly authorized by the issuing judge and previously approved by the Eighth Circuit. The agents inadvertently intercepted numerous attorney communications, but the defendants failed to prove that each of these communications were attorney-client privileged and they also failed to prove that the agents acted in bad faith. It was error to impose suppression as punishment for these inadvertent interceptions of attorney communications. Because there was no bad faith attempt to obtain privileged conversations, those conversations should be suppressed on an individual basis at or before trial. U.S. v. Ozar, 50 F.3d 1440 (8th Cir. 1995).

The Eighth Circuit Court of Appeals expressly disapproved of the government's failure to inform the issuing judge, either in the affidavit or orally, that a person named in the affidavit as a person

who was continuing to commit violations, actually was C/W-1 and not a suspect. "We are not unsympathetic to the need to ensure the safety of cooperating witnesses in this type of situation. However, safety concerns are not compromised by sworn testimony before the issuing judge fully disclosing the fact of and the reasons for masking the witness's identity in the affidavit." U.S. v. Falls, 34 F.3d 674 (8th Cir. 1994).

The court found that the affiant decided to omit the fact that confidential informant number six was a member of the Sons of Silence because he was concerned that the informant's life would be endangered in the event that the Title III affidavit was unsealed prior to indictment. However, at the evidentiary hearing, neither the affiant nor the government could identify a single instance where a Title III affidavit had been unsealed prior to the return of an indictment. "Thus, the court finds Special Agent Terra's reason for omitting the information regarding confidential informant number six's Sons of Silence membership to be objectively unreasonable. Nonetheless, although the court does not condone the action, this was not an attempt to enhance the contents of the affidavit submitted in support of the Tittle III application. Rather, it was a measure employed in order to mask the informant's identity for his own safety. U.S. v. Gruber, 994 F. Supp. 1026 (N.D. Iowa 1998).

In the Sudafed/cyanide poisoning and murder case, the FBI's original Title III application failed to disclose that 1) the principal informant had been convicted of forgery and fraud three times, and though each of these convictions was more than ten years old, he had a panoply of parole violations for similar offenses stretching back to his first conviction; 2) though the FBI rap sheet did not reflect it, Keith Meling had been convicted of a felony in 1990, just one year before the wiretap application, and had been committed to a mental institution, where he experienced auditory and visual hallucinations and was diagnosed as a schizophrenic; and 3) the affidavit failed to mention that Keith Meling came forward at least in part to obtain the $100,000 reward offered for information relating to the poisonings; to the contrary, the affidavit characterized Keith Meling's motives as pure. The FBI did not correct these misstatements and omissions in the extension applications. The Ninth Circuit panel held, however, that the original and extension applications provided probable cause for the wiretap "once the FBI's dissembling is corrected" and therefore no Franks hearing was required. Regarding the omissions and misstatements in the Title III affidavits, the Ninth Circuit panel included the following footnote in its opinion: "This conclusion should in no way commend similar practices to the FBI in the future. We understand the urgency the FBI agents felt as they strove to prevent further poisonings. But this does not justify deliberate or reckless misrepresentations in wiretap applications." U.S. v. Meling, 47 F.3d 1546 (9th Cir. 1995).

The government concedes that it recklessly failed to include in its wiretap affidavit information concerning the times a confidential informant had perjured himself, lied, been arrested and failed to pay income taxes. Several circuit opinions mention the informant by name and impugn his credibility. However, the Ninth Circuit held that the omission was not material. There was overwhelming evidence in the affidavit corroborating the evidence obtained via the subject informant. This evidence included physical surveillance, three other informants and an undercover agent. U.S. v. Bennett, 219 F.3d 1117 (9th Cir. 2000).

Regarding a Title III affidavit's failure to disclose a CI's prior drug trafficking conviction, his past involvement with some defendants, and other indicia of his possible unreliability, the First Circuit held that the CI's information was not material to the finding of probable cause and therefore not a basis for suppression, and that no Franks hearing was required because the defendants failed to make the requisite showing of materiality. Regarding the affidavit's omission of information concerning the CI's background, the Court opined as follows:

> The affidavit was, to put it mildly, economical on this point, stating only that there was no indication that Hernandez "has been less than truthful at any time with regard to this investigation." This statement was crafted carefully to avoid mention of facts that would call Hernandez's trustworthiness into serious question. We are concerned that such significant omissions could thwart the intent of Title III and mislead an issuing judge, who relies on the government to present the full case for its belief in probable cause, including any contraindications. The troubling omissions here have less significance because the affidavit also included large quantities of evidence from sources other than Hernandez.

U.S. v. Nelson-Rodriguez, 319 F.3d 12 (1st Cir. 2003).

"We find troubling Agent Lucas' apparent misrepresentations concerning the past cooperation of the informants involved in this case. Although the government maintains that there was an absence of proof concerning the agent's deliberateness or recklessness in making the misrepresentations, it is unclear how Agent Lucas could have made such statements of an affirmative character for which there was no basis without having acted either deliberately or recklessly. . .However. . .[t]he Supreme Court made it clear in Franks that in order to be entitled to relief a defendant must show. . . that, absent those misrepresentations or omissions, probable cause would have been lacking. . .[T]he mere fact that an informant's trial testimony contradicts information attributed to that informant in an affidavit supporting a warrant does not entitle a defendant to suppression. Instead, the defendant must show that it is the agent, and not the informant, who has made misrepresentations." U.S. v. Novaton, 271 F.3d 968 (11th Cir. 2001).

A Franks motion must challenge the veracity of the affiant, not that of his informant. U.S. v. Staves, 383 F.3d 977 (9th Cir. 2004).

Defendant failed to make requisite preliminary showing that allegations in affidavit were deliberate falsehoods or made with a reckless disregard for the truth, and therefore district court did not have to order a Franks hearing on motion to suppress. U.S. v. Brown, 298 F.3d 392 (5th Cir. 2002).

"The inaccurate code words and summaries demonstrate a troubling carelessness, but do not support an inference that [affiant] was attempting to mislead or was acting with reckless disregard of the true content of the conversations." U.S. v. Estrada, 1995 WL 577757 (S.D.N.Y.).

Alleged misstatements regarding the size and scope of the criminal organization do not negate the conclusion that the Government satisfied the necessity and probable cause requirements for the issuance of a wiretap. U.S. v. Small, 229 F. Supp.2d 1166 (D. Col. 2002).

The government conceded that affiant and DEA were mistaken in their initial identification of subject and the assignment of a criminal history. Once discovered, the government omitted this information from future affidavits, drafted reports to this effect, and informed defendants of the mistake. Such mistakes do not constitute a knowing false statement or reckless disregard for the truth. It also falls short of what is required for a Franks hearing. Even if this were not the case, the misstatements are immaterial to the probable cause determination and therefore a Franks hearing is unnecessary. U.S. v. Velazquez, 1997 WL 564674 (N.D. Ill.). See also U.S. v. Caldwell, 2005 WL 818412 (N.D. Ill.)

Without the support of factual affidavits, defendants' arguments in their memorandum of law almost exclusively dispute the conclusions and inferences drawn by the affiant from the intercepted conversations about defendants' involvement in a scheme to defraud union pension funds. By merely disagreeing about the fair interpretation of the intercepted communications,

which were reproduced or summarized for independent review by the authorizing judges, defendants fail to meet their burden of establishing that the affiant's statements were false or recklessly made. U.S. v. Labate, 2001 U.S. Dist. LEXIS 6509 (S.D.N.Y.).

Title III suppression denial by court contains a thorough discussion of necessity, probable cause, facial sufficiency, informant reliability, staleness, and Franks issues. U.S. v. Hanhardt, 157 F. Supp.2d 978 (N.D. Ill. 2001).

The application established probable cause. The cumulative effect of the alleged misrepresentations and omissions do not undermine the basis for probable cause, and the defendant, having failed to make the requisite showing, is not entitled to a Franks hearing. U.S. v. Jarding, 2002 WL 1905533 (N.D. Ill.).

The application established probable cause. The defendant failed to establish the requisite materiality and intent for a Franks hearing. U.S. v. Mikos, 2003 WL 22462560 (N.D. Ill.); U.S. v. Le, 377 F. Supp.2d 245 (D. Me 2005).

Defendant failed to establish that purported misstatements and omissions with regard to the finding of probable cause were made with the intent to deceive the court, or were necessary to the finding of probable cause. Therefore, a Franks hearing is not required. U.S. v. Moran, 349 F. Supp.2d 425 (N.D.N.Y. 2005).

Defendant failed to make specific allegations regarding false statements in the affidavit, much less a substantial showing or an offer of proof. Accordingly, he has not met the standards for a Franks hearing. U.S. v. Scala, 388 F. Supp.2d 396 (S.D.N.Y. 2005).

(Staleness)

"[W]here the facts adduced to support probable cause describe a course or pattern of ongoing and continuous criminality, the passage of time between the occurrence of the facts set forth in the affidavit and the submission of the affidavit itself loses significance." The confidential sources cited in the government's affidavit depicted the acceptance of payments not only as a routine and continuous practice from 1992-1997, but, as evidenced by CS1's statements concerning Appellant Tursi's extortion in April of 1999, and payments made to inspector O'Donnell from April to October 1999, also as a practice that continued beyond 1997 into late 1999. In other words, there was evidence that the plumbing inspectors' misconduct was an established, routine practice that had spanned numerous years and had continued at least up until just months prior to the District Court's initial authorization of the video surveillance in February of 2000. We therefore conclude that the evidence of the plumbing inspectors' continuous misconduct leading up to the time of the first affidavit's issuance was not stale, and therefore provided probable cause for the video surveillance. U.S. v. Urban, 404 F.3d 754 (3d Cir. 2005).

The principal factors in assessing whether or not the supporting facts have become stale are the age of those facts and the nature of the conduct alleged to have violated the law. U.S. v. Gallo, 863 F.2d 185 (2d Cir.1988) (quoting U.S. v. Martino, 664 F.2d 860 (2d Cir. 1981)). Where a supporting affidavit presents a picture of continuing conduct as opposed to an isolated instance of wrongdoing, the passage of time between the last described act and the presentation of the application becomes less significant. This is especially true in a case involving an ongoing narcotics operation, where intervals of weeks or months between the last described act and the application for a wiretap do not necessarily make the information stale. Rivera v. U.S., 928 F.2d 592 (2d Cir.1991) (dealing with search warrants) (citing U.S. v. Rowell, 903 F.2d 899 (2d Cir.1990) (holding that gap of 18 months did not render information stale); Martino, 664 F.2d at

867 (3 weeks); U.S. v. Fama, 758 F.2d 834 (2d Cir. 1985) (5 weeks)). Here, the district judge properly concluded that the Affidavit did not contain stale information. First, the Affidavit stated
that Roman and other members of the Latin Kings (1) were involved in drug trafficking activities as late as March 1994, within one month of the wiretap application; (2) used telephones to conduct their illegal drug activities; and (3) that Roman's phone was used to make calls to and receive calls from these individuals until March 1994. Moreover, as the district judge found, to the extent that there are acts of past criminal activity that in and of themselves might be stale, such acts "can be sufficient if [an] affidavit also establishes a pattern of continuing criminal activity so there is reason to believe that the cited activity was probably not a one-time occurrence." U.S. v. Wagner, 989 F.2d 69 (2d Cir. 1993). U.S. v. Diaz, 176 F.3d 52 (2d Cir. 1999).

Where recent information corroborates otherwise stale information, probable cause may be found. U.S. v. Ozar, 50 F.3d 1440 (8th Cir. 1995).

Notwithstanding four month period between last observed drug transaction and filing of wiretap application, the on-going nature of the conspiracy was sufficiently established by the affidavit to support finding that probable cause existed for the issuance of the wiretap order. U.S. v. Tallman, 952 F.2d 164 (8th Cir. 1991).

DOJ Authorization

A Title III order issued by a district judge on the application of an AUSA before the Attorney General or her designee has authorized the application is invalid. The interception of communications pursuant to that order are “unlawful” within the meaning of 18 U.S.C. 2518(10)(a)(1) and the evidence thereby obtained must be suppressed. Here, either the assistant or agent told the issuing judge that the written authorization was on its way but had not yet been received. The judge then signed the order and added in his own handwriting: “This order is not to be executed until and unless formal approval in writing is received from the U.S. Attorney General or her designee.” For purposes of the appeal it is assumed that approximately one hour later, an OEO staff attorney faxed the authorization memorandum to the U.S. Attorney’s office. Within minutes of receiving the faxed authorization, the government commenced the wiretap. The Ninth Circuit held: “The statutory sequence of wiretap authorization makes it clear that prior authorization by senior executive branch officials is an express precondition to judicial approval under § 2516; its violation merits suppression. . . A district court may not delegate to law enforcement officials at any level its singular power to set the surveillance mechanism in motion.” U.S. v. Reyna, 218 F.3d 1108 (9th Cir. 2000) (citing U.S. v. Chavez, 416 U.S. 562 (1974)).

Section 2516(1) does not explicitly require written authorization for a Title III application. Telephonic authorization is adequate. U.S. v. Vogt, 760 F.2d 206 (8th Cir. 1985); U.S. v. Cale, 508 F. Supp. 1038 (S.D.N.Y. 1981).

U.S. v. Wright, 156 F. Supp.2d 1218 (D. Kan. 2001):

> The letters of authorization here identify the officials who are responsible for having exercised this approval authority. That another official signed on behalf of the authorizing official does not appear to contravene any statutory requirement. Indeed, Title III does not prescribe the manner in which authorization is accomplished or shown. In United States v. Pichardo, 1999 WL 649020, at *4 (S.D.N.Y. Aug. 25, 1999), the court rejected a defendant's challenge that the person signing the letter was not an authorized individual. "[U]naware of any authority requiring the official authorizing the application to personally sign the letter transmitted to the U.S. Attorney's Office,"

> the court concluded it was enough that the application was signed on behalf of an authorized official. Id. The court agrees with this reasoning and finds no grounds here to question whether the application was properly authorized simply because the application was signed on behalf of the authorizing individual.

Some threshold showing of irregularity is required before government officials (DAAG Keeney and DAAG Richard) may be forced to authenticate their signatures on official documents. U.S. v. Edmond, 718 F. Supp. 988 (D.D.C. 1989) (citing U.S. v. De La Fuente, 548 F.2d 528 (5th Cir. 1977)). Authorizing official is presumed to have properly exercised his power unless the defendant offers evidence, apart from mere conjecture or speculation, to rebut this presumption. U.S. v. Terry, 702 F.2d 299 (2d Cir. 1983).

"We decline to find that the fact that Keeney's signature was stamped rather than originally signed suggests that neither Keeney nor Dennis (both properly designated officials), authorized the intercept application." U.S. v. Citro, 938 F.2d 1431 (1st Cir. 1991).

The Title III authorization clearly identified Mary Lee Warren as a Deputy Assistant Attorney General and therefore she had authority pursuant to 18 U.S.C. 2516 and Order 1950-95 to authorize the wiretap application. U.S. v. Ceballos, 302 F.3d 679 (7th Cir. 2002). See also U.S. v. Gray, 372 F. Supp.2d 1025 (N.D. Ohio 2005)(citing Ceballos; involves DAAG Malcolm and Order 2407-2001).

Assuming that the relevant DAAGs were properly authorized to approve applications, the fact that the memos they signed purported to be "from" Acting AAG or AAG is irrelevant to the purposes of the statute because the individuals who did sign the authorizations were identifiable. U.S. v. Anderson, 39 F.3d 331 (D.C. Cir. 1994). See also, U.S. v. White, 2004 WL 2823225 (E.D. Pa.); U.S. v. Monarrez-Cano, 2002 WL 1485388 (D. Neb.) (DAAG Swartz signed authorization memo prepared for AAG Chertoff's signature; citing Anderson and Citro); U.S. v. Gray, 372 F. Supp.2d 1025 (N.D. Ohio 2005)(citing Monarrez-Cano; DAAG Malcolm signed authorization memo drafted for Chertoff's signature).

The fact that DAAG Keeney and DAAG Richard were operating pursuant to an order issued by departed Attorney General Meese in no way vitiated their authority. U.S. v. Edmond, 718 F. Supp. 988 (D.D.C. 1989) (citing U.S. v. Lawson, 780 F.2d 535 (6th Cir. 1985)(Civiletti authorization in 1981 permitted AAG under Smith to approve application in 1983); U.S. v. Kerr, 711 F.2d 149 (10th Cir. 1983); U.S. v. Terry, 702 F.2d 299 (2d Cir. 1983); U.S. v. Messersmith, 692 F.2d 1315 (11th Cir. 1982); U.S. v. Wyder, 674 F.2d 224 (4th Cir. 1982); U.S. v. Todisco, 667 F.2d 255 (2d Cir. 1981)).

"We choose to join the majority of our sister circuits in holding that a designation continues in force through a change in attorneys general, so long as the designated Deputy Assistant remains in office. We leave for another day the question of whether the First Circuit's position, allowing designations by office rather than person, represents an acceptable application of the statutory command that Deputy Assistants be 'specially designated'." U.S. v. Anderson, 39 F.3d 331 (D.C. Cir. 1994).

The fact that special designation is by job title and applies to more than one person does not invalidate designation as long as designation order clearly identifies and evinces intent to designate authorizing officer. U.S. v. Citro, 938 F.2d 1431 (1st Cir. 1991); U.S. v. Torres, 908 F.2d 1417 (9th Cir. 1990); U.S. v. Nanfro, 64 F.3d 98 (2d Cir. 1995); U.S. v. Bynum, 763 F.2d 474 (1st Cir. 1985); U.S. v. Chen, 2000 WL 1073652 (N.D.N.Y.); U.S. v. Hendricks, 2004 U.S. Dist. LEXIS 8859 (D. V.I.).

A correct, but somewhat general descriptor of the person who authorized the wiretap application ("duly designated official of the Criminal Division, United States Department of Justice") is not a grievous problem as long as that individual was statutorily permitted to make the authorization. Each application was authorized by an individual who has specific delegated authority. The failure to include that individual's specific name in the wiretap order does not warrant suppression. U.S. v. White, 2004 WL 2823225 (E.D. Pa.)(citing U.S. v. Chavez, 416 U.S. 562 (1974) language: "while adherence to the identification requirements of 2518(1)(a) and 4(d) can simplify the assurance that those whom Title III makes responsible for determining when and how wiretapping and electronic surveillance should be conducted have fulfilled their roles in each case, it does not establish a substantive role to be played in the regulatory system."); U.S. v. Small, 229 F. Supp.2d 1166 (D. Col. 2002)(also citing Chavez). See also U.S. v. Fudge, 325 F.3d 910 (7th Cir. 2003)(government's application and order were not models of clarity regarding the identity of the authorizing official but the court could discern it was DAAG Kevin DiGregory. There was no chicanery or deception involved in the application process and the order noted authorization was made pursuant to a power delegated by the Attorney General. Thus, under Chavez, the order's failure to identify the individual who authorized the application did not violate any substantive requirement of Title III and consequently does not warrant suppression).

Wiretap orders that fail to comply with the mandate of 18 U.S.C. 2518(4)(d) that the order specify the identity of the Department of Justice officials who authorized the applications are facially insufficient under 18 U.S.C. 2518(10)(a)(ii), but because these are technical defects that do not undermine the purpose of the statute or prejudice the defendant, the district court's denial of suppression is affirmed. The Tenth Circuit joins the Third, Fifth, Sixth, Seventh, Eighth and Ninth Circuits in holding that the Supreme Court's holdings in U.S. v. Chavez, 416 U.S. 562 (1974) and U.S. v. Giordano, 416 U.S. 505 (1974) that non-substantive violations of Title III do not require suppression of wiretaps found "unlawful" under 2518(10)(a)(i), also applies to wiretap orders found to be facially insufficient under 2518(10)(a)(ii). U.S. v. Radcliff, 331 F.3d 1153 (10th Cir. 2003); U.S. v. Small, 423 F.3d 1164 (10th Cir. 2005)(following Radcliff).

Reading the statute to permit a blanket designation does not render the phrase "specially designated" superfluous. "Under our interpretation, the statute provides the Attorney General with the power to designate any or all Deputy Assistant Attorneys General, but does not command that they be designated. Read in this way, the provision provides discretion to the Attorney General, who may decide, based on the circumstances, whether a designation is appropriate." U.S. v. Nanfro, 64 F.3d 98 (2d Cir. 1995).

Congress did not prescribe methods to be used by AAG to satisfy himself that wiretap was in order or forbid assistance of subordinates in reviewing application. District court properly refused to hold evidentiary hearing into sufficiency of AAG's review of wiretap application where authorization bore signature of official designated in statute. U.S. v. O'Malley, 764 F.2d 38 (1st Cir. 1985).

"[E]ven though the United States concedes that some of the . . . affidavits were changed between the time they were approved by a DOJ official and presented to Judge Roberts, there is no indication that doing so even constituted a violation of the statute or, if it did, that it warrants suppression of the evidence." U.S. v. Eiland, 2005 WL 2679992 (D. D.C.).

Technicalities, Typos and Omissions

Erroneous identification of official authorizing wiretap application did not affect sufficiency of application as long as proper official in fact authorized application. U.S. v. Chavez, 416 U.S. 562 (1974) (cited in footnote in U.S. v. Villegas, 1993 WL 535013 (S.D.N.Y.) concerning AUSA's inadvertent switching of the signature pages of the transmittal letter (Frederick Hess) and the authorization memorandum (Mark Richard)).

"Collating error" resulting in attachment of OEO Director Hess's cover letter signature page as the signature page of AAG William Weld's authorization memorandum did not establish a claim that the application was not authorized by an appropriately designated official. A reading of the documents clearly indicated that Weld, not Hess, authorized the application. U.S. v. London, 66 F.3d 1227 (1st Cir. 1995).

The fact that OEO Director's cover letter forwarding Title III authorization memorandum to the United States Attorney was addressed to the wrong United States Attorney is of no import because the cover letter is not required by statute. Moreover, the appropriate DOJ official approved the application in accordance with 18 U.S.C. 2516. U.S. v. Sappleton, 2003 U.S. App. LEXIS 12756 (4th Cir.)(unpublished).

Alleged variance between description of targeted premises in AAG's authorization and the description in the application submitted to judge was not a violation of 18 U.S.C. 2516(1), since the proposed application was before the AAG when he issued the authorization, and since the issuing judge did not adopt the language of the AAG or the AUSA. Even if the variance in language among the authorization letter, application and order were technical violations of Title III, they did not directly and substantially impede the implementation of the congressional intent to condition use of intercept procedures upon the judgment of a senior official of the Department of Justice, and therefore did not warrant suppression. U.S. v. Ianniello, 621 F. Supp. 1455 (S.D.N.Y. 1985).

Although it is true that Hobbs Act violations are not specifically included in the authorization letter, the omission appears to be a mere oversight. Defendant presents no evidence that the Department of Justice purposefully did not provide authorization for the interception of such offense, or that the failure to get such authorization was done intentionally or recklessly. Although authorization is central to the statutory directive of the statute, Giordano, 416 U.S. at 520, AUSA Lee did receive authorization for the interception of communications. The omission of this one offense from the authorization letter, when viewed against the backdrop that all the facts of the investigation were fully disclosed to the court and to her superiors, is not material to a finding that the authorization order is proper. Authorization orders are presumed proper. See U.S. v. Jabara, 618 F.2d 1319 (9th Cir. 1980). Defendant has presented no information to the court to overcome this presumption. U.S. v. Luong, CR-96-0094 MHP (N.D. Cal. 9/7/99).

Technical accuracy in the order or application is not required. U.S. v. Feldman, 606 F.2d 673 (6th Cir. 1979); U.S. v. Sklaroff, 506 F.2d 837 (5th Cir. 1975); U.S. v. Bennett, 825 F. Supp. 1512 (D. Colo. 1993) ("is authorized" omitted from order, discrepancy in dates on orders); U.S. v. Ishola, 1996 WL 197461 (N.D. Ill. 4/19/96) (no suppression where listing of "pending" application was inadvertently not updated to "authorized").

Clerical errors resulting in an incorrect digit or inversion of digits in target telephone numbers do not invalidate a wiretap application or order. U.S. v. Doolittle, 507 F.2d 1368 (5th Cir. 1975); U.S. v. Sklaroff, 506 F.2d 837 (5th Cir. 1975). Similarly, a typographical error in the defendant's address in the application authorization does not invalidate the application or order. U.S. v. De La Fuente, 548 F.2d 528 (5th Cir. 1977). Government substantially complied with

Title III by mistakenly identifying defendant by mother's maiden name. U.S. v. Ishola, 1996 WL 197461 (N.D. Ill. 4/19/96).

Although wiretap order included language indicating that it would expire ten days from issuance, intent of order was to limit wiretap to statutorily prescribed 30 days. Ambiguity in the order describing duration of wiretap did not require suppression of evidence. U.S. v. Kirkland, 705 F. Supp. 1572 (M.D. Ga. 1989).

"Clerical" mistakes are wording mistakes introduced by accident or lack of care rather than wilfully or with sinister purpose. The flaw in this case (confusing references to "wire" communications and telephones in a state interception order intended to authorize interception of oral communications occurring inside a tavern), although serious, was a discrete set of clerical mistakes in a process that in all other important respects complied with the statute. Very serious "clerical" mistakes are often forgiven depending upon the risk that they pose in fact. Because the judge and the executing officer knew what had been proposed and authorized, there was no substantial threat that this officer would intercept communications other than as authorized. U.S. v. Cunningham, 113 F.3d 289 (1st Cir. 1997).

Amended order correcting clerical mistakes in the list of names contained in the original order of the day before, but in all other respects an exact replica of the original order, did not change the effective date of the original order. U.S. v. Blanco, 1994 WL 695396 (N.D. Cal.).

Judge's act of signing the order (page three was missing) was sufficient to show that the judge made the findings required by statute. The findings were not required to be in writing. U.S. v. Traitz, 871 F.2d 368 (3d Cir. 1989).

Wiretap order inadvertently left unsigned by issuing judge was "insufficient on its face" under 2518(10)(a)(ii), but suppression was not warranted. Neither 2518(3) nor 2518(4) mandate a signed order (likely congressional deference to the judiciary to decide how an order may be "entered," and perhaps also a recognition that modern technology offers ways to replace the personal signature), and the absence of a signature does not violate a core requirement of the statute (Donovan standard). The absence of judge's signature was a technical defect similar to the missing of page 3 from the interception order in the Traitz case. Also, the Leon good faith principle applies to 2518(10)(a) issues, and requires that suppression be denied in this case. U.S. v. Moore, 41 F.3d 370 (8th Cir. 1994).

Wiretap orders that fail to comply with the mandate of 18 U.S.C. 2518(4)(d) that the order specify the identity of the Department of Justice officials who authorized the applications are facially insufficient under 18 U.S.C. 2518(10)(a)(ii), but because these are technical defects that do not undermine the purpose of the statute or prejudice the defendant, the district court's denial of suppression is affirmed. The Tenth Circuit joins the Third, Fifth, Sixth, Seventh, Eighth and Ninth Circuits in holding that the Supreme Court's holdings in U.S. v. Chavez, 416 U.S. 562 (1974) and U.S. v. Giordano, 416 U.S. 505 (1974) that non-substantive violations of Title III do not require suppression of wiretaps found "unlawful" under 2518(10)(a)(i), also applies to wiretap orders found to be facially insufficient under 2518(10)(a)(ii). U.S. v. Radcliff, 331 F.3d 1153 (10th Cir. 2003). See also U.S. v. Callum, 410 F.3d 571 (9th Cir. 2005) (order's failure to specify the identity of the person authorizing the application, as required by 2518(4), was merely a minor facial insufficiency for which suppression is not the appropriate remedy; nor was suppression required because two subsequent orders specified the AAG rather than, correctly, the DAAG as the authorizing official); U.S. v. Gray, 372 F. Supp.2d 1025 (N.D. Ohio 2005)(omission of DAAG Malcolm's name from application and order constituted mere

technical defects; fact of proper authorization made known to issuing judge and defendant apprised of authorization memo at suppression hearing).

Assistant district attorney was not formally sworn before he applied for a wiretap. Although this was a violation of 18 U.S.C. 2518(1), it is insufficient to support a writ of habeas corpus. Even on direct appeal it is likely that suppression would have been prevented under the Donovan (no violation of core requirement) and Leon ("good faith" exception) standards. Rankins v. Murphy, 198 F. Supp.2d 3 (D. Mass. 2002).

As Title III does not require submission of affidavits in support of an interception application but merely requires that a written application be submitted upon oath or affirmation, there was compliance with the statute despite the fact that the FBI agent had failed to sign the affidavit in support of the application, where the judge based his order on the agent's sworn statements made in his presence as well as the written application. Moreover, the affidavit was enclosed as a part of the actual application which did contain the signature of the DOJ attorney. U.S. v. Florea, 541 F.2d 568 (6th Cir. 1976).

Given that the government fully complied with the oath or affirmation requirement by submitting a sworn final version of the application, it is irrelevant that the government also submitted an unsworn courtesy copy to the court the day before the scheduled hearing on the application. The judge carefully reviewed any modifications prior to making a decision on the order. The record is clear theat the district court relied on the final version of the application in granting the wiretap order. U.S. v. Small, 423 F.3d 1164 (10th Cir. 2005).

The judge's Title III order, approving the AUSA's application, stated that the AUSA made the application under oath. "This is more than sufficient to satisfy the oath or affirmation requirement of 2518(1)." U.S. v. Gray, 372 F. Supp.2d 1025 (N.D. Ohio 2005).

Although affidavit in support of wiretap application did not indicate that agent signed it under oath, statutory and Fourth Amendment "oath or affirmation" requirements were satisfied where agent gave uncontradicted testimony that he signed the affidavit under oath administered by the judge who authorized the wiretap at the same time that AUSA verified his application, and where record indicated that AUSA's application was signed under oath when wiretap was authorized. U.S. v. Talbert, 706 F.2d 464 (4th Cir. 1983).

Although a supplemental application did not address the "necessity requirement" as such, it was nevertheless valid, whether under a common sense approach to the Wiretap Act, see U.S. v. Nunez, 877 F.2d 1470 at 1472 (10th Cir. 1989), or under the spirit of guidance enunciated in U.S. v. Ventresca, 380 U.S. 102, 111-12 (1965) (officers did what the Constitution requires). The supplemental order was issued a mere four days after the original order for the sole reason that the telephone number had been changed on a mobile phone targeted in the original order. "We note that, in contrast, the second supplemental order held invalid in Mondragon [appeal by codefendants] authorized surveillance of a new number, listed in the name of a different individual residing at a different location." U.S. v. Quintana, 70 F.3d 1167 (10th Cir. 1995).

Naming Violators/Interceptees

Government is required to name all individuals who it has probable cause to believe are engaged in the criminal activity under investigation and whose conversations it expects will be intercepted. Because this requirement does not play a central or functional role in guarding

against unwarranted use of Title III surveillance, suppression will not be invoked if this requirement is not met. U.S. v. Donovan, 429 U.S. 413 (1977).

The wiretap statute only requires that an application for a wiretap include "the identity of the person, if known, committing the offense and whose communications are to be intercepted." 18 U.S.C. 2518(1)(b)(iv). Likewise, the district court's authorization order must specify "the identity of the person, if known, whose communications are to be intercepted." 2518(4)(a). As the Supreme Court has recognized, "[t]he clear implication of this language is that when there is probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable, a wire interception order may, nevertheless, properly issue under the statute." U.S. v. Kahn, 415 U.S. 143 (1974). U.S. v. Killingsworth, 117 F.3d 1159 (10th Cir. 1997).

In cases where probable cause is doubtful as to some conversers, an investigative agency should be encouraged to name more, rather than fewer, persons in the application. The statute "describes those persons who must be named in the application"; "a judge (may) issue an authorization order upon a showing that probable cause exists with respect to an individual; it does not expressly require a similar showing with respect to each person named in the application." U.S. v. Martin, 599 F.2d 880 (9th Cir. 1979); U.S. v. Marcy, 777 F. Supp. 1400 (N.D. Ill. 1991); U.S. v. Bannerman, 2005 WL 2323172 (D. Mass.)(agreeing with Martin).

Regarding the use of court authorized video surveillance in the vehicles of City of Philadelphia plumbing inspectors, and appellant's claim that the Fourth Amendment required that probable cause supporting the video warrant must be particularized as to him, the Third Circuit said that neither the Fourth Amendment nor Title III proscribes the interception and use of audio or visual data of persons not specifically named in an application seeking judicial authorization of such interception. "As the Supreme Court explained in Donovan, so long as electronic interception is justified by probable cause that the facility or property through or at which the intercepted communication takes place is the means or situs of criminal activity, 'the failure to identify additional persons who are likely to be overheard engaging in incriminating conversations could hardly invalidate an otherwise lawful judicial authorization.'Donovan, 429 U.S. at 435 . . .[T]here is no question here that probable cause existed that plumbing inspectors were accepting cash payments from plumbers on inspection sites. The Fourth Amendment and Title III require nothing more. U.S. v. Urban, 404 F.3d 754 (3d Cir. 2005) (citing U.S. v. Donovan, 429 U.S. 413 (1977) ("It is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named."); U.S. v. Kahn, 415 U.S. 143 (1974) (rejecting interpretation of Title III requiring application for judicial authorization to "identify all persons, known or discoverable, who are committing the offense and whose communications are to be intercepted.") (internal quotation marks omitted)). See also U.S. v. Yannotti, 2005 WL 1231647 (S.D.N.Y.).

U.S. v. Ambrosio, 898 F. Supp. 177 (S.D.N.Y. 1995):

> Like the Fourth Amendment, the wiretap statute does not require that every person whose conversations are intercepted must be named in the application before evidence obtained by the wiretap can be used against him. See United States v. Hyde, 574 F.2d 856, 862 (5th Cir. 1978). Rather, the statute's conditions are satisfied as long as the affidavit names "an individual" for whom there is probable cause to suspect criminal activity. 18 U.S.C. s 2518(3)(a); Vastola, 670 F. Supp. at 1277; Rodriguez, 606 F. Supp. at 1370-71; Martin, 599 F.2d at 885.
>
> Furthermore, both the Fourth Amendment and the wiretap statute require the government to name those individuals for whom it has probable cause. United States v. Donovan, 429 U.S. at 428, 97 S.Ct. at 668 ("We therefore conclude that a wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in the criminal activity under investigation

and expects to intercept the individual's conversations over the target telephone."); United States v. Chiarizo, 525 F.2d 289, 292-93 (2d Cir. 1975); 18 U.S.C. §§ 2518(1)(b)(iv), (4)(a). The government must name persons suspected of criminal activity so that, upon expiration of the warrant, they may be given notice that their conversations were intercepted and the opportunity to review the conversations, application and order. 18 U.S.C. s 2518(8)(d). Since nothing in the statute restricts the government from naming in the affidavit individuals as to whom it may not have probable cause, the statute's goal of providing notice is actually furthered by naming more, rather than fewer, persons. See United States v. Martin, 599 F.2d at 885; United States v. Milan-Colon, 1992 WL 236218 (S.D.N.Y. 1992) (over-inclusion of persons in wiretap affidavit is not a cause for suppression but rather "furthers the policy of preventing unreasonable invasions of privacy" by ensuring that persons will be given notice of the order and intercepted communications).

[See also U.S. v. Trippe, 2001 U.S. Dist. LEXIS 5158 (S.D.N.Y.) (favorably citing Ambrosio)].

New York State court application of state law to suppress wiretap for failure to name violator/interceptee was without effect in federal court. Supreme Court in Donovan held that where wiretap meets Title III standards, "the failure to identify additional persons who are likely to be overheard engaging in incriminating conversations could hardly invalidate an otherwise lawful judicial authorization." U.S. v. Miller, 116 F.3d 641 (2d Cir. 1997).

Defendant failed to establish bad faith on government's behalf, much less any prejudice he suffered, when the government failed to name defendant in wiretap extensions due to a lack of knowledge of true identity of the defendant. U.S. v. Matthews, 213 F.3d 966 (7th Cir. 2000)(applying Donovan).

Because Stephen Edwards was not a named interceptee or a "named or known coconspirator," the interception of his conversations violated the limitations contained in the Title III order authorizing oral interceptions at the law office of Edwin Edwards. The illegal interceptions should have been suppressed, but the error was harmless. U.S. v. Edwards, 303 F.3d 606 (5th Cir. 2002).

Failure to name persons in the wherefore clause of the order does not amount to a substantial violation, given that the persons were named in the findings section of the order. No bad faith, no prejudice. No suppression. U.S. v. Bennett, 825 F. Supp. 1512 (D. Colo. 1993).

The mistaken naming of a person in an application does not warrant suppression. The probable cause requirement in the wiretap context is "satisfied by identification of the telephone line to be tapped and the particular conversations to be seized." U.S. v. Shipp, 578 F. Supp. 980 (S.D.N.Y. 1984). Neither the Fourth Amendment nor Title III requires that a Title III applicant establish probable cause as to every probable interceptee. U.S. v. Martin, 599 F.2d 880 (9th Cir. 1979); U.S. v. Pappas, 298 F. Supp.2d 250 (D. Conn. 2004); U.S. v. Greyling, 2002 WL 424655 (S.D.N.Y.); U.S. v. Labate, 2001 U.S. Dist. LEXIS 6509 (S.D.N.Y.); U.S. v. Bellomo, 954 F. Supp. 630 (S.D.N.Y. 1997); U.S. v. Ambrosio, 898 F. Supp. 177 (S.D.N.Y. 1995); U.S. v. Sorapuru, 902 F. Supp. 1322 (D. Colo. 1995); U.S. v. Milan-Colon, 1992 WL 236218 (S.D.N.Y.); U.S. v. McGuinness, 764 F. Supp. 888 (S.D.N.Y. 1991).

Use of the phrases "above-named persons" and "above-described telephones" in the decretal portion of the order to refer to specific information set out in the findings portion of the order satisfies the requirements of 2518(4)(a) and 2518(4)(c). U.S. v. Williams, 45 F.3d 1481 (10th Cir. 1995).

Particularity Requirement/Telephone Number/Premises

Neither Title III nor Fourth Amendment requires inclusion of telephone number to identify telephone line. 2518(4). The order did not list an unknown "bootleg" telephone number, but the clear purpose of the order was to tap all the telephones in the Bruno home. The addition or deletion of telephone numbers in the wiretap order had no constitutional or statutory significance. U.S. v. Feldman, 606 F.2d 673 (6th Cir. 1979), cert. denied, 445 U.S. 961 (1980).

No suppression is required for conversations obtained through a cell phone wiretap after the instrument (and thus the ESN), but not the telephone number, had been changed without the government's knowledge. The order mandated that "the authorization apply to any changed telephone number assigned to a telephone with the same electronic serial number as Target Telephone #7 . . . ." On January 22, 1997, the government was informed by the cellular provider that the telephone number for target Telephone #7 had been changed, but that the ESN had not been changed. Pursuant to the terms of the wiretap order, the agents continued to monitor Target Telephone #7. On January 27, 1997, however, unbeknownst to the law enforcement officers monitoring the phone, the subject purchased a new cell phone with a different ESN, deactivated the old cell phone and had the telephone number he acquired on January 22 assigned to the new phone. The district judge indicated that he would have had no hesitation about issuing an order continuing the intercept had he known that the ESN had changed because, regardless of the ESN, the telephone number on the new cell phone was clearly linked to the original number in the order. The language of the order is to the same effect. "By authorizing the continued interception of Target Telephone #7 even after the phone number changed, the issuing judge evidenced an intent to authorize interception of communications on any cell phone associated with the phone number identified in the order. The fact that the order only contemplated the possibility of changing telephone numbers, rather than changing ESNs, does not diminish the fact that he intended to, and on the basis of the government's application had the power to, authorize interception on any such cell phone during the period in question." Citing Feldman (see above), the court said that "the order's failure to identify the proper ESN for the intercepted phone, like the order's failure to identify the telephone number of the bootleg phone in Feldman, did not result in a failure to ensure that the surveillance would only occur in situations "clearly calling" for its use. To the contrary, the essential requirement of § 2518 that 'law enforcement authorities . . . convince a District Court that probable cause existed to believe that a specific person was committing a specific offense using a specific telephone,' Donovan, 429 U.S. at 437 n.25, was met. The phone over which the interceptions occurred was connected to the phone identified in the order and there was no bad faith on the part of the intercepting officers." U.S. v. Duran, 189 F.3d 1071 (9th Cir. 1999).

Citing U.S. v. Duran, 189 F.3d 1071 (9th Cir. 1999) for the proposition that ESN's are not required on wiretap applications, a S.D.N.Y. judge found that the failure of a Maryland State court's wiretap authorization order to identify the cellular phone by its electronic serial number does not warrant suppression of the evidence obtained therefrom as a matter of law. The Court also noted that:

> . . .although the wiretap order did not include the electronic serial number it did not identify the particular phone solely by the telephone number. Rather, the order identified the telephone as "the cellular telephone line ... [that] currently bears the telephone number 443-956-7217, or *any subsequent telephone number* or line assigned [to] Den Williams" . . . Thus, it appears that Maryland court recognized the fungibility of cellular telephone numbers and sought to specify that the wiretap authorization applied to the telephone itself, not simply the phone number currently assigned to it.

[It should be noted that the S.D.N.Y. court earlier quotes the state court wiretap order as authorizing interception over "... any subsequent number or line assigned, utilized by Den Williams." The court substitutes the bracketed "to" (see indented quote above) for the phrase

"utilized by" when it discusses the state court authorization language and by doing so appears to misinterpret the state court wiretap order as one limited to a single phone device rather than to "any subsequent number or line assigned, utilized by Den Williams" which would appear to be a grant of roving authority rather than simply an order authorizing a wiretap of a single cellular telephone device.] U.S. v. Otibu, 2002 WL 1033876 (S.D.N.Y.).

Citing the persuasive force of U.S. v. Duran, 189 F.3d 1071 (9th Cir. 1999), the Seventh Circuit, in companion unpublished opinions, agreed that it would be frivolous to argue on appeal that a new interception authorization was necessary when a wiretap subject switched his telephone number to a new cellular telephone bearing a different ESN where the original order specified both the telephone number and the ESN of the original phone. The language of the original authorization contained language almost identical to that in Duran–evidencing the judge's intent to authorize continued interception of any communication traceable to the original target number. U.S. v. Brown, 2002 WL 1357221 (7th Cir.)(unpublished); U.S. v. Jackson, 2002 WL 1357209 (7th Cir.)(unpublished).

Wiretap order applying to a target cellular telephone number and to any changed number subsequently assigned to the same ESN utilized by the target telephone and to any ESN subsequently assigned to the same telephone number utilized by the target cellular telephone, was not a "roving wiretap." A telephone number and ESN were specified with particularity and, therefore, there was no need to resort to 18 U.S.C. 2518(11)(b). U.S. v. Lutcher, 2004 WL 1274457 (E.D. La.).

Florida state wiretap was obtained in the course of a federal/state task force investigation. When the targeted cellular number was reported "out of service," an assistant states attorney immediately called the issuing state judge and advised the judge that the subject of the tap had changed his phone number. The judge verbally approved a change of the wiretap to the new number. The next morning, agents presented the judge with a one-page addendum to their original wiretap request (filed a week earlier) noting the telephone number change. They attached a copy of the original application and authorization. The Eleventh Circuit faced a similar challenge under the Florida wiretap law in U.S. v. Bascaro, 742 F.2d 1335 (11th Cir. 1984) (stating that federal courts must defer to state law on the question of the validity of wiretap orders "obtained by state law enforcement officers in state courts.") As the court explained in Bascaro:

> As distinguished from a change in residence, a change in telephone number only could not conceivably have affected the efficacy of the alternative investigative techniques. Nor . . . could such a change call into question the continued existence of probable cause . . . The naked formality of restating information in the amendment that would, in the context of this case, be necessarily identical in every respect to that presented one or two weeks before to the same circuit judge in the original application was not indispensable.

U.S. v. Glinton, 154 F.3d 1245 (11th Cir. 1998).

Title III does not require that a wiretap order identify the particular locations of various phone line extensions of the targeted line. 2518(1)(b), 2518(4). U.S. v. Escobar De Jesus, 187 F.3d 148 (1st Cir. 1999) (also holding that the identity of the person paying the phone bill is not legally significant to the Title III inquiry, and that subject's desire to use or not use the target phone has no relevance to the Title III inquiry).

See U.S. v. Dorfman, 542 F. Supp 345 (N.D. Ill. 1982) for discussion of particularity requirement.

Although a Title III application must contain a "particular description" of the premises, courts have not required that the application disclose the exact location of where listening devices will be placed. A Title III application satisfies the particularity requirement by using a street address and description of the building. The focus of the Court's analysis should be to determine whether the Title III order gave the FBI sufficient information to determine what communications they were authorized to intercept and where they were authorized to intercept them. U.S. v. Lambert, 771 F.2d 83 (6th Cir. 1985); U.S. v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990). U.S. v. Sparacio, Nos. 95-2053 and 96-1616 (3d Cir. 7/28/98) (unpublished)(government did not need to establish probable cause that the interceptees' relevant conversations would occur in Avena's (lawyer target) private office as opposed to in the law office suite in general).

Title III order to intercept oral communications at “law office of Edwin Edwards” includes the entire group of offices at that address, not merely the personal office of Edwin Edwards. U.S. v. Edwards, 303 F.3d 606 (5th Cir. 2002).

The government's applications, which identify the target premises as "within and in the vicinity of" Chan Wing Yeung's office, satisfy the particularity requirement of the fourth amendment, and the surveillance conducted through the reception area bug pursuant to court orders authorizing surveillance "within and in the vicinity of" Chan Wing Yeung's office did not violate such orders. U.S. v. Yeung, 1996 WL 31235 (E.D.N.Y.).

“The government's warrant provided that ‘to intercept the oral communications occurring at the Visitor Areas located at the Vienna Correction Facility . . . [the government] may make all necessary surreptitious entries to effectuate the purposes of this order, including but not limited to entries to install, maintain and remove electronic listening devices within the Visitation Area located at the Vienna Correctional Facility.’ Based on this language, the scope of the warrant does not preclude the use of wiretaps inside visitors' name-tags for the purpose of intercepting the oral communications occurring in the Visitor Areas of the Vienna Correction Facility.” Branch v. U.S., 2004 U.S. Dist. LEXIS 5836 (N.D. Ill.); Shell v. U.S., 2004 U.S. Dist. LEXIS 16382 (N.D. Ill.) (citing Branch).

Previous Applications

The duty to disclose prior applications under 2518(1)(e) covers all persons named in the application and not just those designated as "principal targets." U.S. v. Bianco, 998 F.2d 1112 (2d Cir. 1993).

"It is simply incorrect as a matter of law that an applicant for an eavesdropping warrant must make inquiries of other law enforcement agencies as to other eavesdropping applications when there is no evidence to suggest that any such eavesdropping applications have ever been made." U.S. v. Persico, 1994 WL 36367 (E.D.N.Y.).

Inadvertent failure under 2518(1)(e) to disclose prior application does not require suppression. U.S. v. Callum, 410 F.3d 571 (9th Cir. 2005); U.S. v. Lujan, 936 F.2d 406 (9th Cir. 1991) (citing U.S. v. Zannino, 895 F.2d 1 (1st Cir. 1990); U.S. v. Pinelli, 890 F.2d 1461 (10th Cir. 1989); U.S. v. Van Horn, 789 F.2d 1492 (11th Cir. 1986)); U.S. v. Bennett, 825 F. Supp. 1512 (D. Colo. 1993); U.S. v. Luong, CR-96-0094 MHP (N.D. Cal. 9/7/99).

The failure of Title III applications to disclose prior applications was inadvertent. Agents testified that three separate searches of FBI and DEA databases failed to disclose the prior

applications. A later search revealed the prior applications under another name. Since the government did not act in bad faith, the district court did not err in denying the motion to suppress. U.S. v. Ceballos, 302 F.3d 679 (7th Cir. 2002)(citing Zannino, Lujan and Pinelli).

The failure of the government to disclose prior electronic surveillance applications was a violation of 2518(1)(e), but 2518(1)(e) is not central to Title III, and the government's nondisclosure was a good faith error, therefore suppression is not appropriate. U.S. v. Bianco, 998 F.2d 1112 (2d Cir. 1993).

Intentional noncompliance with 2518(1)(e) requires suppression. U.S. v. Bellosi, 501 F.2d 833 (D.C. Cir 1974).

Wiretap evidence suppressed because of individual and institutional reckless non-compliance with section 2518(1)(e). U.S. v. Luong, No. CR-94-0094 MHP (N.D. Cal. 7/14/98)(unpublished).

Alternative Investigative Showing

The necessity requirement "is simply designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." U.S. v. Kahn, 415 U.S. 143, 153 n.12 (1974).

Former DOJ Criminal Division AAG, now Judge Stephen Trott, writes on behalf of a Ninth Circuit panel firmly reversing a Central District of California judge's "necessity"-based suppression of wiretap evidence in a major drug conspiracy case. "We are unable to discern anything missing from the affiant's affidavit, and we see nothing in it that justifies the district court's characterization of any part of it as 'boilerplate.' A judicially-imposed requirement that the government attempt to use all potential informants before securing a wiretap would be impractical and contrary to investigatory experience and the force of our precedent. The government need not prove that informants would be totally useless." Trott's opinion is comprehensive and unequivocal in its holding that the agent's Title III affidavit contained a full and complete statement of the facts and that the necessity for the wiretap was clearly established in light of the government's interest in establishing the full scope of the conspiracy, the added difficulty, expense and danger involved in the use of informants to investigate and prosecute persons engaged in clandestine criminal activity, and the critical role wiretap evidence plays in corroborating informant testimony and in ensuring that what investigators are told by the informants is accurate. U.S. v. Canales-Gomez, 358 F.3d 1221 (9th Cir. 2004). See also U.S. v. Fernandez, 388 F.3d 1199 (9th Cir. 2004)(recognizing the "common sense approach" to the necessity issue adopted by the Ninth Circuit in Canales-Gomez).

The district court did not abuse its discretion in finding that the Title III wire, oral and electronic (fax) surveillance of the Montana Freemen during their attempt to establish their own government and financial system was necessary. The Montana Freemen conspiracy was widespread and dangerous. Infiltration alone could not determine the scope of it. The rigor of the government's investigation should fit the threat posed to society by criminals' illicit and coordinated plans. Conspiracies pose a greater threat to society than individual action towards the same end and therefore the government is entitled to more leeway in its investigative methods when it pursues a conspiracy. "The existence of an indictment does not make wiretapping unnecessary." A wiretap can gain evidence to make a prosecution more effective (evidence of guilt beyond a reasonable doubt) and/or gather evidence against those who have not

yet been indicted. U.S. v. McGuire, 307 F.3d 1192 (9th Cir. 2002); U.S. v. Hoang Ai Le, 255 F. Supp.2d 1132 (E.D. Cal. 2003)(following McGuire).

Wiretap affidavit in Mexican Mafia case was sufficient to support a reasonable judge's conclusion that the necessity requirement was satisfied. The Mexican Mafia is a broad-based organization with several hundred members and an unknown number of associates. Several informants–including former members of the Mexican Mafia–could not possibly reveal the full nature and extent of the enterprise and its countless criminal tentacles. A Franks hearing was correctly denied because appellants failed to make a substantial showing that the government made intentional or reckless misrepresentations or omissions, and even if the government made such statements or omissions, they were not material to the district court's finding of necessity). U.S. v. Shryock, 342 F.3d 948 (9th Cir. 2003). See also U.S. v. Fernandez, 388 F.3d 1199 (9th Cir. 2004) (related Mexican Mafia case); U.S. v. Martinez, 2004 WL 2998706 (9th Cir.) (unpublished)(citing Shryock).

"Because the defendants made an adequate initial showing of intentional or reckless material misrepresentations or omissions in the wiretap application, the district court did not err in holding a Franks hearing." U.S. v. Gonzalez, Inc., 412 F.3d 1102 (9th Cir. 2005).

The alternative investigative showing must address the particulars of the instant investigation. U.S. v. Kalustian, 529 F.2d 585 (9th Cir. 1975). Spin-off must contain new particularized showing. U.S. v. Santora, 600 F.2d 1317 (9th Cir. 1979).

A Ninth Circuit panel (2-1) suppressed a wiretap application because it contained material misstatements and omissions regarding the necessity for the wiretap, and when purged of such misstatements and omissions, the application contained only generalized statements that would be true of any narcotics investigation and was bereft of specific facts necessary to satisfy the requirements of 2518(1)(c). The instant application was found to be nearly identical to an earlier wiretap application targeting a codefendant. It appears that no investigation was targeted specifically on the defendant who was the target of the instant wiretap. The Court found that statements regarding previous compromised surveillance activities and the usefulness of informants were untrue and worked to conceal the fact that the wiretap was not necessary. The Court concluded with the following words:

> That pen registers do not reveal the identity of callers; that drug dealers know it is in their best interest to reveal as little as possible; that witnesses cannot lead to the prosecution of an entire drug organization; and that traditional investigative methods do not reveal all are generic problems of police investigation. Their generic nature does not dissipate simply because the government claims a vast investigative purpose. Wiretaps themselves could little achieve the investigative goals stated in the government's application. The government may not cast its investigative net so far and so wide as to manufacture necessity in all circumstances. Doing so would render the requirements of § 2518 nullities.

U.S. v. Blackmon, 273 F.3d 1204 (9th Cir. 2001). See also U.S. v. Fernandez, 388 F.3d 1199 (9th Cir. 2004) (a Mexican Mafia case in which the district court's decision not to suppress was affirmed, but the 9th Circuit noted that portions of the affidavits (particularly the sections discussing pen/trap information and trash searches) suffered the same flaws highlighted in Blackmon: the inclusion of statements that are "nothing more than a description of the inherent limitations" of particular investigative techniques).

The issuing court abused its discretion in concluding that the government established necessity for the wiretap. The government made limited use of traditional and potentially productive investigative methods and did not sufficiently allege that these strategies were reasonably unlikely to succeed or were too dangerous to try. U.S. v. Gonzalez, Inc., 412 F.3d 1102 (9th Cir. 2005).

"We conclude that Title III prohibits monitoring cloned cell phones without a court order." Therefore, the omission of such an illegal investigative strategy from the wiretap application does not detract from the finding of necessity. U.S. v. Staves, 383 F.3d 977 (9th Cir. 2004).

Defendants' claim that CI's cooperation in investigation of LCN controlled securities fraud scheme made electronic surveillance (office bugs) unnecessary was rejected by the court because the affiant's alternative investigative statement showed the danger (physical violence, firearms, a murder) of placing a recording device on the CI, the impracticality of installing such a device on the CI due to battery time limitations, the lack of notice prior to meetings, and the possibility of illegal intercepts if the device was installed in the CI's briefcase. The electronic surveillance furthered the objectives of the investigation by corroborating the CI's statements and ensured the credibility of the fruits of the investigation, which was especially important where the principal (or maybe only) evidence of certain alleged schemes is an evanescent conversation among members of the charged enterprise. The affiant noted that the secretive nature and scope of the enterprise made it less susceptible to conventional investigative techniques. It was not possible for an outsider to infiltrate the Bonnano Crime Family. The subjects were very surveillance conscious. It was also possible that the CI might periodically be absent from meetings or conversations might occur out of ear-shot. U.S. v. Labate, 2001 U.S. Dist. LEXIS 6509 (S.D.N.Y.).

The necessity provision (2518(1)(c)) is constitutional in origin. U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999).

"Each wiretap, including extensions of existing wiretaps, must be separately justified as "necessary" in light of the facts of the particular case." Affidavit for wiretap #3 was silent as to any subsequent physical surveillance or other follow-up through normal investigative techniques in connection with the interception of significant communications during Wiretap #2. The affidavit for wiretap #3 was a nearly verbatim repeat of the affidavit in support of wiretap #2, with no mention of the information gathered during wiretap #2. Wiretap #4 was the least justified of all. By the time of the application, the defendant had been arrested, found in possession of $100,000 in cash, 3 kilos of cocaine and 25 pounds of marijuana and his home was searched pursuant to warrant. The affidavit for wiretap #4 was largely a rehash of the same sections from previous affidavits. Some of the information was clearly stale. The affidavit claimed that several normal investigative techniques, such as subpoenas, search warrants and grand jury investigation, couldn't be used because that "would alert" others that an investigation was going on. At the same time, the affidavit acknowledged that news of the arrest had spread quickly throughout the relatively small community and that the other subjects knew that the defendant was the subject of a federal investigation. The affidavit was absolutely silent about any attempt to question the various other individuals implicated in the investigation even though it would appear an opportune time, with news of the arrest of the kingpin, to interrogate his associates who might well be more than ready to minimize their own exposure. The affidavits in wiretaps #3 and #4 failed to establish that the continuation of the wiretap was "necessary" and therefore the evidence gathered therefrom should be suppressed. U.S. v. Williams, 2000 WL 1273407 (E.D. La.)

"One can always argue that more should have been done or that investigators should have been more patient with other methods. Courts have routinely rejected such arguments challenging similar affidavits providing reasonable and specific explanations as to why other investigative techniques appeared too dangerous or unlikely to succeed." U.S. v. Greer, 2004 U.S. Dist. LEXIS 20253 (S.D. Ind.).

The government need not use every available incentive to induce informants to testify, such as offering protective custody, before seeking a wiretap order. Rather, the government's affidavit need only indicate a reasonable likelihood that alternative techniques would fail to fully expose the crime. Indelicato v. U.S., 106 F. Supp.2d 151 (D. Mass. 2000)(citing U.S. v. Scibelli, 549 F.2d 222 (1st Cir. 1977) and U.S. v. Ashley, 876 F.2d 1069 (1st Cir. 1989)).

The necessity requirement does not mandate that the government organize the release of jailed informants before a wiretap will be authorized. U.S. v. Staves, 383 F.3d 977 (9th Cir. 2004); U.S. v. Canales-Gomez, 358 F.3d 1221 (9th Cir. 2004).

Defendants' argument that there was no need for the wiretaps because the government had already developed abundant evidence against them through alternative investigative techniques fails because the wiretaps targeted the entire conspiracy, not just these defendants. U.S. v. O'Neal, 2000 WL 328110 (9th Cir. 3/24/00) (unpublished).

Wiretap of defendant's cellular telephone, the virtual "nerve center" of a widespread, interstate drug conspiracy was necessary to establish the full scope of the criminal enterprise, notwithstanding what the defendant claimed to be great success by the government in penetrating the criminal enterprise through cooperating individuals and physical surveillance. U.S. v. Washington, 2004 U.S. App. LEXIS 22020 (6th Cir.)(unpublished).

The police need not exhaust every conceivable technique before making an application for a wiretap. U.S. v. Staves, 383 F.3d 977 (9th Cir. 2004); U.S. v. Bankston, 182 F.3d 296 (5th Cir. 1999); U.S. v. Barnes, 47 F.3d 963 (8th Cir. 1995); U.S. v. Clerkley, 556 F.2d 709 (4th Cir. 1977) (quoting 1968 U.S. Code, Cong. & Admin. News 2112, 2190); U.S. v. Wilson, 2002 WL 31236320 (4th Cir.)(Title III authorization permissible even if there exists sufficient evidence to arrest and prosecute the main conspirators; citing Clerkley.).

New York State trooper's wiretap affidavit did not satisfy the necessity requirements of either the New York or federal wiretap statutes. The affidavit disclosed a successful undercover purchase from defendant who was not apprehensive about dealing with the undercover officer and telling the undercover officer to call later to check on the status of proposed future drug purchases. The affidavit did not reveal what, if any, investigative techniques were attempted prior to the wiretap request. U.S. v. Lilla, 699 F.2d 99 (2d Cir. 1983).

The burden that these provisions impose upon the government to show the inadequacy of normal investigative techniques is not great, and the adequacy of such a showing is to be tested in a practical and common sense fashion that does not hamper unduly the investigative powers of law enforcement agents. The government may not make the required showing through a mere boilerplate recitation, but must base its need on real facts and must specifically describe how, in the case at hand, it has encountered difficulties in penetrating the criminal enterprise or in gathering evidence with normal techniques to the point where wiretapping becomes reasonable. U.S. v. Oriakhi, 57 F.3d 1290 (4th Cir. 1995).

The appellate court reviews de novo whether a "full and complete statement" was submitted under 2518(1)(c) and reviews the issuing judge's conclusion under 18 U.S.C. 2518(3)(c) that a wiretap is necessary for an abuse of discretion. U.S. v. Staves, 383 F.3d 977 (9th Cir. 2004); U.S. v. Melton, 2005 WL 1127126 (3d Cir.)(unpublished); U.S. v. Barnett, 2003 U.S. App. LEXIS 6953 (4th Cir.)(unpublished); U.S. v. Ramirez-Encarnacion, 291 F.3d 1219 (10th Cir. 2002)(resolving conflict within circuit and bringing it into accordance with majority of other circuits (see footnote 1 citing other circuits)); U.S. v. Bennett, 219 F.3d 1117 (9th Cir. 2000); U.S. v. Oregon-Cortez, 244 F. Supp.2d 1167 (D. Col. 2003) (applying to the district court the

Ramirez-Encarnacion 2518(1)(c)and 2518(3)(c) review standards); U.S. v. Mack, 272 F. Supp.2d 1174 (D. Col. 2003)(agreeing with district judge in Oregon-Cortez and denying motion to suppress).

The First Circuit applies a unitary standard of review in §2518(1)(c) cases: "When reviewing the government's showing of necessity, our role is not to make a de novo determination of sufficiency as if [we] were [the issuing judge], but to decide if the facts set forth in the application were minimally adequate to support the determination that was made. . .The last affidavit, seeking authorization to wiretap a telephone line over which officers expected to hear 'vital information' on a large cocaine delivery expected to occur the next day, incorporates by reference the statement of necessity set out in a prior (attached) affidavit, instead of setting out a fresh one. Despite [defendant's] characterization of the affidavits as consisting largely of "boilerplate," all the affidavits did contain much that was concrete and pertained to this specific investigation. . .The officer applying for the wiretap authorization stated near the beginning of each affidavit:

> Since this Affidavit is being submitted for the limited purpose of securing an order authorizing the interception of wire communications, I have not included details of every aspect of this investigation to date. Facts not set forth herein are not being relied on in reaching my conclusion that an order should be issued.

The requirement of a full and complete statement cannot possibly mean that every single detail, even if relevant to the wiretap, must be included. The plain language of §2518(1)(c) only requires a full and complete statement 'as to' the crucial issue: 'whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried.'. . . Many aspects of an investigation, especially in a large, complex case like this one, will not be relevant to the question of whether a particular wiretap is necessary. And even if there is some relevance, the officer need not detail every single fact, so long as sufficient facts are described as to the crucial issue and material contrary facts are not omitted. If there are relevant and material omissions, the issuing judge may deny the application or seek additional information, or the defendant may seek a Franks hearing. . . Nor is the government forced to run outlandish risks or to exhaust every conceivable alternative before requesting authorization for electronic surveillance." U.S. v. Yeje-Cabrera, 2005 WL 2868315 (1st Cir.).

In reviewing the validity of an electronic surveillance order, "great deference" is accorded the determinations of the issuing judge. "Thus, the fact that a later trial judge or reviewing court may feel that a different conclusion was appropriate does not require, nor even authorize, the suppression of evidence gained through such a warrant." The purpose of the necessity requirement "is not to foreclose electronic surveillance until every other imaginable method of investigation has been unsuccessfully attempted, but simply to inform the issuing judge of the difficulties involved in the use of conventional techniques." U.S. v. Corrado, 227 F.3d 528 (6th Cir. 2000).

Defendants failed to satisfy the Franks requirements to obtain a hearing. They did not present the district court with any affidavits to support their claim that the affidavit was false in any respect. They merely argued that electronic surveillance was not necessary under the circumstances. The mere fact that some investigative techniques were successful in uncovering evidence of wrongdoing does not mandate that a court negate the need for wiretap surveillance. Wiretapping is particularly appropriate when the telephone is routinely relied on to conduct the criminal enterprise under investigation. It did not appear that the government could have uncovered the full scope of the conspiracy, especially not in a relatively safe manner, without the wiretaps. U.S. v. Stewart, 306 F.3d 295 (6th Cir. 2002).

The mere attainment of some degree of success during law enforcement's use of traditional investigative methods does not alone serve to extinguish the need for a wiretap. A paid informant's willingness to participate in the investigation does not necessarily indicate that further use of this traditional technique could be productive and thereby nullify the government's claim of necessity. A paid informant's credibility would be under attack and would therefore require further corroborating evidence. U.S. v. Bennett, 219 F.3d 1117 (9th Cir. 2000).

When evaluating the effectiveness of other investigative techniques, the government and the court are entitled to consider the heavy burden of proof beyond a reasonable doubt and the potential avenues left open for defense. U.S. v. Soto-Nava, 2002 WL 432084 (S.D. Ind.)(citing U.S. v. Plescia, 48 F.3d 1452 (7th Cir. 1995)).

18 U.S.C. 2518(3)(c) only requires that the court make a determination that the statutory necessity standard has been met, and does not require the sort of detailed factual findings required under Rule 52 of the Federal Rules of Civil Procedure. U.S. v. Soto-Nava, 2002 WL 432084 (S.D. Ind.).

Section 2518(1)(c) does not require exhaustion of normal investigative techniques; rather, it requires only "that the agents inform the authorizing judicial officer of the nature and progress of the investigation and the difficulties inherent in the use of normal law enforcement methods." U.S. v. Torres, 901 F.2d 205 (2d Cir. 1990); U.S. v. Diaz, 176 F.3d 52 (2d Cir. 1999); see also U.S. v. Khan, 993 F.2d 1368 (9th Cir. 1993).

It is sufficient that the government show that other techniques are impractical under the circumstances and that it would be unreasonable to require pursuit of those avenues of investigation. U.S. v. Vento, 533 F.2d 838 (3d Cir. 1976); U.S. v. Melton, 2005 WL 1127126 (3d Cir.)(citing Vento)(unpublished).

Five month's worth of wiretap evidence was suppressed because the affiant withheld information and misrepresented facts to the issuing judge with regard to the adequacy of alternative investigative techniques. "When the deceptive character of the affidavit is considered in light of the agent's conduct at the evidentiary hearing, a pattern of behavior intended to obtain and protect the wiretap emerges and shows that the government acted without respect for the necessity requirements of § 2518(1)(c)." U.S. v. Ailemen, 986 F. Supp. 1228 (N.D. Cal. 1997).

There are circumstances in which information known to one agent, but not communicated to an affiant, may be attributable to the affiant despite his actual ignorance. See, e.g., U.S. v. Sullivan, 586 F.Supp. 1314, 1319 (D. Mass. 1984) (denying suppression because "[t]here is no evidence in this case that the government intentionally concealed information from the court [by choosing an ignorant applicant.] If such showing had been made, we would have a different case."); U.S. v. Tufaro, 593 F. Supp. 476, 485 (S.D.N.Y. 1983) (holding that a subordinate's knowledge would be attributed to the affiant, who was his supervisor). See also U.S. v. Donovan, 429 U.S. 413, 435 n. 23 (stating that "There is no suggestion in this case that the Government agents failed to identify [all of those likely to be heard in incriminating conversations] for the purpose of keeping relevant information from the District Court that might have prompted the court to conclude that probable cause was lacking. If such a showing had been made we would have a different case."). U.S. v. Salemme, 1997 WL 810057 (D. Mass. 12/29/97).

The federal district court in Boston conducted lengthy suppression hearings concerning the FBI's relationship with top echelon informants and their use in connection with Title III surveillance in the investigation of the Boston LCN. The court criticized the FBI for disregarding its "legal obligation of candor" to the court in its Title III applications, and

criticized the DEA and the United States Attorney for their failure to extract material informant information from the FBI prior to requesting Justice Department authorization of Title III applications:

> Blinded by its determination not to confirm for the United States Attorney's Office or the DEA the accuracy of their understanding that Bulger and Flemmi were FBI informants, the FBI recklessly disregarded the government's legal obligation of candor to the court when applying for authority to conduct electronic surveillance in what was represented to be a joint investigation. At the same time, believing that Bulger and Flemmi were FBI informants, but accepting that the FBI would not confirm or discuss their status, the DEA and the United States Attorney's Office recklessly disregarded their legal obligation to seek from the FBI information that, if shared with them, would have resulted in the applications for electronic surveillance now at issue not being filed, let alone approved by the court. The DEA and United States Attorney's Office also acted with reckless disregard for the truth when they filed applications for warrants that in effect represented that electronic surveillance was necessary to obtain evidence that the FBI would use in a Title 18 investigation of Bulger, Flemmi, and others because the prosecutor who was the applicant and the DEA agent who was the affiant did not believe that the FBI would attempt to do so. Rather, they understood that Bulger and Flemmi were FBI informants who the Bureau wished to protect rather than prosecute.
>
> As a result, the applications for the 1984-1985 electronic surveillance targeting Bulger and Flemmi failed to include the "full and complete statement" describing the necessity for electronic surveillance that was required by 18 U.S.C. § 2518(1)(c). More specifically, the applications should have included certain material facts about the targets, including the following. As informants Bulger and Flemmi had made statements about their illegal gambling and loansharking that the government now claims can be used as evidence against them. A review of their files would indicate to the FBI that they were tacitly authorized to engage in such activities. Therefore, the conduct which the government was seeking authority to utilize a wiretap to investigate may not have been criminal. In any event, the FBI did not intend to use any evidence generated by the electronic surveillance in an attempt to develop a prosecutable case against its sources or any of the other named targets, including Kaufman. Moreover, the FBI agent who was most knowledgeable believed that Bulger and Flemmi were not involved in narcotics crimes, but may have mistakenly given that impression while seeking information for the Bureau. No reasonable judge would have granted any request to target Bulger and Flemmi based on an application containing this information.
>
> In fact, if properly informed, the Assistant Attorney General would not have authorized the filing of the application for a warrant at all. The Department of Justice would not have allowed the submission to the court of an application that it knew was false and misleading. Nor would it have, over the FBI's inevitable objection, permitted disclosure to the court, and possibly to potential defendants, of the fact that Bulger and Flemmi were FBI informants. The testimony of DEA SAC Robert Stutman, among other things, indicates that if the DEA had been candidly consulted, it would have deferred to the FBI's interest in Bulger and Flemmi, and abandoned its investigation.

U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999).

A DEA agent working on an OCDETF with an FBI agent had a duty to disclose to the FBI agent all information material to the FBI agent's application for a wiretap. It is as a representative of the government that an applicant for wiretap authorization applies to the court. The government cannot so compartmentalize its activities that it hides from the court information that might be relevant. If the DEA agent had material facts, the duty to disclose was enforceable by the AUSA going to the agent's superiors and obtaining the reports. The DEA agent's intentional failure to disclose is attributable to the FBI affiant. The motive for withholding the information is not relevant. Suppression is not warranted, however, because the nondisclosure of the DEA information ("the bane of government agencies charged with overlapping tasks sometimes more zealous in protecting their turf than in achieving the common objective") in the original FBI Title III affidavit and an inaccurate and misleading statement and omission in an extension affidavit were not material. If the omitted information had been added to the original affidavit and the misleading statement and omission corrected in the extension affidavit, an impartial judge would still have seen the necessity of the wiretaps to "knock out the entire organization."

U.S. v. Aviles, 170 F.3d 863 (9th Cir. 1998). See also U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999)(citing Aviles).

In light of the Title III necessity issues (government failed to reveal existence of confidential informants) being vetted in the ongoing Salemme prosecution in the same district, a Massachusetts federal district judge denied the government's motion to delete the following handwritten language entered by the judge into the margin of a wiretap order he issued:

> "This order is entered on the express representation that there are no other informants presently known to the government knowledgeable of the matters contained herein. If that representation is inaccurate, this order is of no force and effect."

In re Application for Interception of Wire Communications, 2 F. Supp.2d 177 (D. Mass. 1998).

"Necessity" statement should "demonstrate that the government has made a reasonable, good faith effort to run the gamut of normal investigative procedures" before resorting to an electronic interception order. U.S. v. London, 66 F.3d 1227 (1st Cir. 1995).

“There is no rule on the amount of time investigators must try and fail, using other methods, before turning to a wiretap application. . . The issuing judge had the relevant information and was able to weigh the amount of prior investigation among other relevant factors in reaching a decision on the necessity of the wiretap. U.S. v. Nelson-Rodriguez, 319 F.3d 12 (1st Cir. 2003).

“With the government still unaware of the identity of many of the conspiracy's members as well as the organizational structure of the conspiracy, the district court could permissibly allow the government to employ electronic surveillance to uncover the complete range of operations of the target conspiracy.” U.S. v. Villarman-Oviedo, 325 F.3d 1 (1st Cir. 2003); U.S. v. Bannerman, 2005 WL 2323172 (D. Mass.)(citing Villarman-Oviedo).

“The government provided the issuing judge with specific factors--particularly the DEA's inability to identify key conspiracy members and the conspiracy's growing awareness of law enforcement activity--that militated in favor of using a more drastic investigative tool.” U.S. v. Lopez, 300 F.3d 46 (1st Cir. 2002).

The requisite 18 U.S.C. 2518(1)(c) “full and complete” necessity statement was provided in wiretap applications that provided the factual bases for the government’s claim that wiretaps were needed to establish the full extent of the drug conspiracy, that informants and agents could not infiltrate the conspiracy, that telephone records and pen registers could not identify the users or reveal the communications, and that physical surveillance would alert the subjects to the investigation. U.S. v. Ceballos, 302 F.3d 679 (7th Cir. 2002). See also U.S. v. Dumes, 313 F.3d 372 (7th Cir. 2002) (citing Ceballos; necessity review standard is abuse of discretion; government burden not high); U.S. v. Price, 418 F.3d 771 (7th Cir. 2005)(citing Ceballos).

The wiretap was necessary to fill the gaps, secure critical evidence against all of the subjects in an intricate investigation of a large and dangerous drug conspiracy, gauge the depth and scope of the conspiracy, and avoid the logistical quandary of prosecuting each defendant individually. U.S. v. Fudge, 325 F.3d 910 (7th Cir. 2003).

Congress did not intend the statutory phrase "normal investigative procedures" to include electronic eavesdropping techniques. U.S. v. Castillo-Garcia, 117 F.3d 1179 (10th Cir. 1997); U.S. v. Bianco, 998 F.2d 1112 (2d Cir. 1993); U.S. v. Uribe, 890 F.2d 554, (1st Cir. 1989); U.S. v. Lambert, 771 F.2d 83 (6th Cir. 1985).

The district court suppressed four Title III spin-offs (four phones and two pagers) for failure to satisfy the necessity requirements of 2518(1)(c), 2518(3)(c). The Tenth Circuit reversed as to all targeted facilities but one pager and one telephone used by a subject as to whom the government had not made "a full and complete" necessity statement in a particularized manner. "Even with an ongoing investigation of a suspected drug conspiracy, the government may not simply move swiftly from wiretap to wiretap. Rather, under Title III, it must always pause to consider whether normal investigative procedures could be used effectively, particularly in light of any evidence obtained as a result of each succeeding wiretap."

> [T]o obtain an electronic surveillance order, the government must explain fully in its application what investigative techniques have been tried against the target of the wiretap. 18 U.S.C. §§ 2518(1)(c), 2518(3)(c). If any of the four categories of normal investigative techniques referred to in the legislative history of Title III have not been tried, the government must explain with particularity why each of such untried techniques would be either unsuccessful or too dangerous. Those investigative procedures are: (1) standard visual and aural surveillance; (2) questioning and interrogation of witnesses or participants (including the use of grand juries and the grant of immunity if necessary); (3) use of search warrants; and (4) infiltration of conspiratorial groups by undercover agents or informants. In addition, if other normal investigative techniques such as pen registers or trap and trace devices have not been tried, a similar explanation must be offered as to why they also would be unsuccessful or too dangerous. We add pen registers and trap and trace devices to this list because they possess a logical relationship and close affinity to wiretaps and yet are less intrusive. Thus, unless the government can show that they would be ineffective or dangerous they must be tried before resorting to wiretaps. Whether other normal investigative techniques must also be explored before turning to wiretaps will depend on the unique circumstances of each investigation.

U.S. v. Castillo-Garcia, 117 F.3d 1179 (10th Cir. 1997). Accord U.S. v. Killingsworth, 117 F.3d 1159 (10th Cir. 1997)(holding wiretap application "necessity" showing sufficient; filed same day as Castillo-Garcia and citing "necessity" standard articulated in Castillo-Garcia).

The Tenth Circuit affirmed the suppression of all Title III evidence (original and one extension order targeting Arrington's pager; original and one extension order targeting Arrington's cellular telephone) because the affidavit failed to discuss or pursue reasonable alternative investigative methods which were suggested by the facts of the investigation:

> Our concern here is the sufficiency of the affidavit with regard to reasonable investigatory methods in light of the facts discussed in the affidavit. Agent Wilcox states in his affidavit that (1) Arrington told officers he worked at Hightower and Shorty's Used Cars in Commerce City, Colorado; (2) Arrington drove automobiles registered to Hightower and Shorty's Used Cars to meetings with CS-1 for controlled purchases; (3) Arrington used a cell phone for which the billing party was Joe Hightower; (4) Arrington left a meeting with CS-1 and went to the residence of Hightower; (5) Hightower was known by the FBI to have consented to a search of his residence, and in 1996, cocaine, a gun and $13,425 in currency were seized from Hightower's business; (6) Hightower had an extensive record including three arrests for possession of dangerous drug; (7) Hightower is the owner of Hightower and Shorty's Used Cars; (8) Hightower had been identified as a dealer of cocaine and crack cocaine in the Denver area; (9) surveillance was conducted one time at Hightower and Shorty's Used Cars; and (10) numbers traced to Hightower or Hightower and Shorty's showed up numerous times on pen register records for Arrington's phone numbers. Despite the significant amount of information in the affidavit connecting Hightower to the investigation, the statement of the need for interception completely fails to mention any standard investigative methods that were considered with respect to Hightower, or any reasonable investigative methods that would follow from the information included about Hightower.
>
> The shortcomings of the affidavit with respect to reasonable investigative methods that might have been suggested by the evidence that implicated Hightower were amplified with the testimony of Agent Wilcox at the suppression hearing. Agent Wilcox admits no attempts were made to (1) get a search warrant for Hightower's house; (2) secure a statement from Hightower; (3) conduct

> surveillance on him personally; (4) use roving interceptors or mobile tracking devices on him; (5) interview any of his relatives, friends or former employees; or, (6) investigate his tax records.
>
> In light of the above facts, we do not find that the ultimate factual conclusion of the trial court, that the government failed to adequately address its failure to resort to other reasonable investigative methods, and that there was no demonstration that these reasonable investigative methods were unlikely to succeed, was clearly erroneous. Moreover, because the "necessity showing" for the first wiretap was insufficient, we find that the necessity showing for the subsequent wiretaps was insufficient as well.

U.S. v. Arrington, 2000 WL 775576 (10th Cir. 3/29/00) (unpublished).

Government is required to make specific necessity showings only as to the primary targets of the wiretap. A primary target may be the conspiracy or criminal enterprise itself. U.S. v. Barrios, 994 F. Supp. 1257 (D. Colo. 1998); U.S. v. Carrillo, 123 F. Supp.2d 1223 (D. Colo. 2000) (Contains good review of "necessity" jurisprudence in Tenth Circuit. Notes that Arrington court (see above) did not reveal whether Hightower was a primary target of the wiretap application). See also U.S. v. Mitchell, 274 F.3d 1307 (10th Cir. 2001)(18 U.S.C. 2518(1)(b)(iv) does not require that the necessity requirement of 2518(1)(c) be shown as to all named interceptees. In U.S. v. Donovan, 429 U.S. 413 (1977), the Supreme Court held that Congress did not intend that 2518(1)(b)(iv) play "a central, or even functional, role in guarding against unwarranted use of wiretapping or electronic surveillance.").

"Although an extension affidavit must demonstrate the necessity of ongoing surveillance, it need not set forth different information from that which is presented in the original application. Duplication may be unavoidable, in fact, where the basis for necessity remains unchanged over the course of an authorization period." U.S. v. Parks, 1997 WL 136761 (N.D. Ill.).

"Most of the assertions would be true in any drug investigation. . . .The only reason given that was specific to this particular investigation was that the suspects kept the trash container for the residence on the front porch, making it impossible for agents to search the garbage. Although some of these assertions might appear boilerplate, the fact that drug investigations suffer from common investigatory problems does not make these problems less vexing." The affidavit set forth sufficient detail why traditional techniques would not prove successful in the circumstances of the instant case. U.S. v. Milton, 153 F.3d 891 (8th Cir. 1998); U.S. v. Thompson, 210 F.3d 855 (8th Cir. 2000)(quoting Milton).

Although organized crime investigations present similar necessity statements from one investigation to another, such similarity does not render the affidavit language ineffective. U.S. v. Scala, 388 F. Supp.2d 396 (S.D.N.Y. 2005); U.S. v. Bellomo, 954 F. Supp. 630 (S.D.N.Y. 1997).

Utah State wiretap application contained no alternative investigative statement or incorporation by reference of such facts, and therefore suppression of intercepts and derivative evidence was required. The Utah statute mirrors the federal provisions contained in 18 U.S.C. 2518. U.S. v. Mondragon, 52 F.3d 291 (10th Cir. 1995).

In a separate appeal by a Mondragon codefendant, the Tenth Circuit held that although a supplemental application did not address the "necessity requirement" as such, it was satisfied that it was nevertheless valid, whether under a common sense approach to the Wiretap Act, see U.S. v. Nunez, 877 F.2d 1470 at 1472 (10th Cir. 1989), or under the spirit of guidance enunciated in U.S. v. Ventresca, 380 U.S. 102, 111-12 (1965) (officers did what the Constitution requires). The supplemental order was issued a mere four days after the original order for the

sole reason that the telephone number had been changed on a mobile phone targeted in the original order. "We note that, in contrast, the second supplemental order held invalid in Mondragon authorized surveillance of a new number, listed in the name of a different individual residing at a different location." U.S. v. Quintana, 70 F.3d 1167 (10th Cir. 1995).

Other cases where necessity showing was found to be adequate:

U.S. v. Williams, 2005 U.S. App. LEXIS 14776 (3d Cir.)

U.S. v. Cannon, 2005 WL 2269586 (11th Cir.)(unpublished)

U.S. v. Small, 423 F.3d 1164 (10th Cir. 2005)

U.S. v. Lewis, 2005 WL 1678981 (3d Cir.)(unpublished)

U.S. v. Eiland, 2005 WL 2679992 (D. D.C.)

U.S. v. Menendez, 2005 WL 1384027 (S.D.N.Y.)

U.S. v. Gray, 372 F. Supp.2d 1025 (N.D. Ohio 2005)

U.S. v. Gray, 410 F.3d 338 (7th Cir. 2005)

U.S. v. Lynch, 367 F.3d 1148 (9th Cir. 2004)

U.S. v. Rivera-Rosario, 300 F.3d 1 (1st Cir. 2002)

U.S. v. Santana, 342 F.3d 60 (1st Cir. 2003)

U.S. v. Jackson, 345 F.3d 638 (8th Cir. 2003)

U.S. v. Cline, 349 F.3d 1276 (10th Cir. 2003)

U.S. v. Mascarenas, 2002 WL 172685 (10th Cir.)(unpublished)

U.S. v. Santiago, 389 F. Supp.2d 124 (D. Mass. 2005)

U.S. v. Pappas, 298 F. Supp.2d 250 (D. Conn. 2004)

U.S. v. Giovannelli, 2004 U.S. Dist. LEXIS 220 (S.D.N.Y.)

U.S. v. Cepeda, 2004 U.S. Dist. LEXIS 7446 (D. Mass.)

U.S. v. Hendricks, 2004 U.S. Dist. LEXIS 8859 (D. V.I.)

U.S. v. Moran, 349 F.Supp.2d 425 (N.D.N.Y. 2005)

U.S. v. Garcia, 2005 WL 589627 (S.D.N.Y.)

U.S. v. Lazu-Rivera, 363 F. Supp.2d 30 (D. P.R 2005.)

U.S. v. Caldwell, 2005 WL 818412 (N.D. Ill.)

U.S. v. Green, 2005 WL 1041205 (E.D. La.)

U.S. v. Ramirez-Encarnacion, 291 F.3d 1219 (10th Cir. 2002)

U.S. v. Segura, 2001 WL 286850 (D. Conn.)

U.S. v. Iiland, 254 F.3d 1264 (10th Cir. 2001)

U.S. v. Washington, 2004 U.S. App. LEXIS 22020 (6th Cir.) (unpublished)

U.S. v. Bankston, 182 F.3d 296 (5th Cir. 1999)

U.S. v. Kelley, 140 F.3d 596 (5th Cir. 1998)

U.S. v. Diaz, 1998 WL 380935 (10th Cir.)

U.S. v. Stewart, 1998 WL 468735 (4th Cir.)

U.S. v. Miller, 116 F.3d 641 (2d Cir. 1997)

U.S. v. Williams, 124 F.3d 411 (3d Cir. 1997)

U.S. v. Green, 40 F.3d 1167 (11th Cir. 1994)

U.S. v. Le, 377 F. Supp.2d 245 (D. Me 2005)

U.S. v. Lawrence, 2003 WL 22089778 (N.D. Ill.)

U.S. v. Cozzo, 2003 WL 57031 (N.D. Ill.)

U.S. v. Hernandez-Sendejas, 286 F. Supp.2d 1295 (D. Kan. 2003)

U.S. v. Mack, 272 F. Supp.2d 1174 (D. Col. 2003)

U.S. v. Merton, 274 F. Supp.2d 1156 (D. Col. 2003)

U.S. v. Montegio, 274 F. Supp.2d 190 (D. R.I. 2003)

U.S. v. Greyling, 2002 WL 424655 (S.D.N.Y.)

U.S. v. Jarding, 2002 WL 1905533 (N.D. Ill.)

U.S. v. Aparo, 2002 WL 2022329 (E.D.N.Y.)

U.S. v. Santana, 218 F. Supp.2d 53 (D. N.H. 2002)

U.S. v. Herrera, 2002 U.S. Dist. LEXIS 17697 (S.D.N.Y.)

U.S. v. Wager, 2002 U.S. Dist. LEXIS 17739 (S.D.N.Y.)

U.S. v. Small, 229 F. Supp.2d 1166 (D. Col. 2002)

U.S. v. Patterson, 2002 WL 31890950 (S.D.N.Y.)

U.S. v. Hanhardt, 157 F. Supp.2d 978 (N.D. Ill. 2001)

U.S. v. Marra, 2001 U.S. Dist. LEXIS 23063 (W.D.N.Y.)(search for fugitive in investigation of abortion doctor murder)

U.S. v. Cooper, 2000 WL 135248 (D.D.C.)

U.S. v. Soto-Del Valle, 2000 WL 816074 (D. P.R.)

U.S. v. Harris, 2000 WL 1206724 (S.D.N.Y.)

U.S. v. Wells, 2000 WL 1231722 (S.D. Ind.)

U.S. v. Borrayo-Gutierrez, 119 F. Supp.2d 1168 (D. Colo. 2000)

U.S. v. Kaczowski, 114 F. Supp.2d 143 (W.D.N.Y. 2000)

U.S. v. Hogan, 122 F. Supp.2d 358 (E.D.N.Y. 2000)

U.S. v. Lombardo, 1999 U.S. Dist. LEXIS 7078 (S.D.N.Y.)

U.S. v. Crumpton, 54 F. Supp.2d 986 (D. Colo. 1999)

U.S. v. Abbit, 1999 WL 1074015 (D. Or.)

U.S. v. Lopez, 72 F. Supp.2d 5 (D. P.R. 1999)

U.S. v. Benjamin, 72 F. Supp.2d 161 (W.D.N.Y. 1999)

U.S. v. King, 991 F. Supp. 77 (E.D.N.Y. 1998)

U.S. v. Gruber, 994 F. Supp. 1026 (N.D. Iowa 1998)

U.S. v. Charles, 1998 WL 204696 (D. Mass.)

U.S. v. Zambrano-Sanchez, 1998 WL 231077 (D. Kan.)

U.S. v. Velazquez, 1997 WL 564674 (N.D. Ill.)

Civilian Monitors

U.S. v. Lopez, 300 F.3d 46 (1st Cir. 2002):

> We hold that the government must disclose, as a part of its application for a wiretap warrant, any intention to utilize the services of civilian monitors in the execution of the warrant. To hold otherwise would, in our view, run counter to the general duty of candor the statute imposes on the government and impair the issuing judge's ability to preserve important privacy interests protected by Title III. . .We are the first court of appeals to hold that Title III requires the government to disclose any plans to employ civilian monitors; indeed, we appear to be the first court that has been squarely presented with the issue. . .Title III imposes an obligation on the government to disclose

to the issuing judge any plans to use civilian monitors in the execution of a wiretap warrant. In the case at hand, however, the government's failure to make that disclosure, along with the government's seeming violation of an order that did not permit the use of civilian monitors, does not provide a valid basis for suppressing the intercepted communications.

"Intercept"/Jurisdiction

"The language of 2510(4), the legislative history of that section, and the policy considerations of Title III all persuade us that for purposes of 2518(3)'s jurisdictional requirement, a communication is intercepted not only where the tapped telephone is located, but also where the contents of the redirected communication are first to be heard." U.S. v. Rodriguez, 968 F.2d 130 (2d Cir. 1992) (wiretap order issued in S.D.N.Y. for telephones located in New Jersey, but monitored in S.D.N.Y.); U.S. v. Giampa, 904 F. Supp. 235 (D. N.J. 1995)(citing Rodriguez).

“We agree with the the reasoning of the Second Circuit and now hold that interception includes both the location of a tapped telephone and the original listening post, and that judges in either jurisdiction have authority under Title III to issue wiretap orders.” U.S. v. Denman, 100 F.3d 399 (5th Cir. 1996)(applying Rodriguez).

The term "intercept" as it relates to "aural acquisitions" refers to the place where a communication is initially obtained regardless of where the communication is ultimately heard. U.S. v. Nelson, 837 F.2d 1519 (11th Cir. 1988) (state court wiretap order issued in county where telephone located, but monitoring occurred in county not within issuing court's jurisdiction). Territorial jurisdictional limitations do not implicate Congress’s core concerns in passing Title III. Adams v. Lankford, 788 F.2d 1493 (11th Cir. 1986).

In Evans v. Georgia, 314 S.E.2d 421 (1984), the Georgia Supreme Court held that “aural acquisition” occurred at listening post located within the territorial jurisdiction of the issuing judge although target telephones were located outside the jurisdiction of the issuing judge.

A Tenth Circuit panel, citing Rodriguez and footnoting to Nelson, ruled that an Oklahoma State wiretap was properly issued in the judicial district where the communications were actually heard by the monitoring agents, although the phones were located in a different jurisdiction. The court did not reach the issue of whether jurisdiction to issue the order also exists in the judicial district where the target phones were located. U.S. v. Tavarez, 40 F.3d 1136 (10th Cir. 1994); U.S. v. Grist, 1995 WL 331242 (10th Cir. 6/1/95) (Tavarez co-defendant); U.S. v. Edwards, 69 F.3d 419 (10th Cir. 1995) (Tavarez related).

A judge in the N.D. of Illinois had jurisdiction to authorize interception of oral communications occurring in a prison located in the S.D. of Illinois (microphone concealed in prison visitor’s badge) because the intercepted communications were transmitted to the N.D. of Illinois where the agents first heard them. U.S. v. Jackson, 207 F.3d 910 (7th Cir. 2000)(citing Rodriguez, Denman, Tavarez, and Ramirez (see below)); U.S. v. Wilson, 237 F.3d 827 (7th Cir. 2001)(reiterating holding in Jackson); U.S. v. Hoover, 246 F.3d 1054 (7th Cir. 2001)(reiterating holding in Jackson).

("Mobile Interception Device")

On April 28, 1997, the Seventh Circuit issued the first published decision interpreting the "mobile interception device" provision of 18 U.S.C. 2518(3).

The case concerned a Title III order issued in the Western District of Wisconsin to intercept a cellular telephone being used by a Wisconsin resident in furtherance of drug activities during which he traveled back and forth between Minnesota and Wisconsin. The listening post was set up in Minnesota. Within a few days after the order was issued the agents manning the post learned from intercepted conversations that the target cellular telephone was not being used by the subject named in the order. He was using a different phone. The user of the tapped phone did not seem to travel outside Minnesota, but was using the tapped phone in furtherance of the subject drug conspiracy.

Chief Judge Posner, writing for the panel, broadly interprets the provision. The Court notes that the order contained no geographical limitation. The order included 2518(3) language permitting interception anywhere in the United States if the cellular phone was transferred outside the district of the issuing court. The Court also noted that it is not certain that the target cellular phone was transferred outside the issuing court's jurisdiction or whether the phone was ever within the issuing jurisdiction. The Court did not read the order as limited to the case in which the phone was at some time in the district.

> The emphasis in "mobile interception device" falls, it seems to us (there are no other published decisions on the point), on the mobility of what is intercepted rather than on the irrelevant mobility or stationarity of the device. The term in context means a device for intercepting mobile communications, and so understood it authorized the district judge in the Western District of Wisconsin to order a tap on the [cellular] phone thought to be used by [named subject], regardless of where the [cellular] phone or the listening post was.

The Court said that a narrow interpretation of 2518(3) requiring that the listening post or the telephone be located in the authorizing district (applying the Rodriguez and Denman jurisdictional analysis) would merely complicate law enforcement and serve no interest in protecting privacy, since the government could always seek an order in the district of the listening post for nationwide surveillance of cellular phone calls. U.S. v. Ramirez, 112 F.3d 849 (7th Cir. 1997).

Extensions

An order targeting the same subject, at the same location, regarding the same matter as an earlier order, constitutes an "extension" of the earlier order for purposes of section 2518(8)(a) if, but only if, the new order was obtained as soon as administratively practical or any delay is satisfactorily explained, i.e., is shown to have occurred without fault or bad faith on the part of the government. U.S. v. Carson, 969 F.2d 1480 (3d Cir. 1992); U.S. v. Jackson, 207 F.3d 910 (7th Cir. 2000).

The Ninth Circuit rejected the government's attempt to apply a broader view of the term "extension" in the context of cellular telephone Title III orders, and held that a 39 day delay in sealing cellular Title III recordings violated the "immediate sealing" requirements of 2518(8)(a). The circuit panel agreed with the Second and Third Circuits that an order is an extension of an earlier order only if it authorizes continued interception of the same location or the same communications facility specified by the prior order. However, the circuit panel also held that the actual reason for the delay in sealing was the government's mistaken belief that it could delay the sealing because later orders targeting a different cellular telephone number were extensions (the government referred to them as "extensions" in periodic progress reports to the district court and the lower court agreed with the government's view that the later orders were extensions) and the government's explanation was objectively reasonable (citing U.S. v. Ojeda Rios, 875 F.2d 17 (2d Cir. 1989) and U.S. v. Vastola, 915 F.2d 865 (3d. Cir. 1990)) because prior to the instant

opinion, the meaning of the term “extensions” was an open question in the Ninth Circuit. Only the Second and Third Circuits had previously addressed the question. The Principie opinion (531 F.2d 1132 (2d Cir. 1976))(see below), although distinguishable, supported the government’s theory that extensions have a broader meaning, and it has not been expressly overruled by the Second Circuit. U.S. v. Hermanek, 289 F.3d 1076 (9th Cir. 2002).

Government's delay (more than two weeks) in obtaining first extension order was reasonably explained as due to demands of drafting extension affidavit and processing it through the federal bureaucracy. The government sealed the tapes two weeks after the original period in a good-faith effort to comply with 2518(8)(a) "in the face of an innocent delay in processing the request for a second surveillance period." U.S. v. Plescia, 48 F.3d 1452 (7th Cir. 1995).

An order that was entered at least 16 days after a prior order had expired was to be regarded as an "extension" within the meaning of §2518 because it "was clearly part of the same investigation of the same individuals conducting the same criminal enterprise" as was being investigated under the prior order. U.S. v. Principie, 531 F.2d 1132, 1142, and n. 14 (2d Cir. 1976).

Where there is a gap between the expiration of an order and an "extension," the later order can be deemed an extension of the prior one. Where an "intercept is of the same premises and involves substantially the same persons, an extension under these circumstances requires sealing only at the conclusion of the whole surveillance." U.S. v. Scafidi, 564 F.2d 633, 641 (2d Cir. 1977).

The fact that an extension is granted after the term of the initial authorization order has technically expired does not mean that the continuation is not an “extension” within the meaning of the statute. U.S. v. Pichardo, 1999 WL 649020 (S.D.N.Y. 8/25/99).

Nothing in Title III requires that the government secure extension orders prior to the expiration of the preceding order. Thus time gaps may exist between periods of authorized surveillance, so long as the government turns off all listening devices during those gaps and the defendant does not suffer prejudice from the time gap. U.S. v. Gambino, 734 F. Supp. 1084 (S.D.N.Y. 1990); U.S. v. Elson, 968 F. Supp. 900 (S.D.N.Y. 1997);
U.S. v. Merton, 274 F. Supp.2d 1156 (D. Col. 2003)(four day gap legally insignificant).

Federal law "places no limit on the number of orders or extension orders that may be issued to authorize continuation of a given interception." U.S. v. Vazquez, 605 F.2d 1269 (2d Cir. 1979); U.S. v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993).

The phrase "period of the order, or extensions thereof," in the sealing provision of 2518(8)(a) . . . encompasses a continuous authorized wiretap in its entirety, regardless of whether the judicial orders authorizing the initiation or continuation of the tap are denominated "orders," "extensions," "renewals," or "continuations." U.S. v. Vazquez, 605 F.2d 1269 (2d Cir. 1979); U.S. v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993).

Magistrate Judge

On 2/14/92, Judge Edward Korman (E.D.N.Y.) issued a memorandum and order referring Title III applications to a United States magistrate judge pursuant to authority contained in the Federal Magistrates Act of 1968 (28 U.S.C. §§ 631-639). In re U.S. Attorney, 784 F. Supp. 1019 (E.D.N.Y. 1992). The government's mandamus petition was denied by the Second Circuit on 3/23/93 because no Title III application had been referred to a magistrate. On 6/10/93, Judge Korman referred a Title III application to a magistrate judge. On 11/23/93, in a 2-1 decision, the

Second Circuit granted mandamus and ordered Judge Korman not to delegate review of Title III applications to federal magistrate judges and to review personally an application then pending. In re U.S.A., 10 F.3d 931 (2d Cir. 1993). Notwithstanding the "substantial arguments" of Judge Korman, two judges on the panel were "unwilling, in the absence of explicit statutory direction, to expansively interpret Title III's definition of a 'judge of competent jurisdiction,' 18 U.S.C. § 2510(9), to include magistrate judges."

Judge's Preliminary Review of Application/Affidavit

"As long as no action has been taken on the application while the affidavit is in an unsigned condition, the Court cannot find that the judicial economy served by a preliminary review of the materials is improper." U.S. v. Borrayo-Gutierrez, 119 F. Supp.2d 1168 (D. Colo. 2000). See also U.S. v. Small, 229 F. Supp.2d 1166 (D. Col. 2002)(citing Borrayo)(Judge's preliminary review of "courtesy copies" of TIII applications and affidavits does not affect the legality of her decision to grant the Government's request for a Title III order where before signing the order, the judge determined that the final application submitted to her was authorized by an appropriately designated official and the judge determined from the AUSA and agent what, if any, changes had been made to the "courtesy copy").

Location of Authorizing Judge

The authorizing judge does not have to be physically present in his district when he signs the order. U.S. v. Van Horn, 789 F.2d 1492 (11th Cir. 1986); U.S. v. Strother, 578 F.2d 397 (D.C. Cir. 1978); U.S. v. Gomez, 495 F. Supp. 992 (S.D.N.Y. 1979).

Emergency Interception

Evidence from emergency wiretaps suppressed because Government did not demonstrate immediate danger of death or serious injury, such that there was not time, with due diligence, to obtain a court order. U.S. v. Crouch, 666 F. Supp. 1414 (N.D. Cal. 1987).

Kidnap and extortion in progress warranted emergency intercept. Nabozny v. Marshall, 781 F.2d 83 (6th Cir. 1986).

"Congress had in mind by the use of the term 'emergency' an important event, limited in duration, which was likely to occur before a warrant could be obtained." U.S. v. Capra, 501 F.2d 267 (2d Cir. 1974).

Fugitives

In the first reported opinion concerning Title III surveillance to locate a fugitive, § 2516(1)(l), the United States District Court in Maryland, in U.S. v. McKinney, 785 F. Supp. 1214 (D. Md. 1992) held:

18 U.S.C. 2516(1)(l) does not refer to a separate crime, but merely authorizes electronic surveillance where the government seeks to locate one who has obtained the status of a "fugitive from justice," by fleeing prosecution for an enumerated offense.

The issuing court must find probable cause 1) that an individual has fled from authorities in fear that he would otherwise be subject to present or future criminal prosecution for an offense enumerated in § 2516(1); and 2) that particular communications tending to reveal the location of the fugitive will be obtained through the interception sought.

In the W.D.N.Y. a magistrate judge issued a Report and Recommendation denying suppression of evidence obtained from the execution of seven Title III warrants for the interception of communications concerning the location of a fugitive (Charles Kopp in connection with the murder of Dr. Slepian) as defined in 18 U.S.C. 2516(1)(l). U.S. v. Marra, 2001 U.S. Dist. LEXIS 23063 (W.D.N.Y.).

Execution

Order to Service Provider Under 2518(4)

On November 18, 2003, the Ninth Circuit held (2-1 panel split) that Section 2518(4) assistance orders issued to "The Company" (ATX, a competitor of OnStar) in aid of Title III oral communications intercept orders "should not have issued" because they violated the "a minimum of interference" requirement of 2518(4).

> "We hold that whatever the precise limits Congress intended with its "a minimum of interference" limitation, the level of interference with the System worked by the FBI's surveillance is not "a minimum of interference with the services" that the Company "accords the person whose communications are to be intercepted." § 2518(4). Because, given the setup of the System, the surveillance could not be completed with "a minimum of interference," the district court erred in ordering the Company's assistance."

Company v. U.S., 349 F.3d 1132 (9th Cir. 2003).

Time Computation

18 U.S.C. 2518(5) provides that no order may authorize a period of surveillance 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."

The Office of Enforcement Operations has suggested that in light of the fact that the text of 18 U.S.C. 2518(5) ("day on which"; "ten days after the order is entered") does not precisely describe the exact point (clock time or calendar day) from which the interception period is computed, computation of the authorized period of interception should take into account the date and time of the judge's signature and the date and time of the installation and activation of the monitoring equipment.

However, note should be made of recent judicial holdings regarding Title III time computation.

On August 17, 2000, in U.S. v. Smith, 223 F.3d 554 (7th Cir. 2000), regarding the computation of the Title III statutory time period, a Seventh Circuit panel held:

> According to the statute, the 30-day period for the extension began to run on September 15, 1994--the day of the first interception. We think it most sensible to look to Fed. R. Crim. P. 45(a) for guidance on the way the statutory time period should be computed. See, e.g., United States v. Sklaroff, 323 F. Supp. 296, 317 (S.D. Fla. 1971). Under that approach, the first day of the 30-day period is not included but the last is, and the order in this case expired on October 15. Although one district court has chosen not to apply Fed. R. Crim. P. 45(a) to the calculation of the 30-day period, see United States v. Gangi, 33 F. Supp. 2d 303, 309 (S.D. N.Y. 1999) (not applying Fed. R. Crim. P. 45(a) and including both first and last day in calculation of 30-day period), the Third Circuit interpreted the system in the same way we have done. See United States v. Carson, 969 F.2d 1480, 1485 (3d Cir. 1992). We see no reason to create a circuit conflict over this kind of mechanical determination, especially when the general methodology of the Rule is familiar (though we note that we are not applying Rule 45 directly, and thus that we are not necessarily incorporating all of its details such as the way to count weekends and holidays).

[On January 17, 2001, in U.S. v. Wilson, 237 F.3d 827 (7th Cir. 2001), the Seventh Circuit reiterated its holding in U.S. v. Smith, 223 F.3d 554 (7th Cir. 2000)]

"In computing any period of time the day of the act or event from which the designated period of time begins to run shall not be included." Fed. R. Crim. P. 45. Applied to wiretap applications in U.S. v. Villegas, 1993 WL 535013 (S.D.N.Y.); See also U.S. v. Sklaroff, 323 F. Supp. 296 (S.D. Fla. 1971).

FRCP Rule 45 applies to time periods prescribed by statute. U.S. v. Melendez-Carrion, 790 F.2d 984 (2d Cir. 1986).

In computing the thirty day period, the day of authorization is not included. In calculating the length of a sealing delay, the date on which the authorization ends is not included. U.S. v. Gerena, 695 F. Supp. 649, 658 (D. Conn. 1988).

For purposes of Title III, a "day" refers to a calendar day and not an increment of 24 hours, at least where the order does not provide otherwise. The interceptions made on the 31st day under two orders are therefore suppressed. U.S. v. Gangi, 33 F. Supp.2d 303 (S.D.N.Y. 1999); government's motion for reconsideration denied, U.S. v. Gangi, 1999 U.S. Dist. LEXIS 1250 ("The fact that the Office of Enforcement Operations interprets a "day" to mean a "24-hour period" is hardly dispositive, as OEO is a branch of the Department of Justice"). Note that no reference is made to FRCP Rule 45 in the Gangi cases.

In another case, the government argued that, because interception pursuant to a wiretap order commenced on November 8 at approximately 5:36 p.m., the order did not expire until December 8 at 5:36 p.m., and it therefore complied by ceasing interception at 4:31 p.m. on December 8. However, the District Court held that by the terms of the order, the period began to run on the date--not at the time--interception began. Accordingly, the period commenced on, and included, November 8, and expired at the end of the thirtieth day, i.e., December 7. Because no extension was granted until December 9, any communications intercepted on December 8 were unauthorized and must be suppressed. U.S. v. Pichardo, 1999 WL 649020 (S.D.N.Y. 8/25/99).

Although the government intended to begin the wiretap on April 3, and government records show that between April 3 and April 9, some calls were identified merely as to date and time but the agents made no recordings or summaries as to the actual contents of those calls, "interception" did not begin until April 9, when the resolution of technical difficulties with the service provider allowed recording of conversations to begin.18 U.S.C. 2510(4), 2510(8) and 2518(5). U.S. v. Lazu-Rivera, 363 F. Supp.2d 30 (D. P.R. 2005).

Surreptitious Entry

The Fourth Amendment does not prohibit per se a covert entry to install otherwise legal electronic bugging equipment; Congress meant to authorize courts in certain circumstances to approve electronic surveillance without limitation on the means necessary to its accomplishment, so long as they are reasonable under the circumstances; and the Fourth Amendment does not require that a Title III order include a specific authorization to enter covertly the premises described in the order. Dalia v. U.S., 441 U.S. 238 (1979).

[DOJ policy requires that application and order include surreptitious entry language.]

It does not matter that the Title III issuing judge was not told that listening devices had already been installed (microphones hidden in lamps placed by an informant):

> We may suppose (without deciding) that when seeking authorization to listen to conversations the agents should have told the judge that the lamps were already in place, but this does not matter. It is not conceivable that the judge would have said anything like: "Because you used an informant to install one microphone and tricked O'Neill into bugging his own home, I will deny you permission to listen even though you have established probable cause to believe that the bugs will reveal evidence of crime." Cf. *Franks v. Delaware*, 438 U.S. 154 (1978). Perhaps the judge would not have authorized clandestine entry had he realized that bugs already were in place. Prosecutors say that they sought authority to enter in case the lamps should be unplugged or not transmit signals strong enough to be recorded; the judge might have required prosecutors to show one of these problems before authorizing an entry. But in the event no entry was made. So there is no causal chain from the omission to any evidence used against the defendants, and no basis for suppression.

U.S. v. Warneke, 310 F.3d 542 (7th Cir. 2002).

Microphone Installation by Cooperating Individual

Informant's installation of hidden microphones in the defendants' homes (in lamps) and agents' testing of microphone signal (no communications intercepted) before the government obtained a Title III warrant did not violate the Fourth Amendment or Title III.

> The installation of the bugs did not violate the fourth amendment: the Constitution does not protect criminals against the risk that their associates will assist the police. See *Hoffa v. United States, 385 U.S. 293, 300-03, 310-12, 17 L. Ed. 2d 374, 87 S. Ct. 408 (1966).* Placement of these microphones was the result of good police work plus luck. . . Agents drove by O'Neill's residence to find out if this worked; they learned from detecting a carrier signal that it had. Whether this step created a constitutional problem under the holding of *United States v. Karo, 468 U.S. 705, 82 L. Ed. 2d 530, 104 S. Ct. 3296 (1984),* is not a question we need decide, because no evidence based on the monitored signal was used against O'Neill at trial. What *was* used was the ensuing conversations, and their interception was authorized by a warrant issued in response to an affidavit that did not mention the monitored signal (or for that matter the fact that the bug-infested lamp was in place already). Because the agents did not intercept (*i.e.*, did not either record or listen to) any communications until after the warrant had issued, installation of the device at O'Neill's home (and determination that it was working) did not violate statutory limits on eavesdropping; until interception begins, a bug is nothing but a "tracking device" under *18 U.S.C. § 3117*(b). See also *18 U.S.C. § 2510*(12) [preceding language reflects an amendment Ordered and reported at 2003 U.S. App. LEXIS 354]. . .We may suppose (without deciding) that when seeking authorization to listen to conversations the agents should have told the judge that the lamps were already in place, but this does not matter. . . Perhaps the judge would not have authorized clandestine entry had he realized that bugs already were in place. Prosecutors say that they sought authority to enter in case the lamps should be unplugged or not transmit signals strong enough to be recorded; the judge might have required prosecutors to show one of these problems before authorizing an entry.

U.S. v. Warneke, 310 F.3d 542 (7th Cir. 2002).

Title III oral communications interception order authorized surreptitious entry at the target premises. An informant with access to the target premises installed and maintained listening devices therein under the technical supervision of the government. "[T]he Court does not believe that installation or maintenance of devices are tasks exclusively relegated to federal agents by Title III. As long as the interception has been authorized pursuant to Title III, and any person entering private property for the purpose of installing surveillance devices is authorized to enter the property, either by warrant or otherwise, the Court does not perceive further constitutional or statutory requirements relating to the actual installation of the devices. U.S. v. Gambino, 734 F. Supp. 1084 (S.D.N.Y. 1990)

Attorney-Client Privilege

The crime fraud exception ensures "that the seal of secrecy between lawyer and client does not extend to communications made for the purpose of getting advice for the commission of a fraud or crime." U.S. v. Zolin, 491 U.S. 554, 562 (1989).

Defendant (criminal defense attorney charged with conspiracy to provide material support and resources to a designated foreign terrorist organization) moved to compel the government to disclose whether it is engaging in any court-authorized electronic surveillance or monitoring of her communications with her counsel or with her clients, pursuant to either Title III or FISA. Both statutes provide for notice and the opportunity to challenge surveillance after it occurs and before it is used against a defendant. They do not provide for advance notice, however, which would undermine the efficacy of the statutes. While the defendant argues that the possible existence of surveillance interferes with her Sixth Amendment right to the effective assistance of counsel, she cites no authority for the proposition that a bare fear of surveillance, without more, is sufficient to establish a constitutional requirement that the government disclose whether it is engaging in any court authorized surveillance of a criminal defendant under Title III or FISA. Under the statutes there are protections to minimize intrusions, and the government has represented in this case that if any privileged communications were intercepted, screening devices would be used to ensure that the interceptions were not used against the defendants and, thus, that their Sixth Amendment rights would not be violated. Motion denied. U.S. v. Sattar, 2002 WL 1836755 (S.D.N.Y.).

The law places burden on person claiming privilege to establish all of its essential elements, which are that client must have sought legal advice, advice was sought from attorney acting in his professional capacity, communication between attorney and client was for purpose of seeking legal advice, and communication was made in confidence. U.S. v. Gotti, 771 F. Supp. 535 (E.D.N.Y. 1991); U.S. v. Aparo, 2002 WL 2022329 (E.D.N.Y.)(citing Gotti).

There is no protection under the attorney-client privilege where attorney engages in criminal or personal business activities with a client. U.S. v. Cleveland, 1997 WL 208937 (E.D. La. 4/28/97).
Intercepted communications between defendant and his lawyer were not protected by the attorney-client privilege because the defendant was using his lawyer's services to cover up crimes related to extortion. U.S. v. Edwards, 303 F.3d 606 (5th Cir. 2002).

Three years after the Fifth Circuit affirmed his conviction, defendant sought a new trial, Title III information and an evidentiary hearing on the basis of defendant's speculative assertions that the government recorded privileged conversations that revealed his trial strategy to the prosecution team. The court denied the motions, finding that there was no attorney-client privilege protecting the intercepted communications between the defendant's attorneys and third parties. U.S. v. Bankston, 2000 WL 1252582 (E.D. La.).

There is no protection under the attorney-client privilege for an attorney intercepted talking with former client on phone about the attorney's protecting the former client by falsely telling the former client's drug trafficking associates that the former client had been arrested. This scheme was intended to, and did, keep the former client's criminal associates from collecting a drug debt from the former client. U.S. v. Johnston, 146 F.3d 785 (10th Cir. 1998); see also U.S. v. Abbit, 1999 WL 1074015 (D. Or.)(citing Johnston).

The government's efforts to properly minimize conversations between defendant and an attorney were reasonable:

> The reviewing agents were instructed not to intercept privileged attorney-client communications. Moreover, the agents were instructed "[i]f at any time during the investigation it is determined that an attorney is participating in an intercepted conversation, do *not* summarize this conversation in the same log as the rest of the calls. Instead, you will summarize the conversation on a separate system, and immediately notify the Supervising Agent. As soon as it is determined that an attorney is participating in an intercepted conversation involving *legal consultation of any kind or discussing legal strategy*, turn off the monitor and stop recording. All calls in which an attorney is participating will be reviewed by an attorney that is not participating in this investigation." In this case, it appears that these procedures were followed. . .[Defendant] has not proven that all of the communications between himself and [the attorney] are privileged. Even if he were to make such a showing, the calls may be subject to the crime-fraud exception. Moreover, even if we were to find that the communications are privileged and not subject to the crime-fraud exception, the remedy would be suppression of only the privileged calls. See United States v. Abbit, 1999 WL 1074015 (D. Ore.).

U.S. v. Lawrence, 2003 WL 22089778 (N.D. Ill.).

The privilege is applicable: (1) Where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, [then] (3) the communications relating to the purpose, (4) made in confidence (5) by the client, (6) are at this instance permanently protected (7) from disclosure by himself or by the legal advisor (8) unless the protection be waived. Admiral Ins. v. U.S. Dist. Court for Dist. of Ariz., 881 F.2d 1486 (9th Cir. 1989).

Interception of conversations between attorney and client is not presumptively invalid for lack of probable cause to believe exception to attorney-client privilege applies. Title III makes no special provision for privileged communications beyond requiring that the interception be minimized. The absence of such a provision may bespeak a recognition by Congress that "doctors and lawyers have been known to commit crimes." U.S. v. Hyde, 574 F.2d 856, 870 (5th Cir. 1978); see also U.S. v. Abbit, 1999 WL 1074015 (D. Or. 11/24/99)(citing Hyde).

The law of attorney-client privilege places the burden of proof on the proponent of the privilege. Hawkins v. Stables, 148 F.3d 379 (4th Cir. 1998) (articulates "classic test" for determining the existence of attorney-client privilege).

Agents inadvertently intercepted numerous attorney communications, but the defendants failed to prove that each of these communications were attorney-client privileged and they also failed to prove that the agents acted in bad faith. It was error to impose suppression as punishment for these inadvertent interceptions of attorney communications. Because there was no bad faith attempt to obtain privileged conversations, those conversations should be suppressed on an individual basis at or before trial. U.S. v. Ozar, 50 F.3d 1440 (8th Cir. 1995); see also U.S. v. Abbit, 1999 WL 1074015 (D. Or. 11/24/99).

Suppression of only the attorney/client phone call that was inadvertently, but negligently, intercepted by a police officer monitoring a state wiretap was an appropriate remedy for the officer's violation of the amended minimization order. U.S. v. Charles, 213 F.3d 10 (1st Cir. 2000).

Sixth Amendment right to counsel was not violated by government's use of defendant's girlfriend to consensually record her jailhouse conversation with the defendant in connection with the government's investigation of the girlfriend's claim that the defendant had threatened the life of the ATF agent who was involved in the pending prosecution. The Sixth Amendment right to counsel is offense-specific. The government is free to investigate new or additional crimes even though the subject of the investigation is represented by counsel on a pending charge. U.S. v. Kavoukian, 180 F. Supp.2d 402 (N.D.N.Y. 2002)(contains good discussion of Sixth Amendment right to counsel jurisprudence). See also U.S. v. Aparo, 2002 WL 2022329

(E.D.N.Y.)(citing U.S. v. Mapp, 170 F.3d 328 (2d Cir. 1999); U.S. v. Shea, 211 F.3d 658 (1st Cir. 2000); McNeil v. Wisconsin, 501 U.S. 171 (1991) (right to counsel cannot be invoked prospectively)).

Priest-Penitent Privilege

The government's jailhouse nonconsensual taping of a prisoner's "confession" to a priest was a violation of the Religious Freedom Restoration Act (RFRA) (held unconstitutional by Supreme Court on 6/25/97) and the Fourth Amendment. Since the taping was done in the ordinary course of duty of the law enforcement officer (jailor) (18 U.S.C. 2510(5)(a)), the mens rea required for a violation of 2511 was not present and therefore the prosecutor's retention of the intercepted confession was not a violation of 2511. This case was remanded for appropriate injunctive relief barring any future interception of confidential communications between a prisoner and a member of the clergy in the member's professional capacity. Mockaitis v. Harcleroad, 104 F.3d 1522 (9th Cir. 1997).

Marital Communications

The “crime-fraud exception” applies to intercepted wire communications between defendant and his wife involving wife’s knowing participation in attempts to “cover up” crimes committed by husband. U.S. v. Cooper, 2000 WL 135248 (D.D.C.)

Because the marital communications privilege protects only communications made in confidence, the privilege does not apply with regard to communications between husband and wife when one of the spouses is incarcerated. U.S. v. Madoch, 149 F.3d 596 (7th Cir. 1998) (telephone calls on prison phone); See also U.S. v. Harrelson, 754 F.2d 1153 (5th Cir. 1985) (wife visiting husband in prison).

During "no-contact" visits at a private pretrial detention facility (CCA), inmates and visitors sit in different rooms, separated from each other by clear glass. Each visiting station is separated from the adjacent ones by cement block partitions. Visitors communicate with prisoners through an internal communication device that physically resembles a telephone handset. The device, however, is an entirely internal system connecting only the two visiting rooms. It is not connected to any facility capable of transmitting interstate or foreign communications. 18 U.S.C. 2510(1). Accordingly, the visitation conversations are not “wire communications” protected by the federal wiretap law. Although the inmate and his visitor at a private pretrial detention facility claim to have believed that their conversations were private and could not be overheard, any expectation of privacy was objectively unreasonable under the circumstances.

> Prison inmates necessarily have reduced privacy rights because of the nature of incarceration and the myriad of institutional needs and objectives of prison facilities. Hudson v. Palmer, 468 U.S. 517, 524, 82 L. Ed. 2d 393, 104 S. Ct. 3194 (1984); Wolff v. McDonnell, 418 U.S. 539, 555, 41 L. Ed. 2d 935, 94 S. Ct. 2963 (1974). We agree with the district court's conclusion that CCA had legitimate security reasons for monitoring the conversations and that the recordings were not made in an attempt to gather evidence about the robberies or the murder. Because CCA's practice of monitoring and recording prisoner-visitor conversations was a reasonable means of achieving the legitimate institutional goal of maintaining prison security and because those conversing in a prison setting are deemed to be aware of the necessity for and the existence of such security measures, we agree with the district court that the defendants' rights were not violated by the introduction of the recordings. . .
>
> The practice of monitoring conversations reflects CCA's efforts to ensure a high level of security in its facility, and there is no reason to believe that a visitor who converses with an incarcerated

person has any more reasonable basis for his expectation that the conversation will remain private than has the inmate.

U.S. v. Peoples, 250 F.3d 630 (8th Cir. 2001).

Deputization

An interception "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. 18 U.S.C. 2518(5).

State and local officials may assist in Title III monitoring if under supervision of the federal agency ordered to conduct the interception. U.S. v. Lyons, 695 F.2d 802 (4th Cir. 1982).

Federal agents may lawfully monitor state wiretaps. 18 U.S.C. 2517(1) authorizes investigative or law enforcement officers to disclose to other investigative or law enforcement officers the contents of intercepted communications. It makes no difference whether the disclosure occurs after the interception or contemporaneously with the interception. U.S. v. Manfredi, 488 F.2d 588 (2d Cir. 1973).

Deputations not in accordance with DEA's internal procedures do not provide a basis for suppression of otherwise valid wiretaps. U.S. v. Williamston, 1993 WL 527977 (4th Cir. December 21, 1993)(unpublished) (DEA deputations). A court need not exclude evidence obtained in violation of an agency's regulations or rules where neither the Constitution nor statute require adoption of any particular procedures. U.S. v. Caceres, 440 U.S. 741 (1979).

Notwithstanding their obvious status as "Government personnel," it is DOJ policy that state and local law enforcement officials be deputized.

Because Rule 6(e)(3)(A)(ii) of the Federal Rules of Criminal Procedure parenthetically includes the personnel of a state or subdivision of a state, within the term "government personnel," there is some disagreement over whether the term "government personnel" as used in 18 U.S.C. 2518(5) without such parenthetical qualification, includes state and local law enforcement officials.

DOD personnel would appear to qualify as "Government personnel" and could therefore, without deputization, assist in the Title III monitoring process (e.g., as translators) if such assistance does not violate "Posse Comitatus" laws and regulations.

(O.L.C. Opinion)

On April 5, 1994, the AAG, Office of Legal Counsel, in a memorandum to the AAG, Criminal Division, concluded that such assistance by military personnel would not violate the Posse Comitatus Act.

See Posse Comitatus

Supervision of Monitors

U.S. v. Lopez, 300 F.3d 46 (1st Cir. 2002):

> [C]ivilian monitors, who worked sixteen-hour shifts every day for twenty days, were supervised at all times by a shift supervisor. The one apparent exception was a single instance where the supervising agent left the plant for ten to fifteen minutes to conduct routine surveillance. . .[S]uch a *de minimis* departure from the supervision standard is no basis for excluding the communications. This is especially so where, as here, [defendant] makes no attempt to identify any prejudice arising from the interception of communications that might have occurred during the brief unsupervised period.

DEA supervision of police officers monitoring a wiretap was adequate. It is not necessary for a DEA person to be physically present, so long as he is available, and in touch, and can make the discretionary decisions that he is called on to make. U.S. v. Williamston, 1993 WL 527977 (4th Cir. 12/21/93)(unpublished) (DEA deputations).

Posse Comitatus

Although there is no case directly on point, U.S. v. Yunis, 924 F.2d 1086 (D.C. Cir. 1991) and Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990) provide interpretive authority for the argument that assistance from Army personnel in the Title III monitoring process would violate neither the Posse Comitatus Act (18 U.S.C. 1385) nor 10 U.S.C. 375 and the regulations thereunder at 32 C.F.R. 213.10.

32 C.F.R. 213.10(a)(3) provides:

> Restrictions on direct assistance. Except as otherwise provided in this enclosure, the prohibition on use of military personnel "as a posse comitatus or otherwise to execute the laws" prohibits the following forms of direct assistance:
>
> (i) Interdiction of a vehicle, vessel, aircraft or other similar activity.
>
> (ii) A search or seizure.
>
> (iii) An arrest, stop and frisk, or similar activity.
>
> (iv) Use of military personnel for surveillance or pursuit of individuals, or as informants, undercover agents, investigators, or interrogators (emphasis added).

32 C.F.R. 213.10(a)(7) provides:

> Other permissible assistance. The following forms of indirect assistance activities are not restricted by the Posse Comitatus Act:
>
> (i) Transfer of information acquired in the normal course of military operations.
>
> (ii) Such other actions, approved in accordance with procedures established by the head of the DOD component concerned that do not subject civilians to the exercise of military power that is regulatory, proscriptive, or compulsory in nature (emphasis added).

The assistance of DOD personnel in the Title III monitoring process could fairly be characterized as: 1) "indirect assistance" to civilian authorities that does not "subject civilians to the exercise of military power that is regulatory, proscriptive, or compulsory in nature"; 2) services that do not amount to direct active involvement in the execution of the laws (they would be acting under the control and supervision of the civilian federal agency responsible for the investigation and authorized by court order to conduct the interception); and 3) assistance that "is not sufficiently pervasive to rise to the level of enforcement of the law" by the Army. Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990) (Naval Investigative Service agents assisted police with surveillance; one of

its agents made undercover drug purchase and signaled the police when the transaction was completed).

(O.L.C. Opinions)

By memorandum of April 5, 1994 (Re: Use of Military Personnel for Monitoring Electronic Surveillance), Walter Dellinger, Assistant Attorney General, Office of Legal Counsel, responded to Jo Ann Harris, Assistant Attorney General, Criminal Division, that the Office of Legal Counsel has concluded that, under a proper reading of the pertinent statutes, military personnel are presently authorized to assist federal law enforcement officers by monitoring electronic surveillance authorized pursuant to the ECPA.

By memorandum of November 3, 1989 (Re: Extraterritorial Effect of the Posse Comitatus Act) William P. Barr, Assistant Attorney General, Office of Legal Counsel, concluded that the Posse Comitatus Act does not apply outside the territory of the United States. 13 U.S. Op. Off. Legal Counsel 387 (1989 WL 418333 (O.L.C.)).

"Clone Pagers"

The minimization requirement cannot reasonably be applied to clone pagers. "Because it is impossible to tell from the clone beeper whether a conversation even took place, much less the content of any conversation that might have taken place, traditional minimization requirements do not apply." U.S. v. Tutino, 883 F.2d 1125 (2d Cir. 1989); U.S. v. Gambino, 1995 WL 453318 (S.D.N.Y.).

Officers authorized to use a "clone pager" were not required to satisfy the recording requirement where recording such communications electronically was not technically possible. U.S. v. Suarez, 906 F.2d 977 (4th Cir. 1990).

In connection with the government's failure to seal any of its handwritten logs and partial recordings generated on pager receivers in connection with the execution of pager interception orders, the Ninth Circuit held that handwritten logs are not recordings "comparable" to "tape or wire" within the meaning of 2518(8)(a) (citing Suarez), and that although pager receivers (computerized monitors of pager messages) were relatively new in 1994, they were employed effectively by the same FBI office in a contemporaneous investigation and the archive file was printed and sealed in accordance with 2518(8)(a). In the instant case the FBI failed to program the pager receiver accurately and there may have been geographically related reception problems. The circuit panel held therefore that the district court erred in concluding that the use of pager receivers was not possible. But the circuit panel also held that the government offered a "satisfactory explanation" for its omissions because it had an objectively reasonable belief that pager receivers were not recorders within the meaning of 2518 in light of the decisional law. Also, the agents running the investigation became aware of the full capacity of the pager receivers only after the surveillance was terminated. U.S. v. Hermanek, 289 F.3d 1076 (9th Cir. 2002).

Police Department's use of "clone pagers" to intercept numeric transmissions to suspect's digital display pagers pursuant to state court "pen register" order cannot be considered the use of a "pen register" within the meaning of the ECPA, but was an unauthorized interception of electronic communications under 18 U.S.C. 2511. Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995).

Background Conversations

"Plain view" (plain hearing) doctrine applies. No suppression if initial intrusion lawful, discovery inadvertent, and criminal nature of communication immediately apparent. U.S. v. Baranek, 903 F.2d 1068 (6th Cir. 1990).

"Plain View"

> It is true that if government agents execute a valid wiretap order and in the course of executing it discover that it was procured by a mistake and at the same time overhear incriminating conversations, the record of the conversations is admissible in evidence. United States v. London, 66 F.3d 1227, 1234-35 (1st Cir.1995); cf. United States v. Malekzadeh, 855 F.2d 1492, 1496-97 (11th Cir.1988). It is just the "plain view" doctrine (e.g., Horton v. California, 496 U.S. 128, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990); United States v. Ewain, 88 F.3d 689, 693 (9th Cir.1996)) translated from the visual to the oral dimension. It is as if government agents executing a conventional search warrant discover that they have the wrong address but before they can withdraw notice other illegal activity. E.g., Maryland v. Garrison, 480 U.S. 79, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987); United States v. Williams, 917 F.2d 1088 (8th Cir.1990). The discovery of the mistake does not make the search unlawful from its inception, United States v. Fitzgerald, 724 F.2d 633 (8th Cir.1983) (en banc); United States v. Soussi, 29 F.3d 565 (10th Cir.1994); United States v. Noel, 938 F.2d 685, 687-88 (6th Cir.1991), because all that is required for a lawful search is probable cause to believe that the search will turn up evidence or fruits of crime, not certainty that it will. But in either case, the visual or the aural, once the mistake is discovered, the government cannot use the authority of the warrant, or of the order, to conduct a search or interception that they know is unsupported by probable cause or is otherwise outside the scope of the statute or the Constitution. Maryland v. Garrison, supra, 480 U.S. at 87; Dawkins v. Graham, 50 F.3d 532, 534 (8th Cir.1995). No longer would they be merely discovering evidence of crime in the course of a lawful search.

U.S. v. Ramirez, 112 F.3d 849 (7th Cir. 1997).

Attorney Overhearings

USAM 9-7.420

Recording

2518(8)(a) requires recording "if possible."

Officers authorized to use a "clone pager" were not required to satisfy the recording requirement where recording such communications electronically was not technically possible. U.S. v. Suarez, 906 F.2d 977 (4th Cir. 1990).

The Ninth Circuit held that the government's handwritten logs of its pager interceptions are not recordings "comparable" to "tape or wire" within the meaning of 2518(8)(a) (citing Suarez), and that although pager receivers (computerized monitors of pager messages) were relatively new in 1994, they were employed effectively by the same FBI office in a contemporaneous investigation and the archive file was printed and sealed in accordance with 2518(8)(a). In the instant case the FBI failed to program the pager receiver accurately and there may have been geographically related reception problems. The circuit panel held therefore that the district court erred in concluding that the use of pager receivers was not possible. But the circuit panel also held that the government offered a "satisfactory explanation" for its omissions because it had an objectively reasonable belief that pager receivers were not recorders within the meaning of 2518 in light of the decisional law. Also, the agents running the investigation became aware of the full capacity of

the pager receivers only after the surveillance was terminated. U.S. v. Hermanek, 289 F.3d 1076 (9th Cir. 2002).

Duplicate Recordings

"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." 18 U.S.C. 2518(8)(a).

The practice of using a cassette recorder to make a copy of portions of a conversation also being recorded on the original and duplicate original reel-to-reel recorders, was necessary and justified. The government ought to have preserved all work cassettes generated and disclosed the practice during the early discovery stages of the case; however, the defendants were not prejudiced by the later disclosure or by the erasure of all but thirty-nine of the work cassettes. The government was not obligated to present, for judicial sealing, work cassettes which they believed, in good faith, were partial copies of the original and duplicate original reel-to-reel recordings. Similarly, the government was not required to preserve, under 18 U.S.C. 2518(8)(a), the work cassettes, given their good faith belief, that the cassettes were simply partial copies. Thus, that some work cassettes did contain original evidence not found on the reel-to-reel recordings is addressed as inadvertent loss of evidence and not as a knowing violation of Title III sealing and preservation requirements. U.S. v. Gerena, 695 F. Supp. 1369 (D. Conn. 1988).

Minimization

Effort must be objectively reasonable in light of the circumstances confronting the interceptor. "The statute does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations." Scott v. U.S., 436 U.S. 128 (1978).

U.S. v. Bennett, 219 F.3d 1117 (9th Cir. 2000):

> Even assuming the government improperly intercepted all 267 calls as the appellants assert, this was only 3.65% of the total number of calls intercepted. Such a percentage alone is not fatal. See Homick, 964 F.2d at 903 (noting that the interception of "even a relatively high percentage of nonpertinent calls is an inaccurate indicator of whether or not the government complied with the minimization requirement"). "Where, as here, the wire intercept concerns a drug ring, the need to allow latitude to monitoring agents is paramount. . . . The fact that the FBI overheard a few innocent conversations does not render its minimization efforts unreasonable." Torres, 908 F.2d at 1424 (citations omitted). In cases such as the present one involving "a wide-ranging conspiracy with a large number of participants, even a seasoned listener would have been hard pressed to determine with any precision the relevancy of many of the calls before they were completed." Scott, 436 U.S. at 142. Moreover, if phone conversations include guarded or coded language as in this case, a higher rate of nonrelevant intercepted calls should be expected because it takes longer to figure out the meaning of a particular call. See id. at 140. We conclude that the interception of nonrelevant phone conversations were properly minimized.

U.S. v. Lopez, 300 F.3d 46 (1st Cir. 2002):

> Although "blind reliance on the percentage of nonpertinent calls intercepted is not a sure guide" to determining whether the minimization was proper, *Scott v. United States,* 436 U.S. 128, 140, 98 S.Ct. 1717, 56 L.Ed.2d 168 (1978), the nearly flawless performance of the government in this case carries significant weight. *Cf. United States v. Bennett,* 219 F.3d 1117, 1124 (9th Cir.) (minimization requirement met where improperly intercepted calls accounted for only 3.65% of 7322 total intercepted calls), *cert. denied,* 531 U.S. 1056, 121 S.Ct. 666, 148 L.Ed.2d 568 (2000).

> Plus, the findings of the district court support the conclusion that the government established and observed thorough precautions to bring about minimization and that there was a significant degree of judicial supervision over the surveillance process.

U.S. v. Hurley, 63 F.3d 1 (1st Cir. 1995):

> Scott made clear that the statute does not forbid interception of non-pertinent conversations but requires a reasonable effort to minimize such interceptions. Here, the government described the agents' directives to turn off monitoring equipment for irrelevant conversations; it supplied statistics showing that about three-quarters of the time that the agents turned off the monitoring device, they did so because the conversation was deemed non-pertinent; and it pointed to regular reports made to the district court, and to ongoing contacts between the agents and the prosecutors sometimes involving guidance on monitoring. See U.S. v. Angiulo, 847 F.2d 956, 979 (1st Cir. 1988). The Saccoccia enterprise was a widespread and complicated operation in which the illegal conduct was deliberately disguised by the company's legitimate activities. The conspirators employed code phrases that mimicked industry terminology and used code names for each other, banks and clients. Many of the participants were related by blood or marriage, and incriminating exchanges were often interspersed with personal conversation. It is hard to see how the agents could have done more than make a good-faith determination to turn off recording devices when a conversation was seemingly unrelated to the laundering operation.

"The appropriate duration of initial monitoring or the frequency of spot-checking may vary with the circumstances of the call and need not be specifically stated in the Order or the underlying affidavit." U.S. v. Santiago, 389 F. Supp.2d 124 (D. Mass. 2005).

The minimization requirement is satisfied if, on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion. U.S. v. Oriakhi, 57 F.3d 1290 (4th Cir. 1995).

In view of the complex nature of the investigation (bank fraud conspiracy) and the issuing judge's continuing supervision, the government's minimization procedures did not violate 18 U.S.C. 2518(5). The agents submitted their minimizing procedures to the issuing judge and reported minimizing problems to the judge as surveillance progressed. "The agents used the 'two minutes up/one minute down' minimization technique recommended in the Department of Justice Manual, a procedure we reviewed favorably . . . ." This technique provided intermittent spot-checking of minimized conversations, a procedure expressly authorized by the issuing judge and previously approved by the Eighth Circuit. The agents inadvertently intercepted numerous attorney communications, but the defendants failed to prove that each of these communications were attorney-client privileged and they also failed to prove that the agents acted in bad faith. The magistrate's and district court's decision to impose suppression as punishment for these inadvertent interceptions of attorney communications was error. Because there was no bad faith attempt to obtain privileged conversations, those conversations should be suppressed on an individual basis at or before trial. U.S. v. Ozar, 50 F.3d 1440 (8th Cir. 1995).

The government's wiretaps of a major drug ring, intercepted more than 3,500 telephone conversations, including all calls under two minutes in length (almost 1,800). A two minutes up/one minute down, "spot monitoring" procedure was used. Although in affirming the convictions it did not reach the merits of the minimization argument, the Seventh Circuit said the following about the "spot monitoring" provision in the wiretap orders and the government's efforts to comply with the minimization requirement:

> Express limits on the frequency and duration of spot checks may well be impractical, as neither the government nor the authorizing court can know in advance how easy it will be for the monitoring agent to discern whether any given intercepted conversation concerns a subject within the scope of the investigation or not... Notwithstanding the language of the spot-check provision [broad reference to "criminal matters"], then, the overall terms of the orders made reasonably clear that the

> government was permitted to check intercepted conversations solely for discussions pertinent to the government's investigation, the nature and scope of which the face of the orders made clear... Although the adequacy of the government's minimization efforts necessarily depends on the facts of each case, relevant considerations include the kind and scope of criminal enterprise that the government was investigating, the thoroughness of the government's efforts to ensure that nonpertinent calls will be minimized, the extent to which the government could have foreseen that certain types of conversations would be innocuous and thus subject to minimization, use of code, and the extent to which the authorizing judge oversaw the interception efforts...If, after a review of the intercepts, the defendants believed that the government's eavesdropping was too intrusive and that a greater degree of minimization was warranted, then it was incumbent upon them to identify at least a sample of intercepted calls that proves their point...Nor do the defendants identify any concrete harms resulting from the admission of conversations which, in their view, should have been suppressed for want of appropriate minimization.

U.S. v. Mansoori, 304 F.3d 635 (7th Cir. 2002).

"We certainly agree that minimization of short calls is not required." U.S. v. Dumes, 313 F.3d 372 (7th Cir. 2002).

Suppression of only the attorney/client phone call that was inadvertently, but negligently, intercepted by a police officer monitoring a state wiretap was an appropriate remedy for the officer's violation of the amended minimization order. U.S. v. Charles, 213 F.3d 10 (1st Cir. 2000).

Errors in minimizing one particular interception within the context of a lengthy and complex investigation do not automatically warrant the suppression of all the evidence obtained through electronic surveillance. Total suppression would not follow unless the defendant demonstrates that the entire surveillance was tainted. U.S. v. Baltas, 236 F.3d 27 (1st Cir. 2001).

The Fifth Circuit uses a three-part test to determine whether the government's minimization efforts are objectively reasonable in light of the circumstances confronting the interceptor. The test considers: (1) the nature and scope of the criminal enterprise under investigation; (2) the government's reasonable inferences of the character of a conversation from the parties to it; and (3) the extent of judicial supervision. U.S. v. Brown, 303 F.3d 582 (5th Cir. 2002). See also U.S. v. Green, 2005 WL 1041205 (E.D. La.) (citing Brown).

The minimization requirement cannot reasonably be applied to clone pagers. "Because it is impossible to tell from the clone beeper whether a conversation even took place, much less the content of any conversation that might have taken place, traditional minimization requirements do not apply." U.S. v. Tutino, 883 F.2d 1125 (2d Cir. 1989); U.S. v. Gambino, 1995 WL 453318 (S.D.N.Y.).

Where drug jargon is used over the phone, the government may engage in more extensive wiretapping and the interception of innocent calls may be a more reasonable activity. U.S. v. Sanchez, 961 F.2d 1169 (5th Cir. 1992); U.S. v. Williams, 109 F.3d 502 (8th Cir. 1997).

"The Second Circuit has held that calls lasting less than two minutes need not be minimized. See U.S. v. Capra, 501 F.2d 267 (2d Cir. 1974)." U.S. v. Villegas, 1993 WL 535013 (S.D.N.Y.).

Given the large scope of the alleged conspiracy and the large amount of "short calls," the government's effort to minimize was reasonable. U.S. v. Ishola, 1996 WL 197461 (N.D. Ill. 4/19/96)

U.S. v. Parks, 1997 WL 136761 (N.D. Ill.) (excellent examination of seven factors affecting reasonableness of minimization effort).

If the government has made a prima facie showing of compliance with the statute, a defendant must overcome that showing by demonstrating that a substantial number of nonpertinent conversations have been intercepted unreasonably. Minimization is generally inapplicable to calls of less than two minutes in duration. Certain measures taken by the Government are helpful in establishing compliance with the minimization requirement: (1) maintenance of monitoring logs, (2) judicial supervision of the surveillance process, (3) the provision of written and oral instructions to monitoring personnel, and (4) supervision by the prosecutor. U.S. v. Menendez, 2005 WL 1384027 (S.D.N.Y.). See also U.S. v. Gray, 372 F. Supp.2d 1025 (N.D. Ohio 2005).

(Fax Interceptions - Electronic Communications)

In the Title III investigation of the Montana Freemen, the Ninth Circuit concluded that the minimization procedures applied to intercepted faxes (electronic communications) were adequate under the circumstances. The Title III order required that:

> Each facsimile transmission will be printed on the machine used to intercept facsimile transmissions. The monitoring agent and [assistant United States attorney] will decide, based on the identities of the sender and recipient and the subject matter of the transmission, whether the facsimile appears to be pertinent to the criminal offenses listed in the court's order. If the facsimile does not appear to be pertinent, the intercepted transmission will be placed in an envelope and sealed. It will then be placed in a locked drawer until it is turned over to the court with the other intercepted transmissions after the interception order has expired.

The ECPA and Title III do not require that the government mimic conversational minimization procedures by skipping lines in a fax and then continue reading line by line. Citing Scott v. U.S., 436 U.S. 128 (1978) and the ECPA's legislative history, the court said: "We interpret Congress's 'common sense' idea of electronic minimization to mean that law enforcement in some circumstances may look at every communication. Congress intended that the pool of investigative material be filtered. Here the district court established a reasonable procedure to eliminate irrelevant information. Under the circumstances, that is all the ECPA and Title III require. U.S. v. McGuire, 307 F.3d 1192 (9th Cir. 2002).

Other cases supporting government on the minimization issue:

U.S. v. Lucht, 18 F.3d 541 (8th Cir. 1994) (exclusion of bathrooms and bedrooms)

U.S. v. Padilla-Pena, 129 F.3d 457 (8th Cir. 1997)

U.S. v. Homick, 964 F.2d 899 (9th Cir. 1992)

U.S. v. Earls, 42 F.3d 1321 (10th Cir. 1994)

U.S. v. Moody, 977 F.2d 1425 (11th Cir. 1992)

U.S. v. Anderson, 39 F.3d 331 (D.C. Cir. 1994)

U.S. v. London, 66 F.3d 1227 (1st Cir. 1995)

U.S. v. Cleveland, 964 F. Supp. 1073 (E.D. La. 1997)

U.S. v. King, 991 F. Supp. 77 (E.D.N.Y. 1998)

U.S. v. Gruber, 994 F. Supp. 1026 (N.D. Iowa 1998)

U.S. v. Gangi, 33 F. Supp.2d 303 (S.D.N.Y. 1999)

U.S. v. Gotti, 42 F. Supp.2d 252 (S.D.N.Y. 1999)

U.S. v. Crumpton, 54 F. Supp.2d 986 (D. Colo. 1999)

U.S. v. Bankston, 182 F.3d 296 (5th Cir. 1999)

U.S. v. Pichardo, 1999 WL 649020 (S.D.N.Y.)

U.S. v. Abbit, 1999 WL 1074015 (D. Or.)

U.S. v. Soto-Del Valle, 2000 WL 816074 (D. P.R.)

U.S. v. Borrayo-Gutierrez, 119 F. Supp.2d 1168 (D. Colo. 2000)

U.S. v. Santiago, 2002 WL 104911 (S.D.N.Y.)

U.S. v. Cozzo, 2003 WL 57031 (N.D. Ill.)

U.S. v. Merton, 274 F. Supp.2d 1156 (D. Col. 2003)

U.S. v. Moran, 349 F. Supp.2d 425 (N.D.N.Y. 2005)

U.S. v. Menendez, 2005 WL 1384027 (S.D.N.Y.)

U.S. v. Le, 377 F. Supp.2d 245 (D. Me 2005)

U.S. v. Freese, 2005 WL 3005601 (D. Neb.)

Minimization After-the-Fact

"The key to after-the-fact minimization is that the process utilized must protect the suspect's privacy interests to approximately the same extent as would contemporaneous minimization, properly conducted. Accord U.S. v. Gambino, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990)." DEA told the interpreters to stop listening to a tape once they determined that the conversation was beyond the scope of the investigation. "By translating only the portions of the tapes that seemed relevant, the government's actions comported with the expectations of Congress, see, e.g., S. Rep. No. 541, 99th Cong., 2d Sess., 1, 30, reprinted in 1986 U.S. Code Cong. & Admin. News 3555, 3584, and were acceptable under Title III." U.S. v. David, 940 F.2d 722 (1st Cir. 1991). See also U.S. v. Padilla-Pena, 129 F.3d 457 (8th Cir. 1997) (Government reasonably believed intercepted calls would be in English and acted reasonably when it learned after the wiretap was activated that most of conversations were in Spanish. Fast forwarding through non-narcotics related conversations during after-the-fact monitoring was appropriate. Recorded conversations should not be erased.)

After-the-fact minimization conducted as if in “real time” satisfies reasonableness standard for minimization. U.S. v. Luong, CR-96-0094 MHP (N.D. Cal. 9/7/99).

Full recording and after-the-fact minimization of Spanish conversations was reasonable in light of pending 18 U.S.C. 2518(5) language providing for such treatment of foreign language intercepts when no expert is reasonably available. U.S. v. London, 66 F.3d 1227 (1st Cir. 1995).

Termination, Duration and Prosecutive Intent

If the objective of the intercept is to determine a conspiracy's scope, manner and participants, it does not have to terminate merely because one of the subjects has been arrested. U.S. v. Earls, 42 F.3d 1321 (10th Cir. 1994); U.S. v. Wong, 40 F.3d 1347 (2d Cir. 1994).

A wiretap may be lawfully extended where the investigating officers have not yet learned of the extent of the conspiracy and the identity of the coconspirators. U.S. v. Nguyen, 46 F.3d 781 (8th Cir. 1995).

Good faith prosecutorial/investigative decisions to seek extended Title III surveillance authority, and the good faith exercise of prosecutive discretion as to when or whether Title III interceptions will be put to prosecutive use, should have no bearing on the legality of Title III interceptions conducted in accordance with statutory requirements that embody constitutional protections articulated by the Supreme Court. U.S. v. Castellano, 610 F. Supp. 1359 (S.D.N.Y. 1985) (prosecutors are under no duty to file charges before becoming satisfied that they will be able to prove guilt at trial. Lovasco, 431 U.S. at 791, 97 S.Ct. at 2049. Even after a prosecutor has obtained enough evidence to ensure a conviction, no constitutional requirement to commence prosecution exists); U.S. v. Tortorello, 480 F.2d 764 (2d Cir. 1973) (Title III provides for the particularity, judicial supervision and other protective procedures called for in Berger v. New York, 388 U.S. 41 (1967) and Katz v. U.S., 389 U.S. 347 (1967)); U.S. v. Cafero, 473 F.2d 489 (3d Cir. 1973). United States v. Feola, 651 F. Supp. 1068 (S.D.N.Y. 1987) (eleven orders); U.S. v. Orozco, 630 F. Supp. 1418, 1525 (S.D. Cal. 1986).

Federal law "places no limit on the number of orders or extension orders that may be issued to authorize continuation of a given interception." U.S. v. Vazquez, 605 F.2d 1269 (2d Cir. 1979); U.S. v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993).

If the objective of the intercept is to determine a conspiracy's scope, manner and participants, it does not have to terminate merely because one of the subjects has been arrested. U.S. v. Earls, 42 F.3d 1321 (10th Cir. 1994); U.S. v. Wong, 40 F.3d 1347 (2d Cir. 1994).

“The government has the power and discretion to make these judgments about which crimes to investigate and how long to pursue the investigation . . . The law does not require the government to end its investigation once it finds sufficient evidence to convict one or two members of a suspected conspiracy.” U.S. v. Greer, 2004 U.S. Dist. LEXIS 20253 (S.D. Ind.).

A wiretap may be lawfully extended where the investigating officers have not yet learned of the extent of the conspiracy and the identity of the coconspirators. U.S. v. Nguyen, 46 F.3d 781 (8th Cir. 1995).

Twenty-three months of electronic surveillance of lawyer's office did not violate the Fourth Amendment. In U.S. v. Cafero, 473 F.2d 489 (3d Cir. 1973), the Third Circuit held that 18 U.S.C. 2510, et seq. satisfies the Fourth Amendment. Here the government complied with the wiretap

statute by repeatedly obtaining authorization from the district court for the continuation of the electronic surveillance. U.S. v. Sparacio, Nos. 95-2053 and 96-1616 (3d Cir. 7/28/98) (unpublished).

"Congress has chosen to guard against the possibility of indefinite wiretaps not by setting a specific limit on the duration of electronic surveillance, but by requiring a statement of the period of time for interception . . . and by requiring applications for wiretap extensions to meet the same requirements as initial applications." U.S. v. Hoang Ai Le, 255 F. Supp.2d 1132 (E.D. Cal. 2003).

Post-Interception

Sealing

2518(8)(a) requires that the Government explain why a delay occurred and also why it is excusable. U.S. v. Ojeda-Rios, 495 U.S. 257 (1990).

"Three circuits have held that recordings are sealed '[i]mmediately upon the expiration of the period of the order' if they are sealed within one or two days of the expiration. United States v. McGuire, 307 F.3d 1192, 1204 (9th Cir.2002); United States v. Wilkinson, 53 F.3d 757, 759 (6th Cir.1995); United States v. Wong, 40 F.3d 1347, 1375 (2d Cir.1994). We agree with this interpretation." U.S. v. Matthews, 411 F.3d 1210 (11th Cir. 2005).

The Seventh Circuit (Judge Posner writing for the panel), holds that the explanation offered for a ten day sealing delay by two AUSA's (no clear recollection three years after the fact, but each said she had thought the other would take care of the matter) was satisfactory under 2518(8)(a). "Ten days is too long to be thought 'immediate'. . . There was neglect, but it was harmless and therefore, while it was not justifiable, it was excusable. . . [A]n explanation is satisfactory if, in the circumstances, it dispels any reasonable suspicion of tampering. The believability of the explanation is critical, and depends in part simply on its plausibility: the more plausible, the more believable. The length of the delay is relevant as well, and also the nature of the crime, including its notoriety or the notoriety of the defendant, and thus the pressure on the government to obtain a conviction; and also the importance of the tapes to the government's case." Posner suggests that it would have been helpful had the assistant U.S. attorneys memorialized the circumstances giving rise to the delay. The Court treats the satisfactoriness determination as fact-specific and therefore appropriately treated for purposes of appellate review as a factual rather legal determination. U.S. v. Coney, 407 F.3d 871 (7th Cir. 2005).

The Ninth Circuit appointed an out-of-district judge to supervise the wiretapping in the Montana Freemen case because otherwise available federal judges in the District of Montana were recused as a result of prior bad experiences with the Freemen. The agency took special precautions to safeguard the recordings pending judicial sealing. The supervising judge by written order postponed the sealing of the recordings until he could supervise. Three times, the judge ordered the FBI to "maintain all tapes and appropriate material relating to the intercepts" until he returned to Montana to supervise sealing. When the government acts pursuant to a court's order postponing sealing, this factor is entitled to great weight in assessing whether the government has demonstrated a "satisfactory explanation" for any delay that might result. "In light of all of the above reasons, we have no doubt that any delay [in sealing] that occurred in this case [3, 12, 124, and 127 days] was justified by the exigent circumstances and that the government gave a satisfactory explanation. We hold that the FBI in this case thus did not violate Title III's prompt sealing requirement and that the sealing requirement poses no barrier to the admissibility of the challenged wiretap evidence." U.S. v. McGuire, 307 F.3d 1192 (9th Cir. 2002).

The Ninth Circuit rejected the government's attempt to apply a broader view of the term "extension" in the context of cellular telephone Title III orders issued in 1994. The circuit panel held that a 39 day delay in sealing cellular Title III recordings violated the "immediate sealing" requirements of 2518(8)(a). The circuit panel agreed with the Second and Third Circuits (U.S. v. Ojeda Rios, 875 F.2d 17 (2d Cir. 1989) and U.S. v. Vastola, 915 F.2d 865 (3d. Cir. 1990)) that an order is an extension of an earlier order only if it authorizes continued interception of the same

location or the same communications facility specified by the prior order. However, the circuit panel also held that in the instant case the actual reason for the delay in sealing was the government's mistaken belief that it could delay the sealing because later orders targeting a different cellular telephone number were extensions (the government referred to them as "extensions" in periodic progress reports to the district court and the lower court agreed with the government's view that the later orders were extensions) and the government's explanation was objectively reasonable because prior to the instant opinion, the meaning of the term "extensions" was an open question in the Ninth Circuit. Only the Second and Third Circuits had previously addressed the question. The Principie opinion (531 F.2d 1132 (2d Cir. 1976))(see above in chapter on "extensions"), although distinguishable, supported the government's theory that extensions have a broader meaning, and it has not been expressly overruled by the Second Circuit. U.S. v. Hermanek, 289 F.3d 1076 (9th Cir. 2002).

In federal trial, federal law determines whether or not the taped evidence was sealed in a timely manner. U.S. v. Vazquez, 605 F.2d 1269 (2d Cir. 1979).

By its terms, the sealing requirement only applies to subsection (3) of 2517 and not to subsection (2) or (1). U.S. v. Carson, 52 F.3d 1173 (2d Cir. 1995).

Prohibition in 2518(8)(a) on derivative use at trial of improperly sealed tapes is not to be applied strictly to prohibit use of all evidence that can be connected through a chain of causation to a wiretap tainted by improper sealing of the tape. U.S. v. Donlan, 825 F.2d 653 (2d Cir. 1987).

Use permitted by 2517(2) is not subject to the strictures of 2518(8)(a). Accomplice witness could properly refresh his recollection of various telephone conversations by listening to tapes of conversations which had been suppressed (no testimonial use under 2517(3)) because of undue delay in sealing. U.S. v. Ricco, 566 F.2d 433 (2d Cir. 1977).

The sealing requirement of §2518(8)(a) does not apply to tapes of consensual interceptions. It applies only to tapes of conversations intercepted pursuant to judicial authorization under §§ 2516 and 2518. U.S. v. Vancier, 466 F. Supp. 910 (S.D.N.Y. 1979); U.S. v. Benjamin, 72 F. Supp.2d 161 (W.D.N.Y. 1999).

The sealing requirement of section 2518(8)(a) places no restrictions on the form of the disclosure of the contents of recordings in court proceedings. As long as the government complies with Title III (sealing of original tapes), it may, at trial, disclose the contents of the recordings in whatever fashion it chooses, including the use of duplicate and compilation tapes. If Congress barred the use of duplicate tapes, the result would be unwieldy and cumbersome. Moreover, the use of duplicates allows the originals to remain sealed, thereby preserving the authenticity of the original tapes. U.S. v. Rivera, 153 F.3d 809 (7th Cir. 1998).

Numerous courts in the Second Circuit have held a two-day delay in sealing tapes does not violate the "immediate" sealing requirement of 2518(8)(a). U.S. v. Ardito, 782 F.2d 358 (2d Cir. 1986) (five day delay excused where intervening two-day holiday); U.S. v. Burford, 755 F. Supp. 607 (S.D.N.Y. 1991) (wiretap expired on Friday; tapes sealed on Monday); U.S. v. Santoro, 647 F. Supp. 153 (E.D.N.Y. 1986) (Friday expiration; Monday sealing); U.S. v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993); U.S. v. Casso, 843 F. Supp. 829 (E.D.N.Y. 1994); U.S. v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995); U.S. v. Gangi, 33 F. Supp.2d 303 (S.D.N.Y. 1999) (Friday expiration, Monday sealing).

In U.S. v. Pitera, 5 F.3d 624, (2d Cir. 1993), where the order expired on Thursday and the tapes were sealed the following Tuesday, the court held:

> Where the delay is between two and five days, we have indicated that the Government should submit with the tapes an in camera explanation of the delay. See U.S. v. Massino, 784 F.2d 153, 158 (2d Cir. 1986).
>
> Whether or not weekends are counted, the delay in this case is within the two-to five-day range. Though the Government did not attempt to explain the delay until Pitera made a motion to suppress, we agree with the District Court that the explanation is satisfactory. The Government explained that it had miscalculated the expiration date and had not thought it necessary to contact a judge at home in order to seal the tapes over the weekend. We have found satisfactory similar explanations that are based on mistake, see, e.g., U.S. v. Rodriguez, 786 F.2d 472, 477-78 (2d Cir. 1986), and difficulty in sealing tapes over a weekend, see, e.g., U.S. v. Gallo, 863 F.2d 185, 193 (2d Cir. 1988), cert. denied, 489 U.S. 1083 (1989); U.S. v. McGrath, 622 F.2d 36, 43 (2d Cir. 1980). Because the delay here was relatively short and there was no suggestion of bad faith, deliberate disregard of the statute, or tampering, the tapes need not have been suppressed. See U.S. v. Maldonado-Rivera, 922 F.2d 934, 950 (2d Cir. 1990), cert. denied, 111 S. Ct. 2811 (1991).

See also U.S. v. Wong, 40 F.3d 1347 (2d Cir. 1994).

Order expired on September 12, tapes were sealed on September 15. Although surveillance stopped on September 2, 2518(8)(a) does not require sealing until "the expiration of the period of the order." U.S. v. Gangi, 33 F. Supp.2d 303 (S.D.N.Y. 1999).

In companion unpublished opinions, the Seventh Circuit opined on the relationship between the sealing requirement and the authorization period:

> That authority ends on the date specified in the intercept order or when surveillance has achieved its objectives, whichever is sooner. *See* 18 U.S.C. § 2518(5). The wiretap's objectives in this case, as described in the authorizing order, included revealing "fully" the identities of Jackson's "confederates." Although an important confederate- Jackson's heroin source-was still unknown, the government's last intercept occurred on April 19, 1999, eighteen days before the stated May 7 expiration date. The government sealed the tapes on April 28, 1999. At a suppression hearing the agent in charge of the Jackson investigation explained that he ceased monitoring the phone because use by targets had declined, though he did not immediately seal the tapes after April 19 because the objectives of the investigation had not been achieved and he still contemplated periodically checking the phone to determine if the conspirators had resumed using it. Counsel concludes that these facts show that the government indeed sealed the tapes before it even needed to, and we agree that arguing otherwise would be frivolous. *See United States v. Wong*, 40 F.3d 1347, 1375-76 (2d Cir. 1994) (tapes need not be sealed immediately after last intercept if surveillance objectives of the wiretap have not been accomplished and government contemplates further monitoring to complete the investigation); *United States v. Badalementi,* 794 F.2d 821, 824-25 (2d Cir. 1986) (same).

U.S. v. Brown, 2002 WL 1357221 (7th Cir.)(unpublished); U.S. v. Jackson, 2002 WL 1357209 (7th Cir.)(unpublished).

Pursuant to the issuing judge's instructions in state wiretap orders, agents sealed the original tapes on a daily basis, maintained custody of the sealed tapes, and presented the tapes to the issuing judge upon the completion of the wiretap. Although this early sealing, even under the judge's directions, technically violated the requirements of 18 U.S.C. 2518(8)(a), it satisfied rudimentary demands of fair procedure and did not result in a complete miscarriage of justice and therefore a federal court may not allow the state court prisoner's habeas petition alleging violation of federal laws. Rankins v. Murphy, 198 F. Supp.2d 3 (D. Mass. 2002).

The failure to seal immediately because of resource or personnel shortages has been deemed a "satisfactory explanation." U.S. v. Pedroni, 958 F.2d 262 (9th Cir. 1992) (agent in charge of case took time to interview two potential witnesses who became available at the time when the tapes were being prepared for sealing); U.S. v. Massino, 784 F.2d 153 (2d Cir. 1986) (fifteen- day delay because government diverted personnel to investigate leak threatening investigation); U.S. v. Rodriguez, 786 F.2d 472 (2d Cir. 1986) (fourteen-day delay because supervising attorney

occupied with another trial); U.S. v. Scafidi, 564 F.2d 633 (2d Cir. 1977) (seven-day delay because prosecutor preoccupied with upcoming trial).

The unavailability of the issuing or supervising judge may constitute a satisfactory explanation for a sealing delay. U.S. v. Cline, 349 F.3d 1276 (10th Cir. 2003)(tapes were immediately "made available" to the issuing judge but actual sealing was delayed seven days due to the judge's scheduling); U.S. v. Williams, 124 F.3d 411 (3d Cir. 1997) (substitute judge directed that tapes be sealed on Monday following Friday termination of surveillance); U.S. v. Pedroni, 958 F.2d 262 (9th Cir. 1992) (issuing judge was out of town for several days after the tapes were ready for sealing); U.S. v. Fury, 554 F.2d 522 (2d Cir. 1977) (six-day delay because issuing judge was on vacation and unavailable); U.S. v. Rodriguez, 786 F.2d 472 (2d Cir. 1986)(absence of issuing judge is no longer an acceptable explanation for delay because circuit precedent has established that the tapes can be sealed by a judge other than the issuing judge); U.S. v. Maxwell, 25 F.3d 1389 (8th Cir. 1994) (judge scheduled the sealing for seven days after termination); U.S. v. Poeta, 455 F.2d 117 (2d Cir. 1972) (thirteen-day delay because agents assumed issuing judge must seal tapes); U.S. v. Blanco, 1994 WL 695396 (N.D. Cal.) (tapes were ready for sealing within three days of termination, but due to continuing unavailability of the issuing judge and other district judges, a magistrate granted the government's request for a sealing order sixteen days after termination of the interception, and upon return to the district, the issuing judge granted the government's application for an order ratifying the magistrate's sealing order); U.S. v. Lopez, 2000 U.S. Dist. LEXIS 8060 (D. Me.) (six-day delay because issuing judge unavailable; citing Poeta for suggestion that it is not improper to have tapes sealed by another judge when issuing judge is unavailable; "immediate" sealing requirement outweighs secondary concern that issuing judge should be the sealing judge); U.S. v. Wright, 156 F. Supp.2d 1218 (D. Kan. 2001)(seven-day delay due to issuing judge's schedule is a satisfactory explanation in the Tenth Circuit).

Any delay in sealing beyond two days requires a satisfactory explanation by the government. U.S. v. Vazquez, 605 F.2d 1269, 1274 (2d Cir. 1979).

Because the time gaps included intervening weekends, the sealings were "immediate" within the meaning of the statute where an order expired on Wednesday and the tapes were sealed on the following Monday and where an order expired on Thursday and the tapes were sealed on the following Wednesday. U.S. v. Carson, 969 F.2d 1480 (3d Cir. 1992).

Sealing took place on the second business day after the expiration of the order and was therefore "immediate" within the meaning of the statute. Interception ceased on Saturday. Optical Disks were sealed on following Tuesday. U.S. v. Rice, 2005 WL 2180019 (W.D. Ky.).

U.S. v. Carson, 969 F.2d 1480 (3d Cir. 1992) stands for the proposition: When a government attorney's legal conclusion is found to be unreasonable, the explanation for the delay would still be an objectively reasonable "mistake of law" if the government can show that its attorney has adequately researched the law or has otherwise acted reasonably. U.S. v. Vastola, 989 F.2d 1318 (3d Cir. 1993) (Vastola III); U.S. v. Vastola, 25 F.3d 164 (3d Cir. 1994) (affirmed district court's finding on remand that AUSA's combined reading of the law and her reliance on the opinions of more experienced colleagues on the sealing issue was minimally sufficient to meet the standards of a reasonably prudent attorney. The circuit court had previously held that the mistake of law was objectively unreasonable.)

Government's "good faith misunderstanding of the law" regarding the language of the order (that interception must terminate upon the attainment of the authorized objectives) was a satisfactory explanation of the delay in sealing under U.S. v. Ojeda-Rios, 495 U.S. 257 (1990). There was no

indication of prejudice to the defendant, or tampering and or deliberate flouting of the statutory requirement, or effort to gain tactical advantage. U.S. v. Wilkinson, 53 F.3d 757 (6th Cir. 1995).

When caused by administration difficulties, a brief hiatus between the expiration of an order and an extension will not prevent the extension from being deemed an "extension" within the meaning of section 2518(8)(a). Thus, the obligation to seal would not arise until the termination of the final extension. U.S. v. Carson, 969 F.2d 1480 (3d Cir. 1992); U.S. v. Neresesian, 824 F.2d 1294 (2d Cir. 1987) (three day gap); U.S. v. Merton, 274 F. Supp.2d 1156 (D. Col. 2003)(four day gap legally insignificant; citing Carson and Neresesian).

Delays in obtaining extensions, like delays in sealing, should be judged by practicality. Considering the practicalities involved in obtaining authority for an extension and securing the order granting it, a gap of ten days will normally satisfy the statute's immediacy requirement insofar as extensions are concerned, but a delay of that magnitude in ultimately sealing the tapes will not often satisfy the statute's immediacy requirements for sealing. U.S. v. Carson, 969 F.2d 1480 (3d Cir. 1992).

The government reasonably explained the delay between the end of the original surveillance period and the issuance of the first extension order as necessary to draft the extension affidavit and to get the request processed by the federal bureaucracy. The government sealed the tapes two weeks after the original period in a good-faith effort to comply with 2518(8)(a) "in the face of an innocent delay in processing the request for a second surveillance period." U.S. v. Plescia, 48 F.3d 1452 (7th Cir. 1995).

The government intended to obtain an extension order but when it became clear that there would be an indefinite delay in designing a new hidden microphone to replace the one discovered by the target, the government sealed its tapes 32 days after the expiration of the order. Although the prosecutor and the technicians should have communicated with each other more effectively, this failure of communication was not so wanton a blunder as “not to constitute a (barely) satisfactory explanation within the meaning of the statute.” U.S. v. Jackson, 207 F.3d 910 (7th Cir. 2000); U.S. v. Wilson, 237 F.3d 827 (7th Cir. 2001) (reiterating holding in Jackson); U.S. v. Hoover, 246 F.3d 1054 (7th Cir. 2001)(reiterating holding in Jackson; concurring opinion is critical of Jackson panel’s decision to accept as a satisfactory explanation for a 32 day sealing delay the government’s unverified assertions made only in a brief).

Where intercept is of the same premises and involves substantially the same persons, an extension requires sealing only at the conclusion of the whole surveillance. U.S. v. Scafidi, 564 F.2d 633 (2d Cir. 1977).

The fact that an extension is granted after the term of the initial authorization order has technically expired does not mean that the continuation is not an “extension” within the meaning of the statute. U.S. v. Pichardo, 1999 WL 649020 (S.D.N.Y. 8/25/99).

"While we agree that it might be better practice for the issuing judge to sign a formal order directing the sealing and custody of the tapes, and to maintain a record of that proceeding, such procedures are not required by § 2518(8)(a)." U.S. v. Gigante, 538 F.2d 502 (2d Cir. 1976). See also U.S. v. Diana, 605 F.2d 1307 (4th Cir. 1979).

Statutory sealing requirements were met where government attorney advised district judge that the tapes were available for inspection at the time he presented motions for orders sealing them, and it was not necessary that the recordings be sealed in the judge's presence. (Minimum requirements

set for sealing and custody). U.S. v. Abraham, 541 F.2d 624 (6th Cir. 1976); U.S. v. Kincaide, 145 F.3d 771 (6th Cir. 1998).

State wiretap tapes were not sealed in accordance with 2518(8)(a). Their use as evidence in federal trial where the defendant did not seek their suppression or object to their admission into evidence was held not to be plain error. The failure to seal the state wiretap recordings was not obvious to the federal trial judge, and the defendant did not demonstrate that the trial's fairness, integrity or public reputation was affected by the government's failure to properly seal the tapes. U.S. v. Gomez, 67 F.3d 1515 (10th Cir. 1995) (dissenting judge believes that admission of unsealed tapes was plain error, citing U.S. v. Ojeda-Rios, 495 U.S. 257 (1990), for the proposition that the 2518(8)(a) sealing requirement presumes prejudice if the sealing requirements are not met, and Congress has thereby preempted the requirement that the defendant prove prejudice.)

Other recent opinions holding explanation of delays reasonable:

U.S. v. Sawyers, 963 F.2d 157 (8th Cir. 1992)

U.S. v. Bennett, 825 F. Supp. 1512 (D. Colo. 1993) (five day holiday weekend delay and 13 day delay as to some tapes inadvertently overlooked)

U.S. v. Sorapuru, 902 F. Supp. 1322 (D. Colo. 1995)

[Recent opinions suppressing tapes]

Failure to immediately seal wiretap tapes was "simply matter of convenience." U.S. v. Feiste, 961 F.2d 1349 (8th Cir. 1992).

It was improper for the government to send the tapes to Washington for enhancement prior to their sealing. The government cannot delay sealing by unilaterally deciding to do something to the tapes before sealing that could just as easily be done after sealing pursuant to an unsealing order. U.S. v. Carson, 969 F.2d 1480 (3d Cir. 1992).

Suppression was ordered as to tapes that were sealed twenty days after expiration of the order. The government conceded that the tapes "were not sealed as soon as administratively practical." The government failed to supply a satisfactory explanation for the sealing delay. U.S. v. Quintero, 38 F.3d 1317 (3d Cir. 1994).

Four state wiretaps were suppressed because they were not sealed in accordance with 2518(8)(a). However, evidence from subsequent federal wiretap was not suppressed because there was sufficient untainted investigative information in the affidavit to support probable cause. U.S. v. Hernandez, 1999 U.S. Dist. LEXIS 4150 (D. Kan.).

Resealing

"[O]nce the trial level proceedings to which the unsealing order pertained have concluded, the tapes should be resealed in order to preserve their integrity should their admission be sought in another trial." Even after surveillance tapes have been used in another judicial proceeding, they may not be admitted into evidence without a judicial seal "or a satisfactory explanation for the absence thereof," 18 U.S.C. s 2518(8)(a). U.S. v. Scopo, 861 F.2d 339 (2d Cir. 1988); U.S. v. Long, 917 F.2d 691 (2d Cir. 1990); U.S. v. Boyd, 208 F.3d 638 (7th Cir. 2000) (citing Long and Scopo); U.S. v. Gigante, 979 F. Supp. 959 (S.D.N.Y. 1997).

Custody

"2518(8)(a) provides that 'custody of the recordings shall be wherever the judge orders.' The unsealing order in this case authorized the Government to unseal the tapes 'to the limited extent necessary for the Government to duplicate, disclose and otherwise make use of' them for this case." A private audio expert's "custody of the tapes for purposes of enhancement and duplication would have been consistent with this order." Even if the custody provision of 2518(8)(a) had been violated, the defendant could still not obtain relief on a section 2255 petition. See Fiumara v. U.S., 727 F.2d 209 (2d Cir. 1984) ("miscarriage of justice" standard not satisfied by "mere technical violations" of Title III); Alfano v. U.S., 555 F.2d 1128 (2d Cir. 1977) (such "technical violations" include violations of statute's sealing requirements). U.S. v. Persico, 1993 WL 385799 (S.D.N.Y.).

Notice of Inventory

Absent a showing of bad faith or actual prejudice, the failure to serve a formal inventory notice under 2518(8)(d) does not justify suppression. U.S. v. Donovan, 429 U.S. 413 (1977); U.S. v. DeJesus, 887 F.2d 114 (6th Cir. 1989); U.S. v. Davis, 882 F.2d 1334 (8th Cir. 1989); U.S. v. Savaiano, 843 F.2d 1280 (10th Cir. 1988); U.S. v. Crumpton, 54 F. Supp.2d 986 (D. Colo. 1999); U.S. v. Wright, 156 F. Supp.2d 1218 (D. Kan. 2001); U.S. v. Davis, 2004 U.S. Dist. LEXIS 4336 (E.D. Pa.).

Suppression should be required when the statutory violation arose from a conscious decision by the federal authorities to violate the law and to prevent an individual or group of individuals from receiving the post-interception notice. U.S. v. Harrigan, 557 F.2d 879 (1st Cir. 1977).

Plaintiffs (convicted narcotics dealers) brought a §1983 suit against the LAPD and the office of the Los Angeles District Attorney because those law enforcement officials intentionally concealed from the Plaintiffs (convicted narcotics dealers) the existence of state wiretaps that brought the Plaintiffs to the attention of law enforcement officials. The Plaintiffs were neither identified in the wiretap order nor under investigation at the time of the wiretap. The wiretap was the sole source of the authorities' awareness of the Plaintiffs' illicit activities. The Plaintiffs were not informed of the wiretaps until long after their indictments, convictions and confinement. The "hand off" procedure was designed to allow law enforcement officials to make use of the incriminating evidence derived from the wiretap, while at the same time, preventing the defendants from ever learning of the existence of the wiretap. Information from the wiretap is transmitted to a separate police unit, without expressly stating that the information comes from a wiretap. The receiving unit is told to "investigate." The receiving unit then develops "independent" probable cause upon which an arrest can be made or a search warrant obtained. ("Defendants seem to believe that the 'hand off' creates a hermetic seal between the wiretap and the post-"hand off" investigation. The Court disagrees, believing instead that the 'hand off' creates an iron chain that inextricably links the two phases together.") The subject is then prosecuted without ever knowing that he was subjected to the wiretap surveillance. No mention is made of the wiretap in any police reports, discovery disclosures, or by testifying detectives who belong to the receiving unit. "The Court finds that the wiretapping "hand off" procedure, rather deliberately and openly, conflicts with Title III's notice safeguard [18 U.S.C. 2518(8)(d)]. In light of Title III's inextricable intertwinement with the Fourth Amendment . . .the wiretapping "hand off" procedure cannot withstand constitutional scrutiny." The California State wiretap statute inventory notice provision was violated by the government because it failed to disclose information to the court that would have caused the judge to order inventory notice for Plaintiffs. See analogous reasoning in the

federal context, U.S. v. Chun, 503 F.2d 533 (9th Cir. 1974)("the unnamed but overheard are also entitled to Fourth Amendment protection. Specifically, we believe that when the government intends to use the contents of an interception or evidence derived therefrom, to obtain an indictment against an unnamed but overheard individual, such individual must be given notice promptly after the decision to obtain an indictment has been made). The Court grants the Plaintiffs' motion for summary judgment with respect to their §1983 declaratory judgment claim for the per se unconstitutionality of the wiretapping "hand off" procedure." The "hand off" procedure violates both the right to be free from unreasonable searches and seizures (concealing the existence of the wiretap eliminates any challenge to the legal validity of the warrant) and the right to due process of law (under the Brady exculpatory evidence doctrine a criminal defendant has a right to discover the existence of an illegal search). The criminal defendant has a constitutional right to know that he has been subjected to a Fourth Amendment search from which the investigation against him originally arose. "[T]he Court believes that (1) the preservation of the substance of the Fourth Amendment, (2) an analysis of the specified safeguards of the Federal Wiretapping Statute, and (3) a proper understanding of the notion of "independence" all promote a common holding, namely, the per se unconstitutionality of the wiretapping 'hand off' procedure." Because this is an issue of first impression, the law enforcement officials are entitled to qualified immunity on this claim. Whitaker v. Garcetti, 291 F. Supp.2d 1132 (C.D. Cal. 2003).

After service of inventory notice pursuant to 18 U.S.C. 2518(8)(d), the judge, upon filing of a motion, may in his discretion make available for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. The notice of inventory does not compel immediate disclosure of the fruits of the surveillance. The government's decision not to postpone the service of the inventory is not a waiver of the right to oppose disclosure of matters not within the scope of the inventory. "Reconciling § 2520 and § 2518(8)(d) 'is principally a question of timing,'" Application of the United States of America in the Matter of an Order Authorizing the Interception of Wire Communications, 413 F. Supp. 1321 (E.D. Pa. 1976)(emphasis in original). "In camera inspection is the only practical way simultaneously to preserve the interests of the individual under surveillance and the interest of the Government in preserving the secrecy of ongoing criminal investigations." Stoddard v. U.S., 710 F.2d 21 (2d Cir. 1983). See also In re Warrant Authorizing Interception of Oral Communications, 708 F.2d 27 (1st Cir. 1983).

Disclosure

2517 and 2515

The USA Patriot Act and the Homeland Security Act expanded the disclosure authority in 18 U.S.C. 2517 by adding Section 2517(6) (disclosure to Intelligence Community), 2517(7)(disclosure to foreign investigative or law enforcement officers), and 2517(8) (disclosure to federal, state, local or foreign government officials of threats of attack, grave hostile acts, sabotage, terrorism, or spying by foreign powers or their agents).

Foreign law enforcement officers are not included within the definition of "investigative or law enforcement officer" (18 U.S.C. 2510(7)). In a letters rogatory proceeding under 18 U.S.C. 1782, the Government agreed to disclose Title III applications, affidavits and orders but declined to release records of intercepted communications. The district court did not abuse its discretion in declining to order the Government to disclose Title III interceptions. The district court gave the required respect to the English court's order and the important considerations of comity underlying 18 U.S.C. 1782, but recognized that competing domestic law enforcement and privacy concerns articulated by the Government justified withholding some (but not all) of the items in question. Involuntary disclosures of wiretap material are not permitted by 18 U.S.C. 2517 (1) and (2). United Kingdom v. United States of America, 238 F.3d 1312 (11th Cir. 2001).

"When addressing disclosure of the contents of a wiretap, the question is whether Title III specifically authorizes such disclosure, not whether Title III specifically prohibits the disclosure, for Title III prohibits all disclosures not authorized therein." In re: Motion to Unseal Electronic Surveillance Evidence, 990 F.2d 1015 (8th Cir. 1993) (en banc) (citing U.S. v. Underhill, 813 F.2d 105 (6th Cir. 1987) and U.S. v. Dorfman, 690 F.2d 1230 (7th Cir. 1982)).

"No party in a criminal case, including the government, has the unilateral right to disclose in a brief, press release or otherwise, at least prior to the introduction into evidence at either a hearing or trial, intercepted communications or grand jury materials." Defendant, pursuant to the Court's protective order, sealed its pretrial motion containing excerpts from Title III intercepts, but the government's response, containing Title III materials, was not sealed. The better practice for the government would have been to seek the court's guidance on this point. The Court rejected the government's position that Title III materials can be released merely because they have been attached to pretrial motions and/or designated for use at trial. U.S. v. Kemp, 365 F. Supp.2d 618 2005 U.S. Dist. LEXIS (E.D. Pa.) (contains a comprehensive discussion of the issues and case law concerning pretrial release of Title III materials in a public corruption case).

Title III does not forbid the government to make public disclosure of criminal charges even if the charges include information obtained from wiretapping, Smith v. SEC, 129 F.3d 356, 363 (6th Cir. 1997), unless the criminal proceedings are themselves nonpublic, U.S. v. Dorfman, 690 F.2d 1230 (7th Cir. 1982); Certain Interested Individuals v. Pulitzer Publishing Co., 895 F.2d 460 (8th Cir. 1989); In re New York Times Co., 828 F.2d 110 (2d Cir. 1987), and here, as is normally the case, they were public. We cannot find anything in Title III that would bar the government from summarizing the evidence in the indictment and from publicizing the indictment in the same way that it would publicize an indictment not based on evidence obtained by means of wiretapping. The specific charge against the defendant was that he supplied heroin from Nigeria to the United States, and if true that made him an international heroin supplier. The charge was contained in a public indictment, and the government was entitled to announce the indictment publicly. Aversa

v. U.S., 99 F.3d 1200 (1st Cir. 1996). Once privileged information is properly disclosed in a public proceeding, the publicizing of the proceeding is not a violation of the privilege. This principle has been established in cases involving press releases announcing indictments based in part on confidential information in tax returns and grand jury proceedings, Johnson v. Sawyer, 120 F.3d 1307 (5th Cir. 1997); Lampert v. U.S., 854 F.2d 335 (9th Cir. 1988); Stepanian v. Addis, 699 F.2d 1046 (11th Cir. 1983), and its application to Title III is assumed in U.S. v. Jennings, 842 F.2d 159 (6th Cir. 1988), endorsed in In re Globe Newspaper Co., 729 F.2d 47 (1st Cir. 1984) (dictum), and implicit in Title III's authorization of law enforcement personnel who have lawfully obtained knowledge of intercepted communications to "use [the] contents [of the communications] to the extent such use is appropriate to the proper performance of [their] official duties." 18 U.S.C. §§ 2510(7), 2517(2). Apampa v. Layng, 157 F.3d 1103 (7th Cir. 1998); U.S. v. Vanmeter, 278 F.3d 1156 (10th Cir. 2002) (citing Apampa; federal agent was within his official duty when he briefly quoted and paraphrased intercepted telephone communications to establish probable cause in a criminal complaint for defendant's arrest).

District court granted defendant's (Mayor of Waterbury, CT) motion to seal complaint affidavit containing Title III intercepts. Defendant's request to close the bail hearing was also granted. The court concluded that "there is a substantial probability that the defendant's Sixth Amendment right to a fair trial as well as his privacy rights under Title III will be prejudiced by pretrial public disclosure of the information contained in the affidavit and disclosed at the bail hearing, and there are no reasonable alternatives to closure that would adequately protect the defendant's rights. The public's qualified right of access to the information does not outweigh the defendant's paramount rights." The court said its ruling is subject to reconsideration if a suppression hearing establishes that the Title III interceptions were lawfully obtained. U.S. v. Giordano, 158 F. Supp.2d 242 (D. Conn. 2001).

Until a determination has been made whether tapes of allegedly consensual interceptions were in fact obtained with consent, public disclosure of the contents of the tapes is prohibited by 18 U.S.C. §§ 2511(1)(c), 2517. Unless such a determination has been made, the tapes are not admissible at trial, §§ 2515, 2518(10). U.S. v. Cianfrani, 573 F.2d 835 (3d Cir. 1978); U.S. v. Vancier, 466 F. Supp. 910 (S.D.N.Y. 1979).

Although 18 U.S.C. 2518(8)(b) only refers specifically to "applications" and "orders," we construe "applications" to include any related necessary documentation such as affidavits and progress reports. In re Grand Jury Proceedings, 841 F.2d 1048 (11th Cir. 1988).

"[W]here an affidavit supplies the information required by the statute to be included in the application, it must be considered part of the application. To the extent, then, that Title III requires that the application be released, affidavits that are part of the application must also be released" (referring to 18 U.S.C. 2518(9)). U.S. v. Arreguin, 277 F. Supp.2d 1057 (E.D. Cal. 2003).

In Fleming v. U.S., 547 F.2d 872 (5th Cir. 1977), the court found that the wiretap statute is ambiguous on the question of disclosure and that the statute does not make clear the interaction between sections 2517 and 2515. Spatafore v. U.S., 752 F.2d 415 (9th Cir. 1985) followed Fleming. In both of these cases, the interceptions had been made part of the public record in criminal proceedings.

U.S. v. Cleveland, 1997 WL 178644 (E.D. La. 4/7/97) and U.S. v. Cleveland, 964 F. Supp. 1073 (E.D. La. 1997) (suppression denied for unsealing of search warrant affidavits containing Title III interceptions): Fleming v. U.S., 547 F.2d 872 (5th Cir. 1977) precludes suppression of improperly disclosed wiretap interceptions. Other circuits have applied Fleming in other contexts, including that of improper disclosures to the press. See U.S. v. Cardall, 773 F.2d 1128 (10th Cir. 1985)

(sole remedy for violations of 18 U.S.C. s 2517 is civil action under 18 U.S.C. 2520); Dickens v. U.S., 671 F.2d 969 (6th Cir. 1982) (finding suppression remedy appropriate only for wiretap evidence that has been illegally seized and not for evidence that has merely been improperly disclosed); U.S. v. Horton, 601 F.2d 319 (7th Cir. 1979) (main thrust of 18 U.S.C. 2515 is to exclude evidence illegally seized, not evidence the disclosure of which was in violation of chapter 119 of the United States Code); U.S. v. Iannelli, 477 F.2d 999 (3d Cir. 1973) (suppression remedy specified in 18 U.S.C. 2518(10) applies to unlawful interceptions, whereas a civil remedy applies to unlawful disclosures); U.S. v. Dorfman, 532 F. Supp. 1118 (N.D. Ill. 1981) (refusing to apply remedy of suppression as a matter of law when defendants alleged that the government disclosed material obtained from wiretaps and other electronic surveillance to the press in violation of 18 U.S.C. 2517).

The Sixth Circuit finds the language of 2517(2) unclear as to when a disclosure is permitted "use." Resha v. United States, 767 F.2d 285 (6th Cir. 1985).

Section 2517(2) authorizes use of wiretap information in trial briefs and memoranda, U.S. v. Gerena, 869 F.2d 82 (2d Cir. 1989); to refresh recollection of a witness prior to trial, even though tapes were suppressed for testimonial use under 2517(3) due to sealing delay, U.S. v. Ricco, 566 F.2d 433 (2d Cir. 1977); and for purposes of voice identification, U.S. v. Rabstein, 554 F.2d 190 (5th Cir. 1977) and U.S. v. Martinez, 1996 WL 281570 (2d Cir. 5/21/96)(unpublished) (citing Ricco).

The use of “other offense” information by law enforcement officers to prepare a search warrant affidavit is not "testimonial" in nature (Section 2517(3)) such that prior approval (Section 2517(5)) of a judicial officer is needed. Section 2517(5) permits “other offense” disclosure or use under 2517(1) and (2), under which the "proper performance of his official duties" includes the use of the information for such uses as establishing probable cause to search. See U.S. v. Vento, 533 F.2d 838 (3rd Cir. 1976); U.S. v. O’Neill, 52 F. Supp.2d 954 (E.D. Wis. 1999) (citing Vento).

"The disclosures to the secretaries and intelligence analyst were probably valid under section 2517(2). In any event, the remedy of suppression is available for wrongful disclosure under Title III only if the conditions set forth in 18 U.S.C. 2518(10)(a) are satisfied." U.S. v. O'Connell, 841 F.2d 1408 (8th Cir. 1988). See also U.S. v. Le, 2005 U.S. Dist. LEXIS 156 (D. Minn.)(per 2518(5), lay Vietnamese translators were under contract and supervised by a federal agent)(citing O’Connell).

Wisconsin electronic surveillance statutory provisions virtually identical to 18 U.S.C. 2517 (1) and (2) bar the state from including legally intercepted communications in a criminal complaint unless the complaint is filed under seal. This statutory reading honors the statutory distinction between "use" and "disclosure" and respects the statute's purpose to protect privacy. The state is not permitted to unilaterally disclose the contents of intercepted communications to the public at large. The statutory suppression remedy would be undermined if interceptions were disclosed to the public before a court had ruled on the legality of the interceptions. State v. Gilmore, 549 N.W.2d 401 (Wis. 1996).

The legislative history, S. Rep. No. 1097, 90th Cong., 2d Sess., reprinted in 1968 U.S. Code Cong. & Admin. News 2112, 2188, states that neither 2517(1) nor 2517(2) are "limited to evidence intercepted in accordance with the provisions of the proposed chapter, since in certain limited situations disclosure and use of illegally intercepted communications would be appropriate to the proper performance of the officers' duties. For example, such use and disclosure would be necessary in the investigation and prosecution of an illegal wiretapper himself. (See United States v. Gris, 146 F. Supp. 293 (S.D.N.Y. 1956), aff'd, 247 F.2d 860 (2d Cir. 1957)."

"Since receipt and use of wiretap evidence is plainly appropriate for Assistant United States Attorneys prosecuting a civil forfeiture proceeding, disclosure of wiretap evidence to them would seem covered by § 2517(1)." AUSAs, whether working on criminal or civil matters, fall within the § 2510(7) definition of an "investigative or law enforcement officer." U.S. v. All Right, Title and Interest . . ., 830 F. Supp. 750 (S.D.N.Y. 1993).

A House committee conducting inquiry into whether impeachment proceedings are warranted falls within the definition of "investigative officer" contained within 18 U.S.C. 2517(1). In re Grand Jury Proceedings, 841 F.2d 1048 (11th Cir. 1988).

An investigation for an attorney grievance commission is an investigative or law enforcement officer within the meaning of 18 U.S.C. 2517(1). In re Electronic Surveillance, 596 F. Supp. 991 (E.D. Mich. 1984).

The Grievance Administrator of the Michigan Attorney Grievance Commission is an officer empowered to investigate enumerated offenses when those offenses are committed by members of the State Bar of Michigan, and therefore his receipt and use of Title III information was appropriate. Congress clearly intended that the phrase "investigative or law enforcement officer" is not limited to those who enforce criminal law. The text of 2517(1) clearly envisions receipt of Title III information by state officers. The history of 2517(3) also supports this conclusion. "Prior to 1970, disclosure of intercepted communications could only be made in connection with state and federal criminal proceedings. Congress amended the subsection (3) in that year to allow disclosure in any authorized proceeding . . . . Pub.L. No. 91-452, § 902(b), 84 Stat. 947 (1970) . . . . We think that the 1970 amendment makes clear that, once conversations are lawfully intercepted, disclosure is not restricted to criminal proceedings." In re Electronic Surveillance; Berg v. Michigan Attorney Grievance Commission; U.S., 49 F.3d 1188 (6th Cir. 1995).

"Hand Off" Procedure

Plaintiffs (convicted narcotics dealers) brought a §1983 suit against the LAPD and the office of the Los Angeles District Attorney because those law enforcement officials intentionally concealed from the Plaintiffs (convicted narcotics dealers) the existence of state wiretaps that brought the Plaintiffs to the attention of law enforcement officials. The Plaintiffs were neither identified in the wiretap order nor under investigation at the time of the wiretap. The wiretap was the sole source of the authorities' awareness of the Plaintiffs' illicit activities. The Plaintiffs were not informed of the wiretaps until long after their indictments, convictions and confinement. The "hand off" procedure was designed to allow law enforcement officials to make use of the incriminating evidence derived from the wiretap, while at the same time, preventing the defendants from ever learning of the existence of the wiretap. Information from the wiretap is transmitted to a separate police unit, without expressly stating that the information comes from a wiretap. The receiving unit is told to "investigate." The receiving unit then develops "independent" probable cause upon which an arrest can be made or a search warrant obtained. ("Defendants seem to believe that the 'hand off' creates a hermetic seal between the wiretap and the post-"hand off" investigation. The Court disagrees, believing instead that the 'hand off' creates an iron chain that inextricably links the two phases together.") The subject is then prosecuted without ever knowing that he was subjected to the wiretap surveillance. No mention is made of the wiretap in any police reports, discovery disclosures, or by testifying detectives who belong to the receiving unit. "The Court finds that the wiretapping "hand off" procedure, rather deliberately and openly, conflicts with Title III's notice safeguard [18 U.S.C. 2518(8)(d)]. In light of Title III's inextricable intertwinement with the Fourth Amendment . . .the wiretapping "hand off" procedure cannot withstand constitutional scrutiny." The California State wiretap statute inventory notice provision

was violated by the government because it failed to disclose information to the court that would have caused the judge to order inventory notice for Plaintiffs. See analogous reasoning in the federal context, U.S. v. Chun, 503 F.2d 533 (9th Cir. 1974)("the unnamed but overheard are also entitled to Fourth Amendment protection. Specifically, we believe that when the government intends to use the contents of an interception or evidence derived therefrom, to obtain an indictment against an unnamed but overheard individual, such individual must be given notice promptly after the decision to obtain an indictment has been made). The Court grants the Plaintiffs' motion for summary judgment with respect to their §1983 declaratory judgment claim for the per se unconstitutionality of the wiretapping "hand off" procedure." The "hand off" procedure violates both the right to be free from unreasonable searches and seizures (concealing the existence of the wiretap eliminates any challenge to the legal validity of the warrant) and the right to due process of law (under the Brady exculpatory evidence doctrine a criminal defendant has a right to discover the existence of an illegal search). The criminal defendant has a constitutional right to know that he has been subjected to a Fourth Amendment search from which the investigation against him originally arose. "[T]he Court believes that (1) the preservation of the substance of the Fourth Amendment, (2) an analysis of the specified safeguards of the Federal Wiretapping Statute, and (3) a proper understanding of the notion of "independence" all promote a common holding, namely, the per se unconstitutionality of the wiretapping 'hand off' procedure." Because this is an issue of first impression, the law enforcement officials are entitled to qualified immunity on this claim. Whitaker v. Garcetti, 291 F. Supp.2d 1132 (C.D. Cal. 2003).

2518(8)(d) Inspection After Inventory Notice

After service of inventory notice pursuant to 18 U.S.C. 2518(8)(d), the judge, upon filing of a motion, may in his discretion make available for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. The notice of inventory does not compel immediate disclosure of the fruits of the surveillance. The government's decision not to postpone the service of the inventory is not a waiver of the right to oppose disclosure of matters not within the scope of the inventory. "Reconciling § 2520 and § 2518(8)(d) 'is principally a question of timing,'" Application of the United States of America in the Matter of an Order Authorizing the Interception of Wire Communications, 413 F. Supp. 1321 (E.D. Pa. 1976)(emphasis in original). "In camera inspection is the only practical way simultaneously to preserve the interests of the individual under surveillance and the interest of the Government in preserving the secrecy of ongoing criminal investigations. Stoddard v. U.S., 710 F.2d 21 (2d Cir. 1983). See also In re Warrant Authorizing Interception of Oral Communications, 708 F.2d 27 (1st Cir. 1983).

2518(9)

The purpose of the ten day notice requirement in 18 U.S.C. 2518(9) is to afford the defendant "an opportunity to make a pretrial motion to suppress...." S.Rep. No. 1097, 90th Cong., 2d Sess. 105-06, reprinted in 1968 U.S. Code Cong. & Ad.News 2112, 2195. Section 2518(9) also provides that the court may waive the ten-day requirement upon a finding that it was not possible to furnish the required documents timely and that no prejudice will result. In this case the District Court made the requisite findings, which are abundantly supported in the record. The bulk of the required material was furnished a week before the detention hearing of the first defendant, and all defendants were able to make a motion to suppress the results of the electronic surveillance. U.S. v. Melendez-Carrion, 790 F.2d 984 (2d Cir. 1986).

Court properly admitted wiretap evidence despite government's violation of § 2518(9); counsel in Florida proceeding had material, so new counsel in Connecticut proceeding had access. U.S. v. Berrios-Berrios, 791 F.2d 246 (2d Cir. 1986).

The government plainly violated 2518(9), but to effect a reversal of his conviction, the defendant must show that this violation caused him prejudice. Although the government failed to furnish the applications themselves, it notified the defendants that it intended to introduce evidence from the Virginia wiretap and offered to provide the defendants with the application and order well in advance of trial. Defendant's failure to object before trial probably constitutes a waiver. U.S. v. Goodwin, 1997 WL 767408 (2d Cir.)(unpublished)(citing Melendez-Carrion and Berrios-Berrios).

The court ruled that the Government violated 2518(9), stopped the trial before any of the wiretap evidence was introduced and gave the Defendants more than ten days to file their motions to suppress. The motions were ultimately denied, and trial was resumed six weeks later. The court rejected the Defendants' contention that they were prejudiced simply by the fact that the Government failed to provide the required materials ten days before trial. Such a position would convert 2518(9) into a strict liability statute and would mean that once it was violated, the underlying evidence could never be used. Defendants offered no legal support for such an interpretation. The purpose of the 10-day requirement "is to give the defendant an opportunity to make a pretrial motion to suppress wiretap evidence." U.S. v. Caro, 965 F.2d 1548, 1554 (10th Cir. 1992). In order to justify the reversal of a conviction, the violation of § 2518(9) must have caused the defendant prejudice. U.S. v. Winter, 663 F.2d 1120, 1154 (1st Cir. 1981). U.S. v. Tyler, 2002 WL 1354122 (10th Cir.)(unpublished).

Section 2518(9) requires only that a defendant be furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. "There is no statutory requirement that all recordings made pursuant to the court order be produced. To the contrary, Section 2518(10)(a) specifically provides that it rests within the discretion of the trial court to decide whether intercepted communications should be furnished to a defendant." U.S. v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995).

Although the Government failed to furnish the defendants with the Virginia wiretap application and order at least ten days before the commencement of trial, as required by 18 U.S.C. § 2518(9), the Court of Appeals found no ground for reversal. Defense counsel had not objected and the Government, well in advance of trial, notified the defendants that it intended to introduce evidence from the Virginia wiretap and offered to provide the defendants with the application and order. This circumstance, together with the fact that the evidence supporting the defendant's conviction was overwhelming, caused the Court of Appeals to hold that reversal of the conviction on this ground "would be highly inappropriate." There is no basis for § 2255 relief on the ground of inadequate counsel. Piggott v. U.S., 2003 U.S. Dist. LEXIS 228 (S.D.N.Y.).

The district court suppressed wiretap-related evidence because the government failed to provide the defendant, as required by 18 U.S.C. 2518(9), with a copy of the wiretap order ten days before the hearing on the defendant's motion to suppress. Three months later, the case was dismissed without prejudice for violations of the Speedy Trial Act. The government re-indicted the defendant a few days later. Although the Court found the government's representations to the Court to have been disingenuous (it really did intend to let the speedy trial clock run so that it could reprosecute and avoid the effect of the suppression ruling), and its actions to be prejudicial to the defendant, the Court denied the defendant's motions to dismiss for vindictive prosecution and to suppress the wiretap evidence on collateral estoppel or "issue preclusion" grounds. The suppression ruling in the first case was not a "final and valid judgement" but merely a discovery sanction, not a suppression order based on a Fourth Amendment or other Constitutional violation

or a violation of the Wiretap Act that affected the manner in which the wiretapping-related evidence was obtained. The Government was not, therefore, estopped from using the previously suppressed wiretap evidence in reprosecution. U.S. v. Harvey, 243 F. Supp.2d 359 (D. Virgin Islands 2003).

While 2518(9) provides the defendant with due process rights to wiretap applications and orders, the 2518(8)(b) "good cause" requirement makes it clear that the defendant is entitled only to that information that is relevant to his defense and is not protected from disclosure by some other constitutional right or privilege. Even a mandatory statutory provision is still subject to constitutional considerations. U.S. v. Yoshimura, 831 F. Supp. 799 (D. Hawaii 1993). This court cites the following cases where courts have held that certain information in the application and order may be redacted after in camera review: Application of U.S. for an Order Authorizing Interception of Wire and Oral Communications, 495 F. Supp. 282 (E.D. La. 1980); U.S. v. Ferle, 563 F. Supp. 252 (D. R.I. 1983); U.S. v. Brown, 539 F.2d 467 (5th Cir. 1976); U.S. v. Buckley, 586 F.2d 498 (5th Cir. 1978).

On August 7, 2003, a senior district judge in the Eastern District of California ordered the government to provide to each party unredacted copies of a state wiretap application and order used to support a federal wiretap. The court rejected the government's attempt to redact the state wiretap affidavit to protect an informant's identity and to avoid jeopardizing an ongoing investigation. "[A]lthough *Roviaro* [*Roviaro v. U.S.*, 353 U.S. 53 (1957)] governs where a defendant asserts that due process dictates disclosure, it does not govern where the defendant asserts a right under the disclosure provisions of Title III's more stringent statutory scheme. . .Because the plain language of Title III does not provide for disclosure of redacted applications and orders under § 2518(9), and given the legislative purpose of providing more stringent requirements under Title III than those found by the courts in the Constitution, I must conclude that the government is required to disclose wiretap applications and orders in their entirety before it may use evidence derived from such wiretaps." U.S. v. Arreguin, 277 F. Supp.2d 1057 (E.D. Cal. 2003)(Yoshimura case (see above) rejected as unpersuasive).

Search Warrant Affidavits

Section 2517(2) authorizes the use of wiretap information in search warrant affidavits. The legislative history of Title III so indicates. S. Rep. No. 1097, 90th Cong., 2d Sess., reprinted in 1968 U.S. Code Cong. & Admin. News 2112, 2188. Disclosure under 2517(2) is limited by the scope of the investigative or law enforcement officer's official duties. Where FBI agents use wiretap information to prepare search warrant affidavits in performance of their official duties, they lawfully disclose the wiretap information only to others who, as noted by Judge Posner in U.S. v. Dorfman, 690 F.2d 1230 (7th Cir. 1982), are "professionally interested stranger(s)." Disclosure to a limited audience of "professionally interested strangers" in the context of their official duties is not the equivalent to disclosure to the public. "Title III does not allow public disclosure of all lawfully obtained wiretap evidence just because a few officers are privy to its contents; if it were construed to do so, much of the statute would be superfluous, for example, 18 U.S.C. §§ 2517(1)-(3)." Id. at 1234-35. Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990).

Qualified First Amendment right of access applies to documents filed in support of search warrant applications. Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990).

No First Amendment right of access to search warrant affidavit; common law right of access only. In re Baltimore Sun Co., 886 F.2d 60 (4th Cir. 1989). See also Application of Newsday, Inc., 895 F.2d 74 (2d Cir. 1990).

No First Amendment or common law right of access to search warrant affidavits. Times Mirror Co. v. U.S., 873 F.2d 1210 (9th Cir. 1989).

Disclosure of wiretap information in search warrant affidavit is not the testimonial disclosure contemplated in 2517(3) even though affidavits are prepared under oath or affirmation. Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990).

Use and disclosure of wiretap information in search warrant affidavits did not remove that information from protection of nondisclosure provisions of Title III. Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990); U.S. v. Shenberg, 791 F. Supp. 292 (S.D. Fla. 1991).

Redaction or sealing of intercepted conversations in order to protect privacy interests is permissible if district judge finds that important privacy interests cannot otherwise be protected and those interests outweigh public's interest in access; procedural posture of government's criminal investigation must be considered in balancing process, and absence of indictment weighs heavily in favor of privacy interest and nondisclosure. Even redacted versions of search warrant affidavits could not be disclosed prior to indictment of individuals whose privacy interests might be compromised by disclosure of wiretap information. Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990). See also Application of Newsday, Inc., 895 F.2d 74 (2d Cir. 1990).

Publisher did not have qualified First Amendment right of public access to sealed wiretap materials and search warrant affidavits following the return of indictments but prior to a substantive challenge to those materials. U.S. v. Inzunza, 303 F. Supp.2d 1041 (S.D. Cal. 2004).

Affidavit Portrayal of Wiretap as Confidential Reliable Human Source

Chief Judge Patel granted the defendant's motion to suppress because the affiant in a state search warrant affidavit referred to a federal wiretap as a "Confidential Reliable Source," and thereby mislead the issuing magistrate. The affidavit's portrayal of investigators' evaluations of wiretap evidence as the first-hand reports of a reliable witness showed a reckless disregard for truth in the factual assertions set forth in the affidavit upon which the magistrate's finding was based. By describing the wiretap as if it were a human informant, the affiant made a proper determination of probable cause impossible. Law enforcement is not permitted to make misrepresentations in warrant affidavits in order to protect the confidentiality of their sources. Judge Patel suggested the following ways to protect confidential information sources used in search warrant applications:

> [Affiant] could have submitted the warrant affidavit under seal, submitted a redacted affidavit along with an unredacted one to be sealed, or disclosed the nature of the source to the reviewing magistrate in *in camera* sealed proceedings. Furthermore, so that the magistrate has the actual facts to support probable cause rather than the affiant's characterizations, the magistrate must be advised of what is fact and what is characterization. The way to accomplish this is to set forth the pertinent conversation and then interpret them where code or other obscure language is used. Law enforcement must pursue those means of protecting investigations which do not risk compromising the protections of the Fourth Amendment. . .
>
> At least two federal courts have refused to hold a warrant invalid where the affidavit described a wiretap as a 'confidential informant,' but in those cases the magistrate was informed orally of the

> true nature of the source. *United States v. Glinton*, 154 F.3d 1245, 1255 (11th Cir.1998), *cert. denied*, 526 U.S. 1032, 119 S.Ct. 1281, 143 L.Ed.2d 374 (1999); *United States v. Cruz*, 594 F.2d 268, 271-72 (1st Cir.), *cert. denied*, 444 U.S. 898, 100 S.Ct. 205, 62 L.Ed.2d 133 (1979). In each of case, the deciding court emphasized that because of the affiant's oral disclosure, the magistrate had not actually been misled as to any facts. Another federal court of appeals cautioned that mislabeling wiretaps as human informants could affect the determination of probable cause. *United States v. Johnson*, 696 F.2d 115, 118 n. 21 (D.C.Cir.1982). Finally, at least one state court has actually excluded evidence gained from a search warrant in which the facts attested to by the 'confidential reliable source' described in the warrant affidavit turned out to be summaries of wiretap evidence provided to the affiant by a police officer in another state. *Florida v. Beney*, 523 So.2d 744 (Fla. Ct. App. 1988).

U.S. v. McCain, 271 F. Supp.2d 1187 (N.D. Cal. 2003)

Suppression Hearing Exhibits

Because the public has a qualified First Amendment right of access to hearings on motions to suppress and documents on which suppression decisions are based, the court granted a newspaper's request for access to a suppression hearing exhibit, introduced by the defendant, that contained a preliminary transcript of a conversation intercepted pursuant to Title III. The interests of intervening defendants and third parties (neither group were participants in the intercepted conversation), and the preliminary nature of the transcript (there were no material inaccuracies) were not sufficient to overcome the public's qualified right of access to what the government described as "unlitigated Title III material." The government did not claim that disclosure would interfere with ongoing criminal investigations or compromise informant safety. Participants in subject conversation did not oppose disclosure. Rigorous voir dire is available to counter the effect of adverse publicity on the trials of the intervening defendants. U.S. v. White, 855 F. Supp. 13 (D. Mass. 1994).

“No party in a criminal case, including the government, has the unilateral right to disclose in a brief, press release or otherwise, at least prior to the introduction into evidence at either a hearing or trial, intercepted communications or grand jury materials.” Defendant, pursuant to the Court’s protective order, sealed its pretrial motion containing excerpts from Title III intercepts, but the government’s response, containing Title III materials, was not sealed. The better practice for the government would have been to seek the court’s guidance on this point. The Court rejected the government’s position that Title III materials can be released merely because they have been attached to pretrial motions and /or designated for use at trial. U.S. v. Kemp, 365 F. Supp.2d 618 2005 U.S. Dist. LEXIS (E.D. Pa.) (contains a comprehensive discussion of the issues and case law concerning pretrial release of Title III materials in a public corruption case).

Use of Illegal Interceptions

Notwithstanding the prohibition of 18 U.S.C. 2511(1)(c), the First Amendment protects the knowing disclosure of illegally intercepted communications if the communications deal with a matter of public concern and the person making the disclosure played no part in the illegal interception and lawfully obtained access to the communications. Bartnicki v. Vopper, 121 S. Ct. 1753 (2001).

"We hold that, under the unique facts and circumstances of this case--including that the appellees did not participate in or procure the interception [illegally conducted by private parties], and obtained knowledge of the intercepted communications from third parties who made serious charges that an officer was engaged in administrative and criminal misconduct--the appellees'

disclosure and use of the information from the intercepted communications, in conducting a preliminary internal affairs investigation, was authorized by §§ 2517(1) and (2). We caution that this holding is narrow, limited to the facts of this case. It should not be read as undermining the salutary purpose of the Act, or as providing a means of sidestepping it." Forsyth v. Barr, 19 F.3d 1527 (5th Cir. 1994).

As a "clean hands" exception to 18 U.S.C. § 2515, the government may use illegally intercepted communications against the victim of the illegal interceptions if the government played no part in the illegal interceptions. U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995), cert. denied 5/13/96. The perpetrator of an illegal interception, cannot avail himself of the "clean hands" exception under Murdock. Smoot v. United Transportation Union, 246 F.3d 633 (6th Cir. 2001).

> [The efficacy of Murdock was questioned by Chief Judge Merritt's dissent from the panel decision in Doe v. Securities and Exchange Commission, 86 F.3d 589 (6th Cir. 1996), vacated and remanded, sub nom., Smith v. Securities and Exchange Commission, 129 F.3d 356 (6th Cir. 1997) (en banc) (dismissed as moot without addressing the merits)]
>
> [Murdock has since been rejected by the Third Circuit in In re Grand Jury, 111 F.3d 1066 (3d Cir. 1997)); the Ninth Circuit in Chandler v. U.S. Army, 125 F.3d 1296 (9th Cir. 1997)); and on July 14, 1998 by the U.S. Court of Appeals for the District of Columbia in Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998)]

The Third Circuit held that the district court should have granted a Rule 17(c) motion filed by illegal wiretap victims who intervened to quash a grand jury subpoena duces tecum the enforcement of which would have caused the illegal interceptor to produce the illegal tapes in violation of Sections 2515 and 2511(1)(c) of Title 18. The Third Circuit said it does not believe that Congress intended the grand jury and the courts to use their respective powers to compel violations of Title III. The Court strongly rejected the Sixth Circuit's "clean hands" holding in Murdock: "Given the unambiguous language of § Section 2515, compliance with the subpoena would be a violation of an express congressional prohibition. Were we to allow a compelled violation of this federal law, the hands of the grand jury, the district court, and ourselves would all become sullied . . . . In short, it is incomprehensible that Congress intended the admissibility of unlawfully intercepted communications to turn solely on whether the government participated in the interceptions . . . . We have no authority to restrike the balance [law enforcement/privacy] that Congress has already struck by placing in the statute a clean hands exception that Congress did not." In re Grand Jury, 111 F.3d 1066 (3d Cir. 1997) (footnote cites conflicting conclusions in U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995) (clean hands exception) and U.S. v. Vest, 813 F.2d 477 (1st Cir. 1987) (rejecting clean hands exception)).

The Ninth Circuit reversed a summary judgment entered in favor of the Army and against an Army captain who had sued the Army under 18 U.S.C. 2520 for declaratory and equitable relief because the Army, in pursuit of adverse action against the captain, disclosed and used, in violation of 2511(1)(c) and (d), the captain's telephonic communications knowing they had been illegally intercepted and recorded by his wife. The Idaho federal district court granted summary judgment for the Army on the theory that 18 U.S.C. 2517 allowed use of the tape and because a second investigation employing unexposed officials was untainted by use or disclosure of the illegal tape. In reversing the district court, the Ninth Circuit noted that 18 U.S.C. 2517 allows law enforcement officials to disclose and use the contents of a wiretap if they become aware of the contents "by any means authorized by this chapter." A law enforcement officer could obtain by authorized means the contents of an illegal wiretap if the officer did not know that the wiretap was illegal. However, the contents of, or evidence derived from, the illegal wiretap could not be

presented as testimony because 2517(3) requires that such communications must have been "intercepted in accordance with the provisions of this chapter." The Court said that another example of "authorized" knowledge by law enforcement officers of illegally intercepted communications would occur when an emergency wiretap under 2518(7) is not perfected through the necessary filings or is not approved by the court. Intercepted communications from such emergency wiretap could be used and disclosed by law enforcement officials under 2517(1) and (2) but could not be the subject of testimony due to the constraints of 2517(3). The Ninth Circuit rejects the Army's argument that law enforcement authorities can unconditionally disclose and use communications they know to have been intercepted illegally, so long as they do not introduce them as evidence in a proceeding with a judge who can grant motions to suppress. That construction fails because it would render superfluous the language in 2517(1) and (2), "by any means authorized by this chapter, has obtained knowledge." The Court denies that its holding sets up a conflict with the Fifth Circuit's Forsyth v. Barr, 19 F.3d 1527 (5th Cir. 1994). The Court points out that in Forsyth, the informant who told the police officer about the contents of the wiretap, "told [the officer] that a wiretap was not involved, and [the police officer] believed that the telephone had become a party line accidentally." The police department did not learn of the tape's illegality until the department had nearly completed its internal inquiry. No charges were filed by the police department against the victim of the illegal intercept. Forsyth expressly limits its ruling to "the unique facts and circumstances of this case," and is not in conflict with the Ninth Circuit's construction of the statute. The Ninth Circuit favorably cites the First Circuit's U.S. v. Vest, 813 F.2d 477 (1st Cir. 1987) for its rejection of the argument that the government is free to use an illegal intercept so long as it did not participate in the illegal interception. Accordingly, the Ninth Circuit is unable to avoid a conflict with the Sixth Circuit's U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995) which rejected the First Circuit's position in Vest and recognized a "clean hands" exception to 18 U.S.C. 2515 that allows the government to introduce evidence obtained from an illegal private wiretap if the government took no part in the illegal interceptions. The Ninth Circuit disagrees with the Sixth Circuit for two reasons. First, the purpose of the statue is to prevent private, not just governmental, wiretapping. Second, the Court cannot reconcile the Sixth Circuit reading with the statutory language. Chandler v. U.S. Army, 125 F.3d 1296 (9th Cir. 1997).

On July 14, 1998, the U.S. Court of Appeals for the District of Columbia Circuit reversed and remanded the district court's granting of summary judgment for State Department defendants (Inspector General, et al.) in a suit brought by a former acting assistant secretary of state seeking damages for illegal wiretaps by the State Department's operations center of his telephonic communications with another assistant secretary about Bill Clinton's passport files. The appeals court rejected the defendants' arguments for certain exceptions under Title III and sent the case back to the district court for further proceedings. Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).

Subject of illegal wiretap by defendant had standing to object to disclosure of illegal tapes to the defendant for impeachment purposes. The defendant made no specific allegations regarding the potential impeachment of any witness. Disclosure of illegally intercepted communications is a crime and such communications are not admissible in evidence. If the court required the prosecution to disclose the contents of the illegal tapes for purposes of ascertaining whether they contain exculpatory material, the court would cast the prosecution in the role of a party to a crime. The defendant's right to a fair trial does not encompass a right to profit from the fruits of his crime. Anthony v. U.S., 667 F.2d 870 (10th Cir. 1981).

"At the present time there is a split among the circuit courts regarding the necessity of suppressing tapes which were made by a co-conspirator in furtherance of the conspiracy and which contain evidence of the conspiracy." U.S. v. Nietupski, 731 F. Supp. 881 (C.D. Ill. 1990). U.S. v. Vest, 813 F.2d 477 (1st Cir. 1987) (literal interpretation of §2515 prohibited use of co-conspirator's tape

recording of police detective's participation in bribery scheme to prosecute the detective for perjury when he denied that he participated. Tape was made for illegal purpose, i.e., to create "receipt" for the payment.) U.S. v. Underhill, 813 F.2d 105 (6th Cir.), cert. denied, 482 U.S. 906 (1987) (calls taped by gambling operators to maintain a record of bets can be used to prosecute the gambling violations because a literal application of 2515 and 2511(2)(d) would produce an absurd result Congress did not intend.) U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995), cert. denied 5/13/96 (a "clean hands" exception to § 2515 permits the government to use illegal interceptions against the victim of the illegal interceptions if the government played no part in the illegal interceptions); U.S. v. Traficant, 558 F. Supp. 996 (N.D. Ohio 1983) (using the reasoning employed four years later in Underhill: "This court cannot find that Congress intended to [i]nclude discussions of illegal activities within the parameters of those activities having a protectable expectation of privacy.") "We believe that the First Circuit was simply wrong in its conclusion that the statute should be interpreted literally to exclude from evidence recordings made by a co-conspirator during and in furtherance of the conspiracy which contain evidence of the conspiracy." U.S. v. Nietupski, 731 F. Supp. 881 (C.D. Ill. 1990).

Section 2515 of Title 18 requires that recordings of defendant's telephone conversations with a gambling business be suppressed because the recordings were made by the gambling operator in furtherance of an illegal activity, the defendant did not consent to the recording, and the defendant was not shown to be a coconspirator of the gambling operator who illegally recorded the conversations. U.S. v. Lam, 271 F. Supp.2d 1182 (N.D. Cal. 2003) (applying Chandler (rejecting Murdock) and Vest and distinguishing Underhill).

District court granted intervenor's motion under 18 U.S.C. 2515 to suppress illegally videotaped conversations between himself and his attorney that the government sought to use in its prosecution of a sheriff's official for illegally intercepting and disclosing oral communications occurring between lawyers and their clients in the sheriff's office. The government is pursuing a pretrial appeal of the judge's ruling. U.S. v. Grice, 37 F. Supp.2d 428 (D. S.C. 1998).

Until it can be shown that defendants have violated §2511, admission of contents of tape recordings in question or evidence derived therefrom is not barred under §2515; therefore, their disclosure to and use by counsel, for purpose of preparing a defense, is not a crime. Possible inadmissibility of tape recordings at trial is not an adequate reason to foreclose discovery of them. Provisions of §3504 cannot be applied to resolve the issue of admissibility in the ordinary civil case brought under §2520 because requirement of affirmance or denial of the alleged unlawful act would expose the individual to criminal liability under §2511 and violate his Fifth Amendment privilege. McQuade v. Michael Gassner Mechanical, 587 F. Supp. 1183 (D. Conn. 1984).

Where a plaintiff filed a complaint alleging violations of wiretap laws, and where the district court denied plaintiff's request for a protective order foreclosing use of the tapes in the defense, the defendant may disclose to his attorneys the contents of intercepted communications, and the attorneys and defendant may use the contents to prepare a defense to the wiretap charges. Defendant and his attorneys may use the contents in confidence. Any disclosure to third parties or for purposes other than to prepare a defense against the wiretap charges, exceeds the bounds of the privilege ("defense exception"). Both plaintiffs and defendants have an incentive to seek protective orders defining the permissible boundary of a defendant's use in each case. The defense exception does not permit any public disclosure, thus requiring parties initially to file revelatory motions in camera, and does not justify use or disclosure for purposes that do not materially advance a party's defense to wiretap charges. In Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993), the First Circuit recognized an implied "adjudication exception" that permits disclosure of intercepted material to a court for admissibility determinations and to a court or jury for a resolution of illegality. Whatever the outer bounds of the adjudication and defense

exceptions, they do not permit the public disclosure of the contents of an illegally intercepted communication (defendant disclosed certain contents of the intercepted communications in two motions for summary judgment which became part of the public record) where an in camera or sealed disclosure will not materially harm a party's defense. Attorneys are not immune from violations of the wiretap law. Nix v. O'Malley, 160 F.3d 343 (6th Cir. 1998).

The defense and adjudication exceptions under Nix (see above) do not apply to Plaintiff's distribution of the executive session transcript (made from Plaintiff's illegal recording of meeting) to his lawyer or the attachment of the transcript to Plaintiff's complaint because Plaintiff was not, at that time, defending against charges brought under the Wiretap Act. Smoot v. United Transportation Union, 246 F.3d 633 (6th Cir. 2001).

In Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993), the First Circuit noted that no federal appeals court has yet spoken on the issue of whether 18 U.S.C. §2511(1)(c) and (d) make it a crime to disclose illegally intercepted material during the course of attorney consultations. The court said that reasonable arguments might be made on both sides of this question of first impression, but deemed the issue waived because it was not fully argued and developed. The court, in a footnote, cited McQuade as an example of one federal judge who recognized the inherent tension between the wording of the statute and the need for effective trial preparation, holding that the disclosure of the contents of intercepted recordings to counsel, for the purpose of preparing a defense, is not a crime.

"Adjudicatory exception" permits use of illegally intercepted communications in litigation. Oliver v. WFAA-TV, Inc, 1998 U.S. Dist. LEXIS 21532 (N. D. Tex.); Peavy v. Harman, 37 F. Supp.2d 495 (N.D. Tex. 1999). This exception in civil cases is limited to the issue of liability, and does not permit use on the issue of damages. Goodspeed v. Harman, 39 F. Supp.2d 787 (N.D. Tex. 1999).

Use of Illegal Interceptions for Impeachment

The recording of a telephone conversation obtained by the government in violation of Title III can properly be used to impeach the defendant's testimony. "Evidence seized in violation of the Fourth Amendment or the federal wiretapping statute cannot be used by the government in its case in chief. But, if the defendant chooses to testify, and swears to a sequence of events inconsistent with his own previously recorded statements, the Constitution does not require the government to leave the lie (or what it contends to be a lie) unchallenged." U.S. v. Baftiri, 263 F.3d 856 (8th Cir. 2001)(citing Williams v. Poulos, 11 F.3d 271, (1st Cir. 1993); U.S. v. Echavarria-Olarte, 904 F.2d 1391 (9th Cir. 1990); Jacks v. Duckworth, 651 F.2d 480 (7th Cir. 1981); U.S. v. Caron, 474 F.2d 506 (5th Cir. 1973)).

The rule regarding use of illegally seized evidence for purposes of impeachment was not altered by 18 U.S.C. 2515. U.S. v. Caron, 474 F.2d 506 (5th Cir. 1973).

Even if wiretaps were illegal, to the extent they contradicted statements made on direct examination, they were admissible for purposes of impeachment. U.S. v. Echavarria-Olarte, 904 F.2d 1391 (9th Cir. 1990)

The impeachment exception to § 2515 is limited to criminal actions brought pursuant to Title III. Illegal interceptions (and their transcriptions) cannot, pursuant to the criminal impeachment exception, be introduced into evidence for impeachment purposes in civil cases. Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993).

"Impeachment" exception allows use of illegally intercepted communications to impeach a testifying defendant (but not a witness). U.S. v. Lanoue, 71 F.3d 966 (1st Cir. 1995).

Defendant is liable for wiretapping his wife's telephone conversations, but illegal intercepts are admissible to impeach witness's evidence presented to the court in an affidavit, and therefore submission of the transcripts of the illegal intercepts to the court for such purposes was not improper. Culbertson v. Culbertson, 143 F.3d 825 (4th Cir. 1998).

Private Litigants

District court lacked authority to compel the Government to release electronic surveillance tapes to a private litigant pursuing a civil matter. RICO provision allowing disclosure "in any proceeding" did not create "a general civil discovery mechanism." Applications and orders sealed by the judge shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction. 18 U.S.C. 2518(8)(b). National Broadcasting Company v. United States Department of Justice, 735 F.2d 51, 54 (2d Cir. 1984) (government opposed disclosure); Applications of Kansas City Star, 666 F.2d 1168 (8th Cir. 1981).

There is no authority in Title III for pretrial or compelled testimonial disclosure of sealed electronic surveillance evidence to a private civil RICO litigant. In re: Motion to Unseal Electronic Surveillance Evidence, 990 F.2d 1015 (8th Cir. 1993) (en banc).

If by virtue of sections 2511(2)(c) or (d) an interception is not prohibited by Title III, there are no Title III restrictions on its use. Section 2517(3) does not come into play and such questions as whether the section authorizes disclosure only in government proceedings and only at trial drop out; the meaning of "oral communications" also becomes moot. In re High Fructose Corn Syrup Antitrust Litigation, 216 F.3d 621 (7th Cir. 2000).

Plaintiffs in civil action against city and city officials alleging violations of antitrust and racketeering statutes sought to subpoena electronic surveillance materials in possession of U. S. Attorney's office relating to investigation of alleged scheme. Plaintiffs would be allowed to subpoena portions of electronic surveillance material that had already been disclosed during related criminal prosecution; however, plaintiffs' subpoenas would be quashed to extent that they sought surveillance materials which had not previously been disclosed in criminal trials. County of Oakland by Kuhn v. Detroit, 610 F. Supp. 364 (E.D. Mich. 1984).

"Other Offenses"/2517(5)

The use of “other offense” information by law enforcement officers to prepare a search warrant affidavit is not "testimonial" in nature (Section 2517(3)) such that prior approval (Section 2517(5)) of a judicial officer is needed. Section 2517(5) permits “other offense” disclosure or use under 2517(1) and (2), under which the "proper performance of his official duties" includes the use of the information for such uses as establishing probable cause to search. See U.S. v. Vento, 533 F.2d 838 (3rd Cir. 1976); U.S. v. O’Neill, 52 F. Supp.2d 954 (E.D. Wis. 1999) (citing Vento).

Offenses that arose out of and were closely related to one of the original crimes specified in the wiretap application do not fall within the "other offenses" provision of 2517(5). In any event, the government included in its extension application information relating to the non-specified offenses. Because the government kept the court apprised of that information, it was not error for

the court to allow the government to charge the defendant with the non-specified offenses. U.S. v. Homick, 964 F.2d 899 (9th Cir. 1992).

Interceptions pursuant to Title III order premised on Hobbs Act were used in grand jury to support Travel Act and false statement charges. The government corrected any problem by obtaining a judicial order approving the release of information about Travel Act and false statement charges. It then voided the first indictment and took the case before a second and uninfected grand jury, which returned an indictment for violations of the Hobbs Act, Travel Act and false statement statute. It would have been impossible for the government to obtain wiretap authority for false statements because the defendant was not suspected of such violations until after the wiretapping began. The Travel Act and false statement charges were based on the same set of facts as the Hobbs Act violation. Since the government was free to release this information to a grand jury under the Hobbs Act authorization, it is difficult to see how the defendants were harmed when the same facts were presented in the context of different offenses. U.S. v. Shields, 999 F.2d 1090 (7th Cir. 1993).

Government is required to dismiss indictment alleging "other offense." The government must then obtain 2517(5) authorization to use "other offense" evidence before it seeks a superseding indictment before an untainted grand jury. U.S. v. O'Neill, 27 F. Supp.2d 1121(E.D. Wis. 1998) (citing U.S. v. Brodson, 528 F.2d 214 (7th Cir. 1975).

18 U.S.C. 2517(5) does not require that a disclosure order be sought before the disclosure. U.S. v. Barnes, 47 F.3d 963 (8th Cir. 1995) (disclosure order obtained after "other offense" evidence presented to grand jury).

RICO predicate offenses are not "other offenses" for purposes of 2517(5). U.S. v. Daly, 535 F.2d 434 (8th Cir. 1976); U.S. v. Sedovic, 679 F.2d 1233 (8th Cir. 1982).

RICO offense not "other offense" requiring a 2517(5) order when evidence from state narcotics wiretap was used to obtain federal RICO indictment listing the narcotics violations as the predicate crimes. U.S. v. Watchmaker, 761 F.2d 1459 (11th Cir. 1985).

"The § 848 count is hardly an offense "other than those specified in the order"-i.e., narcotics offenses and money laundering. Piggott's conviction on the continuing criminal enterprise charge was based upon his narcotics activity. Piggott v. U.S., 2003 U.S. Dist. LEXIS 228 (S.D.N.Y.).

"Other offense" disclosure authorization required by 18 U.S.C. 2517(5) may be inferred when judge grants a renewal of an interception order after being advised of the essential facts of the unspecified violation. U.S. v. London, 66 F.3d 1227 (1st Cir. 1995); U.S. v. Ardito, 782 F.2d 358 (2d Cir. 1986); U.S. v. Van Horn, 789 F.2d 1492 (11th Cir. 1986); U.S. v. Masciarelli, 558 F.2d 1064 (2d Cir. 1977); U.S. v. Tortorello, 480 F.2d 764 (2d Cir. 1973); U.S. v. Wager, 2002 U.S. Dist. LEXIS 17739 (S.D.N.Y.); U.S. v. Davis, 1995 WL 644051 (E.D. La. 11/1/95); U.S. v. Cleveland, 1997 WL 208937 (E.D. La. 4/28/97); U.S. v. Gruber, 994 F. Supp. 1026 (N.D. Iowa 1998).

Government's interception of mayor's wire communications regarding sexual misconduct (offenses not enumerated in 18 U.S.C. 2516 and not specified in the order) during a wiretap in a public corruption investigation was consistent with the" plain view" doctrine and the government fully complied with the requirements of 18 U.S.C. 2517(5) for the use of such "other offense" interceptions as evidence. U.S. v. Giordano, 259 F. Supp.2d 146 (D. Conn. 2003)(applying U.S. v. Masciarelli, 553 F.2d 1064 (2d Cir. 1977)).

"Other" offenses under 2517(5) may include offenses, federal as well as state, not listed in section 2516 so long as there is no indication of bad faith or subterfuge. The Senate Report (S.Rep. No. 1097) accompanying 2517(5) states that "other" offenses under that section "need not be designated 'offenses.'" In re Grand Jury Subpoena Served on Doe, 889 F.2d 384 (2d Cir. 1989) (tax offenses); U.S. v. Shnayderman, 1993 WL 524782 (E.D. Pa.) (tax offenses).

State judge had authority under 2517(5) to authorize use of communication revealing evidence of federal crimes (tax offenses) which were not among the listed crimes which could have been the legitimate subject of surveillance in the first instance. In re Grand Jury Subpoena Served on Doe, 889 F.2d 384 (2d Cir. 1989); Accord U.S. v. Van Horn, 789 F.2d 1492 (11th Cir. 1986)(Florida circuit judge, federal drug offense).

Government's application under 2517(5) for testimonial use of intercepted "communications relating to offenses other than those specified in the order of authorization" was filed "as soon as practicable" where government possessed tapes for four years and became aware of their relevance seven months prior to filing the application under 2517(5). U.S. v. Vario, 943 F.2d 236 (2d Cir. 1991). Comparable delays under similar circumstances have been upheld on appeal, U.S. v. Van Horn, 789 F.2d 1492 (11th Cir. 1986) (government's request under 2517(5) for testimonial use of state wiretap evidence in federal drug prosecution was timely although made 22 months after federal agents learned of state wiretap and five months after they learned of the contents of the state wiretap); U.S. v. Arnold, 773 F.2d 823 (7th Cir. 1985) (31 month delay was not a violation where original wiretap order was lawfully obtained, in good faith and not as a subterfuge, and 2517(5) application was made as soon as practicable before the proceeding in which the evidence was to be used); U.S. v. Southard, 700 F.2d 1 (1st Cir. 1983) (19 month delay).

There is no violation of 2517(5) where the government uses in a civil tax proceeding lawfully intercepted communications previously made part of the public record in a criminal prosecution. The government did not seek to use the intercepted communications as evidence of a tax offense. London v. Commissioner of Internal Revenue, 1998 Tax Ct. Memo LEXIS 348 (9/29/98).

Freedom of Information

Wiretap recordings, otherwise exempt from disclosure under the FOIA, must nevertheless be released when a requester precisely identifies specific tapes that have been introduced into evidence and played in open court during a public criminal trial. Unless the government can rebut such a specific showing by demonstrating that the recordings have since been destroyed or otherwise removed from the public record, they must be released under FOIA. Cottone v. Reno, 193 F.3d 550 (D.C. Cir. 1999).

DOJ properly invoked FOIA Exemption 1 to withhold aggregate statistical data concerning its use of specific provisions of the Patriot Act. American Civil Liberties Union v. U.S. Department of Justice, 265 F. Supp.2d 20 (D. D.C. 2003).

Title III materials are covered by FOIA Exemption 3 ("specifically exempted from disclosure by statute")-Title III itself-and "refers to particular types of matters to be withheld." Title III refers to the way in which information was collected. In CIA v. Sims, 471 U.S. 159 (1985), the Supreme Court held that a "process" definition in a statute relating to protection of foreign intelligence sources and materials qualified under Exemption 3. Lam Lek Chong v. Drug Enforcement Administration, 929 F.2d 729 (D.C. Cir. 1991); Willis v. Federal Bureau of Investigation, 1999 U.S. App. LEXIS 7354 (D.C. Cir.).

Title III and pen register materials are within the exemption provided by 5 U.S.C. 552(b)(3). Manna v. U.S. Department of Justice, 815 F. Supp. 798 (D. N.J. 1993); Epps v. U.S. Department of Justice, 801 F. Supp. 787 (D.D.C. 1992); Manchester v. Drug Enforcement Administration, 823 F. Supp. 1259 (E.D. Pa. 1993); Delviscovo v. Federal Bureau of Investigation, 903 F. Supp. 1 (D. D.C. 1995); Riley v. Federal Bureau of Investigation, 2002 U.S. Dist. LEXIS 2632 (D.D.C.)(pen register app/order exempt under 552(b)(3) and 552(b)(7)(C); Santos v. DEA, 2005 WL 555410 (D. D.C.).

Prison authorities did not "intercept," consensually or otherwise, any communication within meaning of Title III when they routinely monitored and recorded inmate's conversation with his attorney, in case in which inmate chose not to use available unmonitored line, and thus the recordings were not exempt from disclosure under the FOIA as specifically exempted by statute. The communications were obtained by "law enforcement officers" who "used," "in the ordinary course of [their] duties," some telephone "instrument, equipment or facility, or [a} component thereof." 18 U.S.C. 2510(5)(a)(ii). Smith v. U.S. Department of Justice, 251 F.3d 1047 (D.C. Cir. 2001).

Transcripts

Prosecution was not required to provide defendant with transcription and translation from Spanish to English of all 11,000 telephone conversations which were intercepted where Government concluded that only approximately 1,800 of the conversations were drug-related and gave the defendant English transcriptions of those conversations, and provided defense counsel with the other 9,200 tapes, but no transcriptions or translations. The court repeatedly offered to provide defendant with a translator or interpreter who would sit down with defense counsel and identify any of the other tape recorded conversations, which were in Spanish, which might be crucial to the defense. If any important tapes turned up, the court offered to have those tapes neutrally transcribed and translated. Defense counsel conceded that if the tapes were in English he would have had no right to a transcription. The court found that the procedures used here were reasonable and fully respected the defendant's constitutional rights. U.S. v. Zavala, 839 F.2d 523 (9th Cir. 1988).

Government did not violate criminal rule and due process clause by not providing defendant with transcript of tape recorded conversation in advance of trial where failure of government to produce the transcript did not prejudice defendant's rights at trial, defendant had access to tape and could have had his own transcript made, record did not show that judge or jury had problems understanding tape and defendant was given ample opportunity to review transcript before giving it to jury. U.S. v. Gee, 695 F.2d 1165 (9th Cir. 1983).

The Second Circuit has recognized the obligation of the Government to produce transcripts of a defendant's conversations prior to trial in response to his explicit discovery requests. U.S. v. Cirillo, 499 F.2d 872 (2d Cir. 1974); U.S. v. Crisona, 416 F.2d 107 (2d Cir. 1969). However, a motion for disclosure of all recorded conversations of defendants, other defendants, and co-conspirators, whether or not authorized or lawful, and for disclosure of any documents, logs and transcripts relating to such conversations should be denied insofar as it relates to materials other than the conversations of defendants themselves, unless otherwise producible as Brady material prior to trial or as Section 3500 material to be provided to the defendants at trial.

The prosecutor does not have an obligation under Brady or the Jencks Act to retrieve, review, or disclose information (BOP telephone tape recordings) possessed by other government agencies that have no involvement in the investigation or prosecution at issue. The prosecutor need not

conduct open-ended fishing expeditions of unrelated files. The defense did not make a sufficient materiality showing regarding the BOP tapes. Under the Jencks Act, the phrase "in the possession of the United States" refers to possession by the prosecutorial arm of the federal government. In this case, even if the BOP recorded communications were related to the witnesses' testimony, the BOP was not part of the prosecutorial arm of the federal government as it was not involved in either the investigation or the prosecution of the defendants. U.S. v. Merlino, 2003 WL 22664513 (3d Cir.).

The government did not have to transcribe for the defendants 61 hours of tape recordings the government did not intend to use. The government gave the defendants copies of all 65 hours of tape recordings and provided the defendants with the transcripts of the four hours of recordings the government intended to use at trial. Fair access was provided for the defendants and the government did not violate its Brady obligation. U.S. v. Parks, 100 F.3d 1300 (7th Cir. 1996) (citing Zavala and Gee); U.S. v. Santos-Cruz, 2000 WL 326191 (E.D. Pa.) (Citing Zavala, Gee and Parks).

District courts have wide discretion in determining whether to allow juries to use written transcripts as aids in listening to audiotape recordings. Transcripts can be admitted at trial and used by the jury during their deliberations when the underlying tapes are actually played during the trial. In this case, the jury was clearly instructed that if there was any variation between the tapes and the transcripts, they were to rely solely on the tapes. Defendants' names can be included on the transcripts based on agent or lay testimony identifying the speakers' voices. U.S. v. Breland, 356 F.3d 787 (7th Cir. 2004).

(Draft Transcripts)

U.S. v. Shields, 767 F. Supp. 163 (N.D. Ill. 1991) (reaffirming analysis employed in U.S. v. Finley, 1987 WL 17165 (N.D. Ill. Sept. 3, 1987)):

Defendant requested any and all draft transcripts prepared by the government. There is no legitimate basis for distinguishing between a draft transcript and a final transcript. Each is a reflection of what the defendant purportedly said on the tape, and although the government may believe the final version to be more accurate than the draft, a defendant is entitled to see both versions. Suppose the defendant had been interviewed by two agents and each summarized their interview somewhat differently in their subsequent reports. Surely the government could not contend that the defendant was only entitled to see whichever report it believed most accurate; the defendant would be entitled to have both produced. So it is here. The Court agrees with the defendant that the tapes are often difficult to understand. In this circumstance, there may well be disputes as to the accuracy of final transcripts, and the defendant is entitled to review without conditions not only the final versions but any and all prior drafts prepared by the government as well.

U.S. v. Bailey, 689 F. Supp. 1463 (N.D. Ill. 1987):

Two months following the Finley case, a different judge in the same district, ruled in the Bailey case that because the tapes, rather than the transcripts, would constitute the evidence at trial, and there was no argument that draft transcripts could lead to the discovery of admissible evidence, the only way the draft transcripts could be used at trial would be to impeach a witness who was testifying to the accuracy of a final transcript. Consequently, the draft was not a statement of the defendant discoverable under Rule 16, but a witness statement the government was required to produce under the Jencks Act (18 U.S.C. 3500).

Monitoring Logs

Fed.R.Crim.P. 16(a)(1)(C) (books, papers, documents . . . tangible objects). Monitors' logs, pen register tapes, and telephone records "clearly included under this rule as discoverable objects to which defendants are entitled. U.S. v. Feola, 651 F. Supp. 1068 (S.D.N.Y. 1987).

Trial court correctly denied pre-trial inspection of the monitoring agent's logs. The logs were furnished to the defense after the monitoring agent testified. Complete transcripts of all recorded conversations were made available to the defense during pre-trial discovery. U.S. v. Howell, 514 F.2d 710 (5th Cir. 1975).

Progress Reports

The government did not file the second ten day progress report because it terminated the tap on the nineteenth day and filed a sealing application with the court that day.

> [T]he district court had discretion to require the progress reports in the first place, In re DeMonte, 674 F.2d 1169, 1174 (7th Cir. 1982), and to find that a twentieth day report was not necessary in light of the government's sealing application which indicated that the wiretap surveillance had been discontinued. Cf. United States v. Iannelli, 477 F.2d 999, 1002 (3d Cir. 1973) ("The sufficiency of these reports was a matter for the supervising judge, and the breadth of his discretion must be viewed in light of the fact that he could under 18 U.S.C. § 2518(6) have dispensed with progress reports entirely."). Moreover, even if the district court had found that the government failed to properly comply with its progress report order, suppression of the wiretap evidence is not the automatic remedy, and such a decision is similarly within the district court's discretion. See United States v. Scafidi, 564 F.2d 633, 641 (2d Cir. 1977) ("While these reports should have been timely filed, the sanction for failure to do so is surely not automatic suppression of the tapes."); see also DeMonte, 674 F.2d at 1174 ("Even if the appellant's claim that the reports were not timely filed is true, that does not automatically render the surveillance invalid.").

U.S. v. Breland, 356 F.3d 787 (7th Cir. 2004).

Since progress reports that the government filed pursuant to Title III order represented only summaries of monitored conversations which were available in full for firsthand examination by defendants, defendant was not entitled to have progress reports disclosed. The authorizing judge has broad discretion and can dispense with such progress reports entirely. The sufficiency of these reports is a matter for the issuing judge. U.S. v. Brodson, 390 F. Supp. 774 (E.D. Wis. 1975); U.S. v. Marchman, 399 F. Supp. 585 (E.D. Tenn. 1975); U.S. v. Wright, 121 F. Supp.2d 1344 (D. Kan. 2000); U.S. v. Chimera, 201 F.R.D. 72 (W.D.N.Y. 2001)(comprehensive denial of defendants' requests for government disclosure of progress reports, minimization instructions, pre-intercept investigative records, specimen eavesdropping pleadings and draft applications).

Appropriate sanction for failure to report on progress of electronic eavesdropping (clone pager), required by court order, is discontinuance of eavesdropping authorization, rather than suppression of evidence. U.S. v. Benjamin, 72 F. Supp.2d 161 (W.D.N.Y. 1999).

The government's failure to file a ten day report does not warrant automatic suppression, but it is within the judge's discretion to order sanctions after taking into consideration whether there has been a demonstration of prejudice by the defendant. U.S. v. Scafidi, 564 F.2d 633 (2nd Cir. 1977). A judge's decision to require progress reports under 18 U.S.C. 2518(6), which are designed to evaluate the need for continued surveillance, is completely discretionary. U.S. v. Crozzoli, 698 F. Supp. 430 (E.D.N.Y. 1988). U.S. v. Merton, 274 F. Supp.2d 1156 (D. Col. 2003)(citing Scafidi and Crozzoli); U.S. v. Padin, 2005 U.S. Dist. LEXIS 5994 (W.D.N.Y.)(footnote cite to Scafidi and Benjamin).

Work Product

U.S. v. Feola, 651 F. Supp. 1068 (S.D.N.Y. 1987):

Telephone logs themselves are discoverable under Rule 16, but any work product exposing the theory of the Government is not. The court in U.S. v. Payden, 613 F. Supp. 800 (S.D.N.Y. 1985), aff'd. 768 F.2d 487 (2d Cir. 1985), denied requests for analysis performed on toll records and other conclusions of investigative officers in that these were internal government documents made in connection with the investigation of the case.

Memoranda, logs or notes related to wiretapping, eavesdropping or other surveillance by the government which have been developed by the prosecution are specifically exempted from discovery. Fed.R. Crim.P. 16(a)(2). U.S. v. Spagnuolo, 549 F.2d 705 (9th Cir. 1977); U.S. v. Nakashian, 635 F. Supp. 761 (S.D.N.Y. 1986); U.S. v. Payden, 613 F. Supp. 800 (S.D.N.Y. 1985); U.S. v. Smith, 405 F. Supp. 144 (E.D. Pa. 1975); U.S. v. Chimera, 201 F.R.D. 72 (W.D.N.Y. 2001).

U.S. v. Wright, 121 F. Supp.2d 1344 (D. Kan. 2000):

> The court concurs with the government that an agent's summary of the call or conversation is protected from discovery, because it is the officer's mental impressions amounting to work product and is an internal document solely prepared for the criminal investigation under Rule 16(a)(2). The defendants have not shown that the information typically found in this segment of a monitor log sheet would be material to their minimization challenge. As far as a call summary containing discoverable information under Brady or Giglio, the court expects the government will be mindful of these other guiding principles of discovery when it redacts the call summary from a monitor log sheet. Outside of these discovery principles, the decision to redact the call summaries obviously remains a matter within the government's discretion.
>
> The court appreciates the additional burden placed on the government in producing the monitor log sheets rather than a printout from its Pen-Link database. The burden in this case, however, is not outweighed by the defendants' need to discover the information originally generated by officers to substantiate their minimization efforts. The defendants are entitled in this instance to view the original and best evidence of minimization, and the court will not require the defendants to assume the government correctly downloaded the information into its Pen-Link database. The court also encourages the government to provide any further information to these defendants it deems arguably relevant in the court's decision whether to conduct a minimization hearing.

3504 Motion

The manner in which the government is required to respond to a claim made under 18 U.S.C. 3504 will vary depending on the specificity of the claim. U.S. v. Yaganita, 552 F.2d 940, 944 (2d Cir. 1977) (bad faith, untimely motion filed on opening day of trial; government's response adequate under the circumstances (trial AUSA denial and affidavit of AUSA's superior regarding oral representation from ATF)). A substantial claim will necessitate a thorough file search by the government agencies most closely associated with the investigation. In re Millow, 529 F.2d 770, 774 (2d Cir. 1976). However, a frivolous assertion of misconduct that lacks even a colorable basis does not constitute a claim under § 3504 sufficient to require a response from the government. Id. U.S. v. Blumberg, 1998 WL 136174 (D. Conn.).

Trial

Recusal

The fact that the judge who granted the Title III order also ruled on the suppression motion is not a basis for recusal. U.S. v. Williams, 2005 U.S. App. LEXIS (3d Cir.) (unpublished).

U.S. v. Hanhardt, 134 F. Supp.2d 972 (N.D. Ill. 2001)(recusal motion denied; Court issued 175 orders, including numerous wiretaps during four and a half year investigation)(good review of recusal jurisprudence):

> Although there has been no specific ruling from the Seventh Circuit as to whether a district court's orders entered during pre-indictment investigations warrant that court's recusal, several other Circuits have considered the issue and found that recusal is generally inappropriate. See Camacho v. Autoridad de Telephonos de Puerto Rico, 868 F.2d 482, 490 (1st Cir. 1989) (emphasizing that nothing about the fact that the judge signed the orders would lead a reasonable person to question the jurist's impartiality); Cf. United States v. Foddrell, 523 F.2d 86, 87 (2nd Cir. 1975) (holding that recusal was not warranted for conducting a hearing on wire tapping); United States v. Diana, 605 F.2d 1307, 1316 (4th Cir. 1979) (holding that the judge properly refused to recuse himself from issuing an order to seal tapes obtained through surveillance); United States v. De La Fuente, 548 F.2d 528, 541 (5th Cir. 1977) (presiding at a pretrial suppression hearing regarding wiretap evidence does not warrant recusal from trial). And, in United States v. Nicholson, the Eastern District of Virginia found that ex parte communications conducted during an investigation, and the court's entering orders concerning the Foreign Intelligence Surveillance Act of 1978, did not warrant recusal. United States v. Nicholson, 955 F. Supp. 582, 583-84 (E.D. Va. 1997). The court analogized its involvement to that of a judge dealing with a Title III action, and ruled that recusal was not warranted in that instance. Id.

The mere fact that a judge who is ruling on a Title III suppression motion is the judge who granted that Title III order, is not a valid basis for recusal. U.S. v. Lewis, 2005 WL 1678981 (3d Cir.)(unpublished)(citing Hanhardt).

Standing

The standing requirements of Title III are "'to be construed in accordance with the standing requirements usually applied to suppression claims under the fourth amendment'" and, therefore, named targets of electronic surveillance who were not actually intercepted lack standing to move to suppress. U.S. v. Ruggiero, 928 F.2d 1289 (2d Cir. 1991); U.S. v. Charles, 1998 WL 204696 (D. Mass.); U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999).

Because the defendants were corporate officers and directors of a small family-run business who not only had ownership of the targeted office but also exercised full access to the building as well as managerial control over its day-to-day operations, they had a reasonable expectation of privacy over calls made on the premises. Owners of the premises where an illegal wiretap occurs have standing to challenge the interception, even if the owners did not participate in the intercepted conversations. U.S. v. Gonzalez, Inc., 412 F.3d 1102 (9th Cir. 2005)(citing Alderman v. U.S., 394 U.S. 165 (1969); U.S. v. King, 478 F.2d 494 (9th Cir. 1973)).

Defendants were named as subjects in the Title III orders authorizing the interception of oral communications and therefore have standing to contest the introduction of the interceptions into evidence. U.S. v. Wager, 2002 U.S. Dist. LEXIS 17739 (S.D.N.Y.).

Although defendant has standing to challenge the validity of the wiretaps on Lines 7, 8, or 9, the lines on which his communications were intercepted, he attacks those wiretaps only on the ground that probable cause for them resulted from the tap of Line 1, which he contends was invalid. Defendant lacks standing, however, to challenge the tap of line 1 because that line did not serve his premises, nor were any of his conversations intercepted on that line. U.S. v. Mercado, 2004 U.S. App. LEXIS 19053 (9th Cir.)(unpublished).

Standing to challenge evidence obtained through use of electronic surveillance techniques requires a showing by a defendant that his or her voice was heard on the wire or that his or her telephone was tapped. U.S. v. Fury, 554 F.2d 522, 525 (2d Cir. 1977); U.S. v. Greyling, 2002 WL 424655 (S.D.N.Y.)(citing Fury); U.S. v. Menendez, 2005 WL 1384027 (S.D.N.Y.)(citing Fury).

Under either the Fourth Amendment or 18 U.S.C. 2510(11), only a person whose conversations or communications were intercepted or who had conversations of others intercepted from his premises has standing to challenge the legality of the wiretap. U.S. v. Santana, 218 F. Supp.2d 53 (D. N.H. 2002).

A federal district judge in Boston held that Minnesota v. Carter, 525 U.S. 83 (1998) indicates that the bugging of the LCN induction ceremony did not violate DeLuca's Fourth Amendment rights because as a visitor to 34 Guild Street, who did not stay over night, and who engaged in only business discussions, he did not have an expectation of privacy that society would today deem to be justified. In addition, the court finds that when Title III was enacted it was intended that evolving, contemporary conceptions of reasonable expectations of privacy be applied in deciding whether an intercepted conversation constitutes an "oral communication" as defined in 2510(2). In view of the decision in Carter, the court is compelled to find that DeLuca did not at 34 Guild Street have a justified expectation that he would not be intercepted and, therefore, did not engage in what the statute defines as an "oral communication." Thus, DeLuca is not an "aggrieved person" as defined in § 2510(11). Accordingly, he does not have standing, under § 2518(10)(a), to seek suppression for an alleged violation of Title III concerning the electronic surveillance conducted at 34 Guild Street. Therefore, his motion to suppress must be denied. U.S. v. Salemme, 91 F. Supp.2d 141 (D. Mass. 1999).

Government's warrantless use of hidden video cameras to observe defendants in hotel room after consenting informants left the room is a privacy intrusion sufficiently serious to support a finding that the defendants had a reasonable expectation of privacy under the Fourth Amendment that their activities while alone in a hotel room would not be subject to surveillance by hidden cameras. Minnesota v. Carter, 525 U.S. 83 (1998) is distinguishable because the privacy intrusion in Carter was a police officer looking through a ground floor apartment window. The nature of the intrusion may affect the legitimacy of an expectation of privacy, as the Supreme Court recently opined in Bond v. U.S., 529 U.S. 334 (2000), wherein the Court held that an agent's warrantless manipulation of a bus passenger's bag in an overhead compartment violates the Fourth Amendment because the passenger has a reasonable expectation that he will not be subjected to such a severe intrusion (tactile observation) into his privacy. U.S. v. Nerber, 222 F.3d 597 (9th Cir. 2000).

U.S. v. Labate, 2001 U.S. Dist. LEXIS 6509 (S.D.N.Y.):

> Only "a defendant who was not a named target or interceptee of a wiretap must submit proof by affidavit that he or she was overheard on the wiretap in order to establish standing to seek suppression of such evidence." United States v. Bellomo, 954 F. Supp. 630, 639 (S.D.N.Y. 1997). Where a defendant was not named as a target of surveillance or an interceptee, standing may be established "only by sworn evidence, in the form of affidavit or testimony, from the defendant or someone with personal knowledge." United States v. Montoya-Eschevarria, 892 F. Supp. 104 at 106

> & n.1 (S.D.N.Y. 1995); accord Bellomo, 954 F. Supp. at 640 (defendant lacked standing 'absent a sworn statement by [defendant] or someone with personal knowledge averring that [defendant's] voice was intercepted'). Unsworn assertions in an attorney's memorandum of law do not suffice. Montoya-Eschevarria, 892 F. Supp. at 106. . . However, a defendant must make a greater showing to establish standing to challenge minimization procedures employed by the Government. The Second Circuit has indicated that only persons with a possessory or proprietary interest in the premises where the interceptions occur have standing to contest minimization procedures. United States v. Ruggiero, 928 F.2d 1289, 1303 (2d Cir. 1991); United States v. Fury, 554 F.2d at 426; United States v. Hinton, 543 F.2d 1002, 1010-11 & n.13 (2d Cir. 1976).

Defendant, who was not a named target or interceptee of a wiretap, did not provide the Court with an affidavit or sworn testimony that he was overheard on the allegedly unlawful wiretap and therefore he has no standing to contest the legality of the wiretap or evidence that was produced from it. U.S. v. Santiago, 2002 WL 104911 (S.D.N.Y.)(citing Labate and Bellomo)(see above).

An individual does not have standing to raise the issue of minimization as the failure to minimize the intercepted conversations is held to be an invasion of the targeted individual's privacy. See Alderman v. U.S., 394 U.S. 165 (1969); U.S. v. Fury, 554 F.2d 522 (2d Cir. 1977). See also U.S. v. Poeta, 455 F.2d 117 (2d Cir. 1972) (where wiretap was on targeted individual's telephone, another party did not have standing to contest invasion of target's privacy rights); U.S. v. Moore, 811 F. Supp. 112 (W.D.N.Y. 1992); U.S. v. Villegas, 1993 WL 535013 (S.D.N.Y.); U.S. v. Persico, 1994 WL 36367 (E.D.N.Y.); U.S. v. Sanchez-Flores, 1995 WL 765562 (S.D.N.Y.); U.S. v. Charles, 1998 WL 204696 (D. Mass.).

Any defendant who was the subject of electronic surveillance has standing to argue that the government acted with "flagrant disregard" for the minimizaton statute. If the evidence supports such a finding, then the defendants who either filed or adopted minimization challenges would be entitled to the suppression of every intercepted conversation that took place on their premises or to which they were parties. Such evidence would nonetheless remain available against any other defendant who lacked standing to challenge it. U.S. v. Parks, 1997 WL 136761 (N.D. Ill.).

[A] defendant may challenge only that evidence resulting from surveillance of his property or of which he was a target or interceptee." U.S. v. Eiland, 2005 WL 2679992 (D. D.C.).

Defendant is not an "aggrieved person" with standing to raise Fourth Amendment and Title III suppression issues regarding the DEA's capture of cell-site data from his co-defendant's phone. U.S. v. Forest, 355 F.3d 942 (6th Cir. 2004).

The Confrontation Clause, Title III and CI Recordings

Title III recordings are not "testimonial" for purposes of Crawford v. Washington, 541 U.S. 36 (2004). Party admission and coconspirator portions of conversations consensually recorded by a CI are also nontestimonial and thus not subject to the Crawford rule. The CI's portions of the conversations the CI surreptitiously recorded with the defendants were admissible for a purpose other than establishing the truth of the matters contained therein. Crawford recognized that the Confrontation Clause does not bar the use of testimonial statements for purposes other than establishing the truth of the matter asserted. The deceased informant's portions of the conversations were reasonably required to place the defendant or coconspirator's nontestimonial statements into context. U.S. v. Hendricks, 395 F.3d 173 (3rd Cir. 2005).

Suppression

18 U.S.C. 2515 & 2518(10)(a)

Not every failure to comply fully with any requirement provided in Title III would render the interception unlawful. Suppression is required only for a failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures. U.S. v. Donovan, 429 U.S. 413 (1977).

Appropriate sanction for failure to report on progress of electronic eavesdropping (clone pager), required by court order, is discontinuance of eavesdropping authorization, rather than suppression of evidence. U.S. v. Benjamin, 72 F. Supp.2d 161 (W.D.N.Y. 1999).

The government's failure to file a ten day report does not warrant automatic suppression, but it is within the judge's discretion to order sanctions after taking into consideration whether there has been a demonstration of prejudice by the defendant. U.S. v. Scafidi, 564 F.2d 633 (2nd Cir. 1977). A judge's decision to require progress reports under 18 U.S.C. 2518(6), which are designed to evaluate the need for continued surveillance, is completely discretionary. U.S. v. Crozzoli, 698 F. Supp. 430 (E.D.N.Y. 1988). U.S. v. Merton, 274 F. Supp.2d 1156 (D. Col. 2003)(citing Scafidi and Crozzoli).

Wiretap order inadvertently left unsigned by issuing judge was "insufficient on its face" under 2518(10)(a)(ii), but suppression was not warranted. Neither 2518(3) nor 2518(4) mandate a signed order, and the absence of a signature does not violate a core requirement of the statute (Donovan standard). The absence of judge's signature was a technical defect similar to the missing of page 3 from the interception order in the Traitz case. Also, the Leon good faith principle applies to 2518(10)(a) issues, and requires that suppression be denied in this case. U.S. v. Moore, 41 F.3d 370 (8th Cir. 1994).

Wiretap orders that fail to comply with the mandate of 18 U.S.C. 2518(4)(d) that the order specify the identity of the Department of Justice officials who authorized the applications are facially insufficient under 18 U.S.C. 2518(10)(a)(ii), but because these are technical defects that do not undermine the purpose of the statute or prejudice the defendant, the district court's denial of suppression is affirmed. The Tenth Circuit joins the Third, Fifth, Sixth, Seventh, Eighth and Ninth Circuits in holding that the Supreme Court's holdings in U.S. v. Chavez, 416 U.S. 562 (1974) and U.S. v. Giordano, 416 U.S. 505 (1974) that non-substantive violations of Title III do not require suppression of wiretaps found "unlawful" under 2518(10)(a)(i), also applies to wiretap orders found to be facially insufficient under 2518(10)(a)(ii). U.S. v. Radcliff, 331 F.3d 1153 (10th Cir. 2003).

"Even if the reviewing court determines that probable cause was lacking, the drastic remedy of suppression is proper only where (1) the judicial officer issuing the warrant abandoned his or her detached, neutral role, or (2) the agent was dishonest or reckless in preparing the affidavit supporting the issuance of the wiretap order, or (3) the agent's reliance on the warrant was not objectively reasonable. U.S. v. Leon, 468 U.S. 897 (1984)." U.S. v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993); U.S. v. Stokes, 1996 WL 727400 (S.D.N.Y.).

U.S. v. Corrado, 227 F.3d 528 (6th Cir. 2000):

> In reviewing the validity of an electronic surveillance order, we will accord "great deference" to the determinations of the issuing judge. See United States v. Alfano, 838 F.2d 158, 162 (6th Cir. 1988). "Thus, the fact that a later trial judge or reviewing court may feel that a different conclusion was appropriate does not require, nor even authorize, the suppression of evidence gained through such a warrant." Id.

Evidence derived from a lawful wiretap during a criminal investigation and disclosed to revenue agents was not subject to suppression. Extreme remedy of suppression is authorized under section 2515 only when evidence is derived from unlawful, improper or unauthorized interceptions. Legislative history and court decisions require that section 2515 be read "in light of" 18 U.S.C. 2518(10)(a). S. Rep. No. 1097, 90th Cong., 2d Sess. 96, reprinted in (1968) U.S. Code Cong. & Ad. News 2112, 2185. The report declared that section 2518(10)(a) must be read in connection with sections 2515 and 2517, which it limits. It provides the remedy for the right created by section 2515. The Supreme Court has consistently limited suppression under section 2515 to the grounds contained in section 2518(10)(a). U.S. v. Giordano, 416 U.S. 505 (1974); U.S. v. Chavez, 416 U.S. 562 (1974); U.S. v. Donovan, 429 U.S. 413 (1977).

The ECPA does not provide an independent statutory remedy of suppression for interceptions of electronic communications that are nonconstitutional violations. 18 U.S.C. s 2518(10)(c) (1988); S.Rep. No. 99-541, 99th Cong., 2d Sess. 23, reprinted in 1986 U.S. CODE Cong. & Admin. News 3555, 3577. U.S. v. Meriwether, 917 F.2d 955 (6th Cir. 1990); U.S. v. Jones, 364 F. Supp.2d 1303 (D. Utah 2005); U.S. v. Wells, 2000 WL 1231722 (S.D. Ind.).

There is no suppression for nonconstitutional violations of 18 U.S.C. 2701, et seq.(information revealed to third parties is not protected by Fourth Amendment). The only remedy is a civil action pursuant to the provisions of section 2707. U.S. v. Charles, 1998 WL 204696 (D. Mass.); U.S. v. Allen, 2000 CAAF LEXIS 921.

With respect to challenges to the validity of electronic surveillance, the governing law should be that of the place where the electronic surveillance occurred. U.S. v. Longo, 1999 U.S. Dist. LEXIS 13106 (W.D.N.Y.); U.S. v. Restrepo, 890 F. Supp. 180 (E.D.N.Y. 1995); U.S. v. Gerena, 667 F. Supp. 911 (D. Conn. 1987).

No suppression where fact of police officer's use of pen register for illegal "audio tests" was omitted from Title III affidavit, because if the information had been included in the affidavit it would not have diminished probable cause. U.S. v. Lucht, 18 F.3d 541 (8th Cir. 1994).

No suppression where government's inclusion in Title III affidavit of unauthorized pen register information collected during three day period between expiration and renewal of pen register order was not material. U.S. v. Ishola, 1996 WL 197461 (N.D. Ill. 4/19/96).

Chief Judge Korman of the Eastern District of New York denied defendants' motion to suppress conversations recorded through a wiretap on their co-defendant's phone "because the immunized statements that were included in the wiretap application were not material to the issuance of the warrant or to the ultimate recording of the conversations. But even if the immunized statements had been material, that would not have provided a basis for suppression because the statements were made in an effort to receive transactional immunity for a crime that took place nearly a decade before the distinct crime for which the [defendants} are now charged." U.S. v. Sasson, 334 F. Supp.2d 347 (E.D.N.Y. 2004) (includes a comprehensive review and analysis of fifth amendment privilege jurisprudence).

Prohibition in 2518(8)(a) on derivative use at trial of improperly sealed tapes is not to be applied strictly to prohibit use of all evidence that can be connected through a chain of causation to a wiretap tainted by improper sealing of the tape. U.S. v. Donlan, 825 F.2d 653 (2d Cir. 1987).

Use permitted by 2517(2) is not subject to the strictures of 2518(8)(a). Accomplice witness could properly refresh his recollection of various telephone conversations by listening to tapes of

conversations which had been suppressed (no testimonial use under 2517(3)) because of undue delay in sealing. U.S. v. Ricco, 566 F.2d 433 (2d Cir. 1977).

"We hold that, under the unique facts and circumstances of this case--including that the appellees did not participate in or procure the interception [illegally conducted by private parties], and obtained knowledge of the intercepted communications from third parties who made serious charges that an officer was engaged in administrative and criminal misconduct--the appellees' disclosure and use of the information from the intercepted communications, in conducting a preliminary internal affairs investigation, was authorized by §§ 2517(1) and (2). We caution that this holding is narrow, limited to the facts of this case. It should not be read as undermining the salutary purpose of the Act, or as providing a means of sidestepping it." Forsyth v. Barr, 19 F.3d 1527 (5th Cir. 1994).

As a "clean hands" exception to 18 U.S.C. § 2515, the government may use illegally intercepted communications against the victim of the illegal interceptions if the government played no part in the illegal interceptions. U.S. v. Murdock, 63 F.3d 1391 (6th Cir. 1995), cert. denied 5/13/96. The perpetrator of an illegal interception, cannot avail himself of the "clean hands" exception under Murdock. Smoot v. United Transportation Union, 246 F.3d 633 (6th Cir. 2001).

Suppression remedy specified in 18 U.S.C. 2518(10) applies to unlawful interceptions, whereas a civil remedy (18 U.S.C. 2520) applies to unlawful disclosures. U.S. v. Iannelli, 477 F.2d 999 (3d Cir. 1973); U.S. v. Williams, 124 F.3d 411 (3d Cir. 1997); U.S. v. Vento, 533 F.2d 838 (3d Cir. 1976); Fleming v. U.S., 547 F.2d 872 (5th Cir. 1977). See U.S. v. Cardall, 773 F.2d 1128 (10th Cir. 1985); Dickens v. U.S., 671 F.2d 969 (6th Cir. 1982); U.S. v. Horton, 601 F.2d 319 (7th Cir. 1979) (main thrust of 18 U.S.C. 2515 is to exclude evidence illegally seized, not evidence the disclosure of which was in violation of chapter 119 of the United States Code); U.S. v. Barnes, 47 F.3d 963 (8th Cir. 1995). U.S. v. Dorfman, 532 F. Supp. 1118 (N.D. Ill. 1981) (refusing to apply remedy of suppression as a matter of law when defendants alleged that the government disclosed material obtained from wiretaps and other electronic surveillance to the press in violation of 18 U.S.C. 2517); U.S. v. Cleveland, 1997 WL 178644 (E.D. La. 4/7/97) (suppression denied for alleged violation of 18 U.S.C. 2517 involving unsealing of search warrant affidavits containing Title III interceptions); London v. Commissioner of Internal Revenue, 1998 Tax Ct. Memo LEXIS 348 (9/29//98).

Agents inadvertently intercepted numerous attorney communications, but the defendants failed to prove that each of these communications were attorney-client privileged and they also failed to prove that the agents acted in bad faith. It was error to impose suppression as punishment for these inadvertent interceptions of attorney communications. Because there was no bad faith attempt to obtain privileged conversations, those conversations should be suppressed on an individual basis at or before trial. U.S. v. Ozar, 50 F.3d 1440 (8th Cir. 1995).

Suppression of only the attorney/client phone call that was inadvertently, but negligently, intercepted by a police officer monitoring a state wiretap was an appropriate remedy for the officer's violation of the amended minimization order. U.S. v. Charles, 213 F.3d 10 (1st Cir. 2000).

Errors in minimizing one particular interception within the context of a lengthy and complex investigation do not automatically warrant the suppression of all the evidence obtained through electronic surveillance. Total suppression would not follow unless the defendant demonstrates that the entire surveillance was tainted. U.S. v. Baltas, 236 F.3d 27 (1st Cir. 2001).

Because Stephen Edwards was not a named interceptee or a “named or known coconspirator,” the interception of his conversations violated the limitations contained in the Title III order authorizing oral interceptions at the law office of Edwin Edwards. The illegal interceptions should have been suppressed, but the error was harmless. U.S. v. Edwards, 303 F.3d 606 (5th Cir. 2002).

"Although neither the Supreme Court nor the Second Circuit has squarely addressed this issue, several courts have held that a failure to minimize interceptions requires suppression only of the unauthorized interceptions and not of all conversations--much less the fruits of all conversations--overheard pursuant to the court-authorized surveillance." U.S. v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995).

Utah State wiretap application contained no alternative investigative statement or incorporation by reference of such facts, and therefore suppression of intercepts and derivative evidence was required. The Utah statute mirrors the federal provisions contained in 18 U.S.C. 2518. U.S. v. Mondragon, 52 F.3d 291 (10th Cir. 1995).

The district court suppressed four Title III spin-offs (four phones and two pagers) for failure to satisfy the necessity requirements of 2518(1)(c), 2518(3)(c). The Tenth Circuit reversed as to all targeted facilities but one pager and one telephone used by a subject as to whom the government had not made "a full and complete" necessity statement in a particularized manner. "Even with an ongoing investigation of a suspected drug conspiracy, the government may not simply move swiftly from wiretap to wiretap. Rather, under Title III, it must always pause to consider whether normal investigative procedures could be used effectively, particularly in light of any evidence obtained as a result of each succeeding wiretap.” U.S. v. Castillo-Garcia, 117 F.3d 1179 (10th Cir. 1997).

The Tenth Circuit affirmed the suppression of all Title III evidence (original and one extension order targeting a pager; original and one extension order targeting a cellular telephone) because the original affidavit failed to discuss or pursue reasonable alternative investigative methods which were suggested by the facts discussed in the affidavit. U.S. v. Arrington, 2000 WL 775576 (10th Cir.) (unpublished) (see above “Alternative Investigative Showing” section for opinion details).

Wiretap evidence was suppressed because the affiant withheld information and misrepresented facts to the issuing judge with regard to the adequacy of alternative investigative techniques. "When the deceptive character of the affidavit is considered in light of the agent's conduct at the evidentiary hearing, a pattern of behavior intended to obtain and protect the wiretap emerges and shows that the government acted without respect for the necessity requirements of § 2518(1)(c)." U.S. v. Ailemen, 986 F. Supp. 1228 (N.D. Cal. 1997).

A DEA agent working on an OCDETF with an FBI agent had a duty to disclose to the FBI agent all information material to the FBI agent's application for a wiretap. It is as a representative of the government that an applicant for wiretap authorization applies to the court. The government cannot so compartmentalize its activities that it hides from the court information that might be relevant. If the DEA agent had material facts, the duty to disclose was enforceable by the AUSA going to the agent's superiors and obtaining the reports. The DEA agent's intentional failure to disclose is attributable to the FBI affiant. The motive for withholding the information is not relevant. Suppression is not warranted, however, because the nondisclosure of the DEA information ("the bane of government agencies charged with overlapping tasks sometimes more zealous in protecting their turf than in achieving the common objective") in the original FBI Title III affidavit and an inaccurate and misleading statement and omission in an extension affidavit

were not material. If the omitted information had been added to the original affidavit and the misleading statement and omission corrected in the extension affidavit, an impartial judge would still have seen the necessity of the wiretaps to "knock out the entire organization." U.S. v. Aviles, 170 F.3d 863 (9th Cir. 1999).

Regarding a Title III affidavit's failure to disclose a CI's prior drug trafficking conviction, his past involvement with some defendants, and other indicia of his possible unreliability, the First Circuit held that the CI's information was not material to the finding of probable cause and therefore not a basis for suppression, and that no Franks hearing was required because the defendants failed to make the requisite showing of materiality. Regarding the affidavit's omission of information concerning the CI's background, the Court opined as follows:

> The affidavit was, to put it mildly, economical on this point, stating only that there was no indication that Hernandez "has been less than truthful at any time with regard to this investigation." This statement was crafted carefully to avoid mention of facts that would call Hernandez's trustworthiness into serious question. We are concerned that such significant omissions could thwart the intent of Title III and mislead an issuing judge, who relies on the government to present the full case for its belief in probable cause, including any contraindications. The troubling omissions here have less significance because the affidavit also included large quantities of evidence from sources other than Hernandez.

U.S. v. Nelson-Rodriguez, 319 F.3d 12 (1st Cir. 2003).

Defendant's request for a Franks hearing was denied because he failed to make the requisite showing that affiant's omission of alleged "exculpatory" conversation between cooperating witness and defendant was intentionally misleading and material. U.S. v. Bankston, 182 F.3d 296 (5th Cir. 1999).

The government conceded that affiant and DEA were mistaken in their initial identification of subject and the assignment of a criminal history. Once discovered, the government omitted this information from future affidavits, drafted reports to this effect, and informed defendants of the mistake. Such mistakes do not constitute a knowing false statement or reckless disregard for the truth. It also falls short of what is required for a Franks hearing. Even if this were not the case, the misstatements are immaterial to the probable cause determination and therefore a Franks hearing is unnecessary. U.S. v. Velazquez, 1997 WL 564674 (N.D. Ill.).

The application established probable cause. The cumulative effect of the alleged misrepresentations and omissions do not undermine the basis for probable cause, and the defendant, having failed to make the requisite showing, is not entitled to a Franks hearing. U.S. v. Jarding, 2002 WL 1905533 (N.D. Ill.).

Wiretap evidence suppressed because of individual and institutional reckless non-compliance with section 2518(1)(e) (disclosure of previous applications). U.S. v. Luong, No. CR-94-0094 (N.D. Cal. 7/14/98)(unpublished).

"18 U.S.C. § 371 was an enumerated offense for the purposes of 18 U.S.C. § 2516, where the wiretap order concurrently authorized investigation of two other offenses specifically listed in § 2516. However, this case presents no opportunity to determine whether a wiretap order including only 18 U.S.C. § 371, without additional explicitly enumerated offenses, would survive appellate review." Mere references to non-enumerated offenses will not invalidate wiretap application documents or orders. "[T]he incorrect description of suspected non-enumerated offenses as enumerated in application materials and findings in a wiretap order does not invalidate that order where the authorization to wiretap itself was limited to only enumerated offenses. The question of whether an order authorizing wiretapping in investigation of both enumerated and non-

enumerated offenses would survive review is saved for another day." U.S. v. Smart, 278 F.3d 1168 (10th Cir. 2002).

"The reference to additional statutory violations was irrelevant; once the acts of taping were justified under 18 U.S.C. § 2518 by any adequate evidence, that reference furnishes no basis of suppression." U.S. v. Mongelli, 799 F. Supp. 21 (S.D.N.Y. 1992).

"The inaccurate code words and summaries demonstrate a troubling carelessness, but do not support an inference that [affiant] was attempting to mislead or was acting with reckless disregard of the true content of the conversations." U.S. v. Estrada, 1995 WL 577757 (S.D.N.Y.).

Wiretap interception of conversations generated by an illegal detention and unconstitutional search must be suppressed as fruit of the poisonous tree. U.S. v. Elmore, 2001 WL 1339002 (S.D. Ohio).

Internet service provider MindSpring supplied a police officer with defendant's name, address, credit card number, e-mail address, home and work telephone numbers, fax number, and the fact that the Defendant's account was connected to the Internet using a specific Internet Protocol (IP) address. At the hearing on the defendant's motion to suppress, the government conceded the invalidity of the New Hampshire state subpoena used to obtain the information from the defendant's ISP, Mindspring, located in Atlanta, Georgia. The question before the court was whether the court must suppress the information obtained from MindSpring, and all that flowed from it, because the government failed to obtain a proper subpoena. Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA does not represent a legislative determination of a reasonable expectation of privacy in non-content information released by ISPs. The ECPA does not even provide for the relief requested in this case (suppression). Section 2707 provides a civil remedy for aggrieved individuals and Section 2708 states that this is the only remedy for nonconstitutional violations of 18 U.S.C. 2701-2711. U.S. v. Hambrick, 2000 U.S. App. LEXIS 18665 (4th Cir) (unpublished); Freedman v. America Online, Inc., 2005 WL 1899381 (D. Conn.) (citing Hambrick).

Impeachment Exception to 2515

The recording of a telephone conversation obtained by the government in violation of Title III can properly be used to impeach the defendant's testimony. "Evidence seized in violation of the Fourth Amendment or the federal wiretapping statute cannot be used by the government in its case in chief. But, if the defendant chooses to testify, and swears to a sequence of events inconsistent with his own previously recorded statements, the Constitution does not require the government to leave the lie (or what it contends to be a lie) unchallenged." U.S. v. Baftiri, 263 F.3d 856 (8th Cir. 2001)(citing Williams v. Poulos, 11 F.3d 271, (1st Cir. 1993); U.S. v. Echavarria-Olarte, 904 F.2d 1391 (9th Cir. 1990); Jacks v. Duckworth, 651 F.2d 480 (7th Cir. 1981); U.S. v. Caron, 474 F.2d 506 (5th Cir. 1973)).

The rule regarding use of illegally seized evidence for purposes of impeachment was not altered by 18 U.S.C. 2515. U.S. v. Caron, 474 F.2d 506 (5th Cir. 1973).

Even if wiretaps were illegal, to the extent they contradicted statements made on direct examination, they were admissible for purposes of impeachment. U.S. v. Echavarria-Olarte, 904 F.2d 1391 (9th Cir. 1990)

The impeachment exception of §2515 is limited to criminal actions brought pursuant to Title III. Illegal interceptions (and their
transcriptions) cannot, pursuant to the criminal impeachment exception, be introduced into evidence for impeachment purposes in civil cases. Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993).

"Impeachment" exception allows use of illegally intercepted communications to impeach a testifying defendant (but not a witness). U.S. v. Lanoue, 71 F.3d 966 (1st Cir. 1995).

Defendant is liable for wiretapping his wife's telephone conversations, but illegal intercepts are admissible to impeach witness's evidence presented to the court in an affidavit, and therefore submission of the transcripts of the illegal intercepts to the court for such purposes was not improper. Culbertson v. Culbertson, 143 F.3d 825 (4th Cir. 1998).

Federal Use of State Wiretap Evidence

"Congress was agreeable to allowing the states to enact measures that were more strict than the federal law, but was not agreeable to allowing more restrictive state laws to govern federal prosecutions." Federal law governs the admissibility of state wiretap evidence. U.S. v. McNulty, 729 F.2d 1243 (10th Cir. 1984) (en banc).

Where the issue involves the validity of a state wiretap order, rather than violation of state law governing the post-interception preservation or use of the information, the more stringent state requirements must be respected by federal courts. It is only wiretapping by state officers under § 2516(2) which requires further authorization by state statute. Section 2515 requires the exclusion of wiretap evidence from any court proceeding if its disclosure would violate the federal act; no mention is made of any state law. The federal statute itself requires deference to state law on the question of the validity of a wiretap order obtained in state court under state law. U.S. v. McNulty, 729 F.2d 1243 (10th Cir. 1984) (en banc); U.S. v. Sotomayor, 592 F.2d 1219 (2d Cir. 1979).

No federal suppression of Louisiana wiretaps signed by an assistant attorney general pursuant to delegated authority and monitored by private contractors. U.S. v. Davis, 2005 U.S. App. LEXIS 3770 (5th Cir.)(unpublished).

The state law cannot preempt the federal unless the federal act itself sanctions the application of state standards. Warrantless interceptions where one party consents are specifically permitted under 18 U.S.C. 2511(2)(c) and (d). Where one party consented and no state court order or warrant was obtained, the requirement of 18 U.S.C. 2516(2) that the applicable state law must be complied with, does not come into play. It is only wiretapping by state officers under § 2516(2) which requires further authorization by state statute. State law is simply irrelevant in a federal prosecution if the investigating officers, even state officers acting alone, are not acting under the authorization of a state court. The legislative intent that federal law is to prevail in case of conflict is further indicated by 18 U.S.C. 2520, which provides that a good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under Chapter 119 "or under any other law." U.S. v. Glasco, 917 F.2d 797 (4th Cir. 1990); U.S. v. Masko, 2000 U.S. App. LEXIS 19057 (4th Cir.)(unpublished)(following Glasco); U.S. v. D'Antoni, 874 F.2d 1214 (7th Cir. 1989); U.S. v. McNulty, 729 F.2d 1243 (10th Cir. 1984) (en banc); U.S. v. Nelligan, 573 F.2d 251 (5th Cir. 1978); U.S. v. Workman, 80 F.3d 688 (2d Cir. 1996); U.S. v. Mathis, 96 F.3d 1577 (11th Cir. 1996).

State court's suppression order did not foreclose consideration of the state wiretap evidence by the federal grand jury and it was not binding on the federal district court. U.S. v. Miller, 116 F.3d 641 (2d Cir. 1997).

It is a general rule that federal district courts will decide evidence questions in federal criminal cases on the basis of federal, rather than state, law. "We are not aware of any provision of Title III that requires or authorizes the suppression of evidence in federal court simply because a state court would have ordered suppression as a remedy for a violation of the state disclosure provision." U.S. v. Williams, 124 F.3d 411 (3d Cir. 1997).

"We have consistently held that evidence obtained in violation of a state law is admissible in a federal criminal trial if the evidence was obtained without violating the Constitution or federal law." U.S. v. Padilla-Pena, 129 F.3d 457 (8th Cir. 1997).

In federal criminal prosecutions, the admissibility of wiretap evidence is a question of federal law. U.S. v. Sutherland, 929 F.2d 765 (1st Cir. 1991); U.S. v. Charles, 213 F.3d 10 (1st Cir. 2000) (citing Sutherland, Miller, Williams and Padilla-Pena).

Federal court need not decide whether one party consensual recording (lawful under 18 U.S.C. 2511(2)(d)) of defendant's call violated California law because federal law governs the admissibility of evidence in a federal criminal trial. "Evidence admissible under federal law cannot be excluded because it would be inadmissible under state law." U.S. v. Pforzheimer, 826 F.2d 200 (2d Cir. 1987) (quoting U.S. v. Quinones, 758 F.2d 40 (1st Cir. 1985); U.S. v. Adams, 694 F.2d 200 (9th Cir. 1982); U.S. v. Morrison, 153 F.3d 34 (2d Cir. 1998).

Plaintiff may use one-party consensual recording to advance its federal law claim even though the recording violated Illinois state law. Century Consultants, Ltd. v. Miller Group, Inc., 2005 WL 3108455 (C.D. Ill.) (unpublished).

Federal law governs the admissibility of evidence in federal diversity suits, not state law. Tapes of consensually recorded telephone conversations, lawful under 18 U.S.C. 2511(2)(d), were admissible. Bauers v. Board of Regents of the University of Wisconsin, 2002 WL 486062 (7th Cir.)(unpublished).

Good Faith Exception

The good faith exception articulated in U.S. v. Leon, 468 U.S. 897 (1984) has been extended by numerous courts to electronic surveillance evidence. See U.S. v. Moore, 41 F.3d 370 (8th Cir. 1994); U.S. v. Holloway, 1998 U.S. App. LEXIS 30022 (6th Cir.) (footnote, citing Moore, acknowledges that good faith exception may apply to wiretaps); U.S. v. Tham, 948 F.2d 1107 (9th Cir. 1991); U.S. v. Malekzadeh, 855 F.2d 1492 (11th Cir. 1988); U.S. v. Scala, 388 F. Supp.2d 396 (S.D.N.Y. 2005); U.S. v. Padin, 2005 U.S. Dist. LEXIS 5994 (W.D.N.Y.); U.S. v. Gotti, 42 F. Supp.2d 252 (S.D.N.Y. 1999); U.S. v. Gangi, 33 F. Supp.2d 303 (S.D.N.Y. 1999); U.S. v. Bellomo, 954 F. Supp. 630 (S.D.N.Y. 1997); U.S. v. Ambrosio, 898 F. Supp. 177 (S.D.N.Y. 1995) U.S. v. Milan-Colon, 1992 WL 236218 (S.D.N.Y.); U.S. v. Gambino, 741 F. Supp. 412 (S.D.N.Y. 1990). Some courts have refused to do so. See, e.g., U.S. v. Orozco, 630 F. Supp. 1418 (S.D. Cal. 1986); U.S. v. Ward, 808 F. Supp. 803 (S.D. Ga. 1992); see also U.S. v. McGuinness, 764 F. Supp. 888 (S.D.N.Y. 1991); U.S. v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995) (noting conflict among courts).

Good faith exception to exclusionary rule precluded suppression of wiretap where applicant for pen register relied on existing legal interpretation of statute. U.S. v. Butz, 982 F.2d 1378 (9th Cir. 1993); U.S. v. Aiello, 771 F.2d 621 (2nd Cir. 1985).

Exclusionary rule does not apply to evidence obtained by police who relied in good faith upon an Illinois statute authorizing warrantless administrative searches, but which was subsequently found to violate the Fourth Amendment. Illinois v. Krull, 480 U.S. 340 (1986)

The good faith exception to the exclusionary rule applies to sneak and peek search warrants. U.S. v. Ludwig, 902 F. Supp. 121 (W.D. Tex. 1995).

Compilation Tapes

As long as the government complies with Title III (sealing of original tapes), it may, at trial, disclose the contents of the recordings in whatever fashion it chooses, including the use of duplicate and compilation tapes. If Congress barred the use of duplicate tapes, the result would be unwieldy and cumbersome. Moreover, the use of duplicates allows the originals to remain sealed, thereby preserving the authenticity of the original tapes. Also significant is that the DEA's set of tapes was as "original" as the set of tapes sealed in accord with Title III (monitoring equipment made three sets of original recordings). Either set of tapes could have been chosen to be sealed, and the government was not required to compare the two sets of tapes to determine that they were the same: the procedure (and supervision over the procedure) established that the two sets of tapes were twins. Addressing the same issue, the First Circuit noted that no comparison of the tapes was required: "This is not a situation, as defendant implies, where one tape recording was made and subsequently copies were made from it. There was no need for [the agent] to check his tape against the original tape; he used an original tape." U.S. v. Rengifo, 789 F.2d 975, 980 (1st Cir.1986). And Special Agent Grant did compare the compilation tape he made to the DEA's set of tapes. Other courts have specifically approved the same procedure used by the government in this case. In U.S. v. Denton, 556 F.2d 811, 816 (6th Cir.1977), the Sixth Circuit held that the government could enter a composite tape as a summary pursuant to Fed.R.Evid. 1006, and that the government laid a proper foundation regarding the accuracy and authenticity of the composite tape. U.S. v. Rivera, 153 F.3d 809 (7th Cir. 1998).

Foundation

A proper foundation for the admission of audiotapes may be established in two ways: a chain of custody could establish that the tapes are in the same condition as when recorded, or alternatively, other testimony could be used to establish the accuracy and trustworthiness of the evidence. A presumption that a system of regularity accompanies the handling of evidence attaches if the exhibits are at all times within official custody. Furthermore, the possibility of a break in the chain of custody of evidence goes to the weight of the evidence, not its admissibility. U.S. v. Rivera, 153 F.3d 809 (7th Cir. 1998).

Authentication

Tape recorded conversations can be authenticated by someone who did not participate in or personally overhear the subject matter of the recording in evidence. It is sufficient that the testifying witness state that he supervised the activities of the agents actually manning the listening post, and visited the listening post periodically to observe the agents. The witness also

described in detail the custody procedures followed to maintain the integrity of the recordings. According to the court, this testimony was sufficient to raise a presumption of official regularity, discharging the government's burden of authentication. U.S. v. Rengifo, 789 F.2d 975 (1st Cir. 1986); U.S. v. Green, 175 F.3d 822 (10th Cir. 1999); U.S. v. Millan, 817 F. Supp. 1072 (S.D.N.Y. 1993).

It is essential to distinguish between excluding evidence for want of adequate authentication, and challenging its weight. The defendants were entitled to and did question the weight that the jury should give the tape recordings in light of the possibility of tampering, but questions of authentication are governed by Fed. R. Evid. 901(a), which merely requires "evidence sufficient to support a finding that the matter in question is what its proponent claims," that is, that the recordings played to the jury were in fact recordings of the defendants' conversations. Testimony by an "ear" witness is sufficient. Only in "extraordinary" circumstances will the appellate court reverse the trial judge's decision to admit tape recordings over objections based on lack of authentication. U.S. v. Boyd, 208 F.3d 638 (7th Cir. 2000).

Informant's consensually recorded oral and wire communications contained erasures, gaps and some unintelligible words, and no chain of custody was established. The informant testified that they were accurate recordings of his conversations. There was no evidence of tampering. The defendants did not deny that it is their voices on the tapes. Authentication under FRE 901 requires nothing more than adequate evidence of genuineness. There are no rigid rules for such. Any complaint about possible exculpatory material on the omitted portions of the recorded conversations would not raise a Brady issue in that the defendants were parties to the conversations and therefore equally aware. U.S. v. Dawson, 425 F.3d 389 (7th Cir. 2005).

Transcript Use

It is not a necessary predicate for admission of transcripts of tape recordings that each officer who prepared the transcript testify to its accuracy. U.S. v. Green, 40 F.3d 1167 (11th Cir. 1994).

Government agent's testimony that a pen register intercepted and recorded pager messages and a clone pager confirmed the accuracy of that system was sufficient, under Rule 901, to authenticate the pager charts as records of the messages sent to the pager of a purported drug organization leader. U.S. v. Alicea-Cardoza, 132 F.3d 1 (1st Cir. 1997).

District court did not abuse its discretion in allowing use of transcript at trial (audibility problems and no stipulation as to accuracy). U.S. v. Wilkinson, 53 F.3d 757 (6th Cir. 1995).

Because the defendants pointed to no specific error in the identifications of the speakers, and because a sufficient foundation existed supporting the identifications, there was no abuse of the district court's discretion in its decision to permit the jurors to view the transcripts. U.S. v. Frazier, 280 F.3d 835 (8th Cir. 2002).

While transcripts of English conversations are typically used as
aids for the jury and not admitted into evidence, courts have admitted English transcripts of foreign language conversations as substantive evidence in view of the fact that the jury would not understand the spoken language. See U.S. v. Pena-Espinoza, 47 F.3d 356 (9th Cir. 1995); U.S. v. Garcia, 20 F.3d 670 (6th Cir. 1994); U.S. v. Gonzalez-Balderas, 11 F.3d 1218 (5th Cir. 1994). In this case the district court cautioned the jury with respect to the transcripts of the Spanish language conversations, noting that there was no agreement or stipulation as to the identity of speakers or the accuracy of the transcripts. Under the circumstances, we find that the district court

did not abuse its discretion in admitting into evidence the written translations of the Spanish language conversations. U.S. v. Borda, 1999 WL 294540 (4th Cir (Md.))(unpublished).

Spanish police duplicated conversations onto cassettes from master tape which was reused. Generally, the Spanish police made a Spanish language transcript while listening to the duplicate cassette, but on occasions the transcript was made directly from the master tape. The district court noted that the procedures fell short of the safeguards provided in this country, but comported with Spanish law. Defense counsel had ample opportunity to cross-examine the Spanish police officers in front of the jury on the procedures that they followed in making the transcripts and on the accuracy of their identification of the participants. U.S. v. Ross, 33 F.3d 1507 (11th Cir. 1994).

Audibility

The mere fact that portions of a tape are inaudible does not require exclusion of the tape. "Unless the unintelligible portions are so substantial as to render the recordings as a whole untrustworthy the recording is admissible, and the decision should be left to the sound discretion of the judge." U.S. v. Arango-Correa, 851 F.2d 54 (2d Cir. 1988); U.S. v. Wilkinson, 53 F.3d 757 (6th Cir. 1995); U.S. v. Rrapi, 175 F.3d 742 (9th Cir. 1999).

Admission of Tapes

All the tapes admitted by the district judge consisted of conversations to which the defendant was a party. Thus, the conversations were admissions by a party-opponent and not hearsay, pursuant to Fed. R. Evid. 801(d)(2)(a). U.S. v. Quintana, 70 F.3d 1167 (10th Cir. 1995).

Expert Testimony

"This Court has repeatedly held that in narcotics cases, expert testimony can assist the jury in understanding transactions and terminology." The expert witness's chart that was admitted into evidence included data from intercepted calls not offered into evidence, but the original tape recordings were made available both to the defendant and the court. This complied with the requirements of Fed. R. Evid. 1006. In addition, the district judge cautioned the jury that the chart was simply representative of the expert's testimony. U.S. v. Quintana, 70 F.3d 1167 (10th Cir. 1995).

Two DEA agents testified as experts on drug code language. They were properly qualified as experts under Federal Rules of Evidence 702. The agents' lack of fluency in Spanish does not prohibit them from interpreting drug code language obtained from English translations of Spanish conversations. The defendants' use of simple pronouns during intercepted conversations was a proper subject of expert testimony on drug code language. U.S. v. Ceballos, 302 F.3d 679 (7th Cir. 2002).

Qualified Privilege of Nondisclosure for Sensitive Investigative Techniques

The government has a qualified privilege not to disclose sensitive investigative techniques. This privilege can be overcome if the defendant can show an authentic and sufficient need (no adequate alternative means) for the information that outweighs the government's privilege. U.S.

v. Angiulo, 847 F.2d 956 (1st Cir. 1988); U.S. v. Cintolo, 818 F.2d 980 (1st Cir. 1987); U.S. v. Van Horn, 789 F.2d 1492 (11th Cir. 1986); U.S. v. O'Neill, 52 F. Supp.2d 954 (E.D. Wis. 1999).

National Security

Emergency Under 2518(7)(a)(ii)

No help is found in the legislative history.

Treatise research yields the following:

Fishman (Wiretapping and Eavesdropping), in the December 1991 Pocket Part at page 251, states that, notwithstanding the reference to national security, the only law enforcement contexts in which 2518(7) permits warrantless emergency surveillance are those involving "immediate danger of death or serious physical injury to any person," or "conspiratorial activities characteristic of organized crime." Interceptions conducted primarily for national security purposes, rather than to enforce the criminal law, are regulated by FISA. Senate Report Judiciary Committee, No. 98-225 at 395 n.9.

Carr (Electronic Surveillance), at page 3-116 states:

"Though not repealed upon adoption of the Foreign Intelligence Surveillance Act, the authorization in 2518(7) to conduct warrantless national security surveillance has been superseded by the more stringent requirement of prior notice to a judicial officer found in 1805(e) of FISA."

Foreign Intelligence Surveillance Act (FISA)

50 U.S.C. 1801-1811 (1982)

FISA does not violate the Fourth Amendment. U.S. v. Johnson, 952 F.2d 565 (1st Cir. 1991); U.S. v. Pelton, 835 F.2d 1067 (4th Cir. 1987); U.S. v. Cavanagh, 807 F.2d 787 (9th Cir. 1987); U.S. v. Duggan, 743 F.2d 59 (2d Cir. 1984).

Post-USA Patriot Act FISA permitting the government to obtain FISA orders when the investigation has “a significant” foreign intelligence purpose is constitutional because the surveillances it authorizes are reasonable. In re: Sealed Case No. 02-001, 310 F.3d 717 (F.I.S. Ct. 2002).

An immunized witness refused to testify before a special grand jury and was thereafter incarcerated pursuant to the district court’s civil contempt order. The witness unsuccessfully asserted that the government was collaterally estopped from seeking contempt given another court’s decision five years earlier that incarceration would not coerce the witness into testifying at that time before a different grand jury. The witness also claimed that his presence before the grand jury was procured through information gained in illegal FISA surveillance. The Circuit Court reviewed the FISA materials and procedures in this case and held that there is no need to disclose any of the FISA materials to the Appellant and that the FISA orders were properly issued. In Re: Grand Jury Proceedings of the Special April 2002 Grand Jury, 2003 U.S. App. LEXIS 20262 (7th Cir.).

Extraterritoriality

Fourth Amendment

The Fourth Amendment does not apply to searches and seizures abroad if the target of the search is an alien with no voluntary attachment to the United States. U.S. v. Verdugo-Urquidez, 494 U.S. 259 (1990); U.S. v. Barona, 56 F.3d 1087 (9th Cir. 1995) (Danish and Italian wiretaps).

A U.S. court has proper jurisdiction over a criminal defendant forcibly abducted from his country if the forcible abduction is not a treaty violation. U.S. v. Alvarez-Machain, 504 U.S. 655 (1992).

A defendant (El-Hage, an American citizen) in the prosecution of the Bin Laden terrorist organization sought suppression of evidence derived from warrantless wiretaps conducted by the United States intelligence community on several telephone lines in Nairobi, Kenya and from a warrantless search of his residence in Nairobi, Kenya. The district court denied the motion without a hearing. The court adopted the foreign intelligence exception to the warrant requirement for searches conducted abroad, primarily for foreign intelligence purposes, targeting foreign powers (or their agents), and authorized by the President (or his delegate, the Attorney General). "Despite El-Hage's assertions to the contrary, the language employed by the Justices in Verdugo-Urquidez, 494 U.S. 259 (1990) who challenged the overseas application of the warrant requirement does not suggest that the criticisms were limited to cases involving noncitizens. The Justices' skeptical remarks were universally critical of the impotence of American warrants overseas and were not explicitly limited to application to noncitizens. There was no indication that any of the Justices would espouse a different view of the warrant requirement for searches of Americans abroad." All warrantless searches are still governed by the reasonableness requirement and can be challenged in ex post criminal or civil proceedings. The automated recording of the phone lines was not unreasonable (scope of activities, actual use, foreign language and possibility of code use). U.S. v. Bin Laden, 126 F. Supp.2d 264 (S.D.N.Y. 2000).

Although the Fourth Amendment applies when the FBI has a cooperating witness consensually monitor conversations in Japan without Japan's authorization, there was no violation of the Fourth Amendment rights of the non-consenting party because he does not have a reasonable expectation of privacy in utterances voluntarily, but unknowingly, made to the cooperating witness and therefore there was no search cognizable under Fourth Amendment jurisprudence. The fact that such monitoring violated Japanese law was only one factor in determining the reasonableness of the search. The ultimate determination of admissibility of the evidence is governed by U.S. law. The extent to which the government violated Japanese law raises a political question of international relations and is outside the court's jurisdiction. U.S. v. Andreas, 1998 WL 42261 (N.D. Ill. 1/30/98).

There are two exceptions to the rule that the exclusionary rule does not require suppression of evidence seized by foreign police agents: where foreign police conduct shocks the judicial conscience, and where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts. U.S. v. Mitro, 880 F.2d 1480 (1st Cir. 1989); U.S. v. Delaplane, 778 F.2d 570 (10th Cir. 1985) (Canadian wiretap); Stowe v. DeVoy, 588 F.2d 336 (2d Cir. 1978) (Canadian wiretap) U.S. v. Mount, 757 F.2d 1315 (D.C. Cir. 1985) (British police search)); U.S. v. Barona, 56 F.3d 1087 (9th Cir. 1995) (Danish and Italian wiretaps).

DEA's supplying of telephone numbers and wiretapping equipment to Turkish officials did not render Turkish taps subject to Fourth Amendment. U.S. v. Maturo, 982 F.2d 57 (2d Cir. 1992).

Even when no authorization for a foreign wiretap was secured, in violation of the foreign law itself, evidence was not excluded under the "shocks the judicial conscience" rationale. If the wiretap was a joint venture involving U.S. and foreign agents, the court must decide whether the search was reasonable under the Fourth Amendment by first consulting the law of the relevant foreign countries. The Fourth Amendment protects a much narrower class of individuals ("the People of the United States") than the Fifth Amendment ("persons"). U.S. v. Barona, 56 F.3d 1087 (9th Cir. 1995) (Danish wiretaps were joint ventures; Italian wiretap was not joint venture).

Suppression of evidence derived from Canadian wiretap and evidentiary hearing concerning circumstances under which the wiretap was obtained were not required on ground that defendants in United States could not obtain access to sealed application and affidavit where it was pure speculation that unsealing of packet might have revealed conduct capable of shocking judicial conscience. U.S. v. Mitro, 880 F.2d 1480 (1st Cir. 1989).

The fact that information about an imminent heroin transaction in New York was given to DEA by Colombian law enforcement agents who were conducting a Colombian wiretap does not lessen its reliability. DEA verified that the Colombian wiretap was valid under Colombian law. Defendants did not argue that the Colombian wiretap investigation "shocks the judicial conscience" or was conducted with the cooperation of domestic law enforcement officials. See Maturo. U.S. v. Gutierrez, 1999 U.S. Dist. LEXIS 11436 (S.D.N.Y. 7/28/99).

Wiretaps conducted in Dominican Republic were not joint ventures with the United States nor were they shocking to the judicial conscience. U.S. v. Castro, 175 F. Supp.2d 129 (D. P.R. 2001).

Office of Legal Counsel Opinions

Authority of the Federal Bureau of Investigation to Override Customary or Other International Law in the Course of Extraterritorial Law Enforcement Activities, June 21, 1989, Memorandum for Dick Thornburgh, Attorney General, from William P. Barr, Assistant Attorney General, Office of Legal Counsel:

> This Office concludes that at the direction of the President or the Attorney General the FBI may use its statutory authority under 28 U.S.C. § 533(1) and 18 U.S.C. § 3052 to investigate and arrest individuals for violations of applicable United States law, even if those actions depart from customary international law or unexecuted treaties. Moreover, we conclude that the President, acting through the Attorney General, has inherent constitutional authority to deploy the FBI to investigate and arrest individuals for violations of United States law, even if those actions contravene international law. Finally, we conclude that an arrest that is inconsistent with international or foreign law does not violate the Fourth Amendment.

13 U.S. Op. Off. Legal Counsel 195 (1989 WL 418311 (O.L.C.)).

Extraterritorial Effect of the Posse Comitatus Act, November 3, 1989, William P. Barr, Assistant Attorney General, Office of Legal Counsel, concluding that the Posse Comitatus Act does not apply outside the territory of the United States. 13 U.S. Op. Off. Legal Counsel 387 (1989 WL 418333 (O.L.C.)).

Electronic Surveillance Statute

Like the Omnibus Crime Control and Safe Streets Act of 1968 which it revises, the Electronic Communications Privacy Act regulates only those interceptions conducted within the territorial United States. S. Rep. No. 541, p. 12.

The Bill of Rights has extraterritorial application to the conduct abroad of federal agents directed against U.S. citizens. 18 U.S.C. 2510, et seq. has no application outside of the United States. U.S. v. Toscanino, 500 F.2d 267 (2d Cir. 1974). The citizenship of the person whose phone is tapped is irrelevant. Stowe v. DeVoy, 588 F.2d 336 (2d Cir. 1978) (Canadian wiretap).

Pen Register/Trap and Trace

Practice

Use of pen register does not constitute a search for purposes of Fourth Amendment analysis. Smith v. Maryland, 442 U.S. 735 (1979).

Both federal and Oregon courts recognize that trap and trace devices do not intercept the substance or content of communications, do not reveal the identity of the parties who might be communicating, and do not indicate whether a communication actually took place. Thus, the defendants (city and police officers) could not have disclosed the content of any communication, as the trap and trace devices did not intercept any communication. American Agriculture, Inc. v. Shropshire, 2001 U.S. Dist. LEXIS 13355 (D. Or.).

"Title III makes it clear that devices which satisfy the statutory definition of pen registers or trap and trace devices set forth in 18 U.S.C. § 3127 are exempted from its requirements. See 18 U.S.C. § 2511(2)(h)." U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995).

Pen register's mere potential for an invasion of privacy does not implicate the Fourth Amendment. U.S. v. Shnayderman, 1993 WL 524782 (E.D. Pa.); U.S. v. Love, 859 F. Supp. 725 (S.D.N.Y. 1994).

Title III guards against actual infringements of privacy, not purely hypothetical ones. Section 2516(2)'s reference to compliance with state law for wiretap authorizations was not applicable to the pen registers employed here (New York state) and that section provided no basis for requiring the district court to hold a hearing to determine whether those pen registers, though not capable in the form used of intercepting the contents of wire communications, were capable of being modified to enable such interception. U.S. v. Miller, 116 F.3d 641 (2d Cir. 1997); U.S. v. Veksler, 62 F.3d 544 (3d Cir. 1995) ("mere suggestion that pen register equipment is now capable of misuse does not give us a basis to depart from the controlling precedent of the Smith case").

No suppression where fact of police officer's use of pen register for illegal "audio tests" was omitted from Title III affidavit, because if the information had been included in the affidavit it would not have diminished probable cause. U.S. v. Lucht, 18 F.3d 541 (8th Cir. 1994).

Magistrate judges in the Southern District of New York were authorized under 18 U.S.C. 3123 to issue orders for "the installation and use" of pen registers at DEA headquarters in the Southern District of New York to monitor telephones located in New Jersey. U.S. v. Rodriguez, 968 F.2d 130 (2d Cir. 1992); U.S. v. Burford, 755 F. Supp. 607 (S.D.N.Y. 1991) (District Court in the Southern District of New York had jurisdiction to issue order authorizing installation and use of pen register device "installed and used" at DEA headquarters in New York, even though the telephones being monitored were located in Maryland).

Information obtained from pen register can be used as evidence in criminal trial even though the court order authorizing its installation does not comply with statutory requirements. Statute (3121-3127) does not provide for exclusion. Suppression not warranted in the absence of a constitutional violation. U.S. v. Thompson, 936 F.2d 1249 (11th Cir. 1991); U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995).

No suppression where government's inclusion in Title III affidavit of unauthorized pen register information collected during three day period between expiration and renewal of pen register order was not material. U.S. v. Ishola, 1996 WL 197461 (N.D. Ill. 4/19/96).

Judicial review in connection with pen register and trap and trace requests is not so narrowly limited and essentially ministerial as to subject the courts to discretion of the Executive in violation of the constitutional separation of powers. U.S. v. Hallmark, 911 F.2d 399 (10th Cir. 1990).

"The judicial role in approving use of trap and trace devices is ministerial in nature . . . ." U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995) (citing Hallmark).

The court must issue a pen register order on the mere statutory certification of the applicant that the information sought is relevant to an ongoing criminal investigation. In re Application of U.S. for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device, 846 F. Supp. 1555 (M.D. Fla. 1994); U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995).

As long as the statutory prerequisites are met, there is no limitation on the number of times a pen register order may be extended. In re Application of U.S. for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device, 846 F. Supp. 1555 (M.D. Fla. 1994) (citing and concurring in the opinion of United States District Judge Ralph W. Nimmons, Jr. (M.D. Fla., Nov. 17, 1993) (NO. 93-15-MISC-T-21)).

"We believe that the caller identification service is a "trap and trace device" as that term is defined in 18 U.S.C. s 3127(4)." U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995).

The caller ID display unit itself is not a trap and trace device. The trap and trace is performed by the service provider’s signaling equipment and software necessary to use the Caller ID display device. Sparshott v. Feld Entertainment, Inc., 311 F.3d 425 (D.C. Cir. 2002).

Defendant argued that the Omaha Police Department did not properly obtain enhanced caller identification services under a pen register/trap and trace order issued by the state court because a warrant or subpoena was not obtained pursuant to the requirements of 18 U.S.C. 2703 for access to the subscriber names that are supplied with enhanced caller ID services. The federal judge, however, found that the affidavits submitted to the state magistrate (pen register/caller ID application) and to the state court judge (wiretap application) were sufficient to make the showing (relevance and materiality to an ongoing criminal investigation) required by 2703(d) and therefore the judges’ orders effectively authorized the use of enhanced caller identification services. U.S. v. Escarcega, 2000 U.S. Dist. LEXIS 10643 (D. Neb.).

"[W]e are not persuaded to hold that every device used in a criminal investigation which is not specifically authorized by statute is prohibited . . . ." U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995).

The Caller ID subscriber is the "user" referred to in section 3121(b)(3). By purchasing the Caller ID service, the subscriber consents to the trap and trace. Ohio Domestic Violence Network v. Public Utilities Commission of Ohio, 638 N.E.2d 1012 (Ohio 9/21/94). See also Wisconsin Professional Police Association v. Public Service Commission of Wisconsin, 555 N.W.2d 179 (Wis. Ct. App. 1996); Southern Bell Tel. & Tel. Co. v. Hamm, 409 S.E.2d 775 (S.C. 1991) (similar South Carolina state law)).

Police Department's use of "clone pagers" to intercept numeric transmissions to suspect's digital display pagers pursuant to state court "pen register" order cannot be considered the use of a "pen register" within the meaning of the ECPA, but was an unauthorized interception of electronic communications under 18 U.S.C. 2511. Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995).

Cell Site Simulator

A cell site simulator (CSS) electronically "forces" a cellular telephone to autonomously register its MIN and ESN when the target telephone is turned on but is not being used.

The Legal Authorities Required to Locate Cellular Telephones

(The following analysis was prepared by attorney Richard W. Downing of the Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice.)

I. Compelling Providers to Disclose Cell-phone Location Records

In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone. Depending on the number of towers in a particular area and other factors, this information may be used to identify the location of a phone to within a few hundred yards. Some providers routinely update this information at all times that the cell phone is turned on; others update it only when the user places a call. Carriers generally keep detailed historical records of this information for billing and other business purposes. At times, law enforcement authorities seek to compel carriers to preserve that information prospectively for use in a criminal investigation.

A. Obtaining Historical Records from Cellular Providers

Law enforcement investigators may use a search warrant or an order under section 2703(d) of title 18 in order to obtain historical records from cellular carriers. Section 2703(c)(1) provides:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity
>
> > (A) obtains a warrant issued using the procedures described in the Federal Rules of criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
> >
> > (B) obtains a court order for such disclosure under subsection (d) of this section;
> > ....

18 U.S.C. 2703(c)(1).

It remains doubtful whether law enforcement authorities may use a subpoena to obtain this same information. The amendments to section 2703(c) enacted in the USA PATRIOT Act of 2001 (the "USA PATRIOT Act") broadened the scope of records that may be obtained using a subpoena. In section 2703(c), the Act changed "local and long distance telephone toll billing records" to "local and long distance telephone *connection* records, *or records of session times and*

durations." The legislative history does not comment on the intent of this change nor did this topic arise in any of the negotiations surrounding the passage of the Act. There is no evidence, however, that Congress expanded the scope of this definition in order to include cell phone location information. Thus, although there are arguments on both sides, the better practice is to use 2703(d) orders and search warrants – rather than subpoenas – to obtain cell phone location information from providers.

B. Compelling Providers to Collect Cell Phone Location Information Prospectively

In order to require a provider to collect cell-phone location information prospectively (e.g., for the following 60 days), law enforcement authorities must obtain a court order. One possibility is an order under section 3123, the Pen Register and Trap and Trace Statute ("Pen/Trap Statute"). The USA PATRIOT Act amended the definitions of "pen register" and "trap and trace device" to include any device or process that collects the "dialing, routing, addressing, and signaling information" associated with a communication. Although no legislative history directly addresses whether "signaling" includes such information as the nearest cell tower, the face used by that cell tower, and the signal strength, a House Judiciary Committee Report on a preceding bill (commenting on language identical to that eventually enacted in the USA PATRIOT Act) suggests that the pen/trap statute governs such information. It states:

> This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media*.

H.R. Rept. 107-236, 107th Cong., 1st Sess. 53 (2001) (Rept. to Accompany H.R. 2975) ("House Report") (emphasis supplied). For a more in-depth discussion of this idea, see *infra* Section II.B.

Even if the pen/trap statute's amended definitions include such information, however, it remains doubtful that this non-specific language overrules the previously existing prohibition on carriers providing location information in response to a pen/trap order. In 1994, Congress explicitly prohibited providers from providing cell phone location information in response to a pen/trap order:

> (a) ... a telecommunications carrier shall ensure that its equipment, facility or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of –
>
> ...
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier–
>
> ...
>
> *except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber* (except to the extent that the location may be determined from the telephone number)....

Public Law 103-414, sec. 103(a) (1994) ("CALEA") (emphasis supplied). A court is likely to find that this clear expression of Congressional intent, which makes explicit reference to the

definitions of pen registers and trap and trace devices, continues to prohibit providers from supplying cell phone location information in response to a pen/trap order.

Because of the 1994 prohibition, law enforcement authorities have sought other means to compel providers to supply this information prospectively. Most commonly, investigators have used orders under section 2703(d) to obtain this information. Although section 2703(d) generally applies only to stored communications, nothing in that section requires that the provider possess the records at the time the order is executed. Moreover, use of such an order does not improperly evade the intent of the CALEA prohibition. Section 2703(d) court orders provide greater privacy protection and accountability than pen/trap orders by requiring (1) a greater factual showing by law enforcement and (2) an independent review of the facts by a court. Indeed, the very language of the CALEA prohibition – limiting its application "to information acquired *solely* pursuant to the authority for pen registers and trap and trace devices" – indicates that Congress intended that the government be able to obtain this information using some other legal process. Public Law 103-414, sec. 103(a) (emphasis supplied). Thus, 2703(d) orders are an appropriate tool to compel a provider to collect cell phone location information prospectively.

Finally, some have suggested that such orders should rely on the Mobile Tracking Devices statute, 18 U.S.C. § 3117. Although making reference to this statute would not be harmful, it does not provide much legal support for such an order. The statute refers to the "installation" of a "mobile tracking device." This language probably would apply to the provider's use of a software program to track the location of a particular cell phone, even though such a program is not literally a physical "device."

More importantly, however, the language of section 3117 assumes that the court has authority from some other source to order the installation of the device. Section 3117 only gives the court authority to authorize the use of such a device outside of the court's jurisdiction. This added benefit will rarely be an issue where a court issues a 2703(d) order for the collection of cell phone location information by a provider, since amendments in the USA PATRIOT Act assure that 2703(d) orders have nationwide effect. Moreover, a provider may well be able to execute such an order at one central point and not require the "use" of the device outside of the court's jurisdiction.

II. Collection of Cell Phone Location Information Directly by Law Enforcement

Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cellular phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.

In order to use such a device the investigator generally must know the target phone's telephone number (also known as a Mobile Identification Number or MIN). After the operator enters this information into the tracking device, it scans the surrounding airwaves. When the user of that phone places or receives a call, the phone transmits its unique identifying information to the provider's local cell tower. The provider's system then automatically assigns the phone a particular frequency and transmits other information that will allow the phone properly to transmit the user's voice to the cell tower. By gathering this information, the tracking device determines which call (out of the potentially thousands of nearby users) on which to home in. While the user remains on the phone, the tracking device can then register the direction and signal strength (and therefore the approximate distance) of the target phone.

A. Use of Law Enforcement Cell Phone Tracking Devices Prior to the USA Patriot Act of 2001

In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information "traditionally" collected using a pen/trap device. This analysis concluded that the "signaling information" automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the "contents" of a communication. Moreover, the analysis reasoned – prior to the 2001 amendments – that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of "pen register" and "trap and trace device." Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.

B. The Pen/Trap Statute, As Amended By The USA Patriot Act of 2001

Although the analysis remains unchanged with respect to the Fourth Amendment and the wiretap statute, substantial amendments to the definitions of "pen register" and "trap and trace device" in the USA PATRIOT Act alter the applicability of the pen/trap statute. The new definitions, on their face, strongly suggest that the statute now governs the use of such devices. Where the old definition of "pen register" applied only to "numbers dialed or otherwise transmitted," "pen register" now means

> a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted....

18 U.S.C. § 3127(3). "Signaling information" is a broader term that encompasses other kinds of non-content information used by a communication system to process communications. This definition appears to encompass all of the non-content information passed between a cell phone and the provider's tower.

Similarly, the USA PATRIOT Act broadened the definition of "trap and trace device." Where before the definition included only "the originating number of an instrument or device," the new definition covers "the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication...." 18 U.S.C. § 3127(4). Like the definition of "pen register," this broader definition appears to include such information as the transmission of a MIN, which identifies the source of a communication.

Moreover, the scant legislative history that accompanied passage of the Act suggests Congress intended that the new definitions apply to all communications media, instead of focusing solely on traditional telephone calls. Although the House Report cannot definitively state the intent of both houses of Congress when passing the final bill, it does strongly suggest that Congress intended that the statute would apply to all technologies:

> This section updates the language of the statute to clarify that the pen/register [sic] authority applies to modern communication technologies. Current statutory references to the target "line," for example, are revised to encompass a "line or other facility." Such a facility includes: *a cellular telephone number*; *a specific cellular telephone identified by its electronic serial number (ESN)*; an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)(C) allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced using any of these or other identifiers.

> Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain *any* non-content information – "dialing, routing, addressing, and signaling information" – utilized in the processing and transmitting of wire or electronic communications....
>
> This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media* ... ([and includes] packets that merely request a telnet connection in the Internet context).

H.R. Rept 107-236, at 52-53 (emphasis added). Indeed, this last reference to a packet requesting a telnet session – a piece of information passing between machines in order to establish a communication session for the human user – provides a close analogy to the information passing between a cell phone and the nearest tower in the initial stages of a cell phone call.

Finally, the House Report recognizes that pen registers and trap and trace devices could include devices that collect information remotely. The Report states:

> Further, *because the pen register or trap and trace 'device' is often incapable of being physically 'attached' to the target facility due to the nature of modern communication technology*, section 101 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the section allows the pen register or trap and trace device to be 'attached or applied' to the target facility [such as an ESN]. Likewise, the definitions of 'pen register' and 'trap and trace device' in section 3127 are revised to include an intangible 'process' (such as a software routine) which collects the same information as a physical device.

H.R. Rept 107-236, at 53 (emphasis added). Thus, the statutory text and legislative history strongly suggest that the pen/trap statute governs the collection of cell phone location information directly by law enforcement authorities.

C. The Inapplicability of CALEA's Prohibition on Collection Using Pen/Trap Authority

In passing CALEA in 1994, Congress required providers to isolate and provide to the government certain information relating to telephone communications. At the same time that it created these obligations, it created an exception: carriers shall not provide law enforcement with "any information that may disclose the physical location of the subscriber" in response to a pen/trap order. (A fuller quotation of the language appears, above, in Section I.B.). By its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones.

D. Conclusion

The amended text of the pen/trap statute and the limited legislative history accompanying the 2001 amendments strongly suggest that the non-content information that passes between a cellular phone and the provider's tower falls into the definition of "dialing, routing, addressing, and signaling information" for purposes of the definitions of "pen register" and "trap and trace device." A pen/trap authorization is therefore the safest method of allowing law enforcement to collect such transmissions directly using its own devices.

Cases Re: Cell-Site Data

DEA's capture of defendant's cell-site data did not violate the defendant's Fourth Amendment or Title III rights. Assuming without deciding that cell-site data fits within the definition of "electronic communication," the Court points out that suppression is not a permissible statutory remedy under Title III for the illegal interception of an electronic communication. 18 U.S.C. 2510(1)(c). (The Court finds that a strong argument exists that cell-site data is not a form of communication at all, in that it is not a message and it is not exchanged between individuals, but is just data sent from a cellular phone tower to the provider's computers.) Under the rationale of U.S. v. Knotts, 460 U.S. 276 (1983), the defendant has no legitimate expectation of privacy in the cell-site data because a person has no reasonable expectation of privacy regarding his travel on public thoroughfares, and the surveillance agents could have obtained the same information by following the defendant's car on the public highways. DEA simply used the cell-site data to "augment" sensory faculties, which is permissible under Knotts. Defendant's argument that DEA's use of the defendant's cell-site data effectively turned his cell phone into a tracking device within the meaning of 18 U.S.C. 3117, undermines the defendant's contention that suppression is appropriate under Title III. The definition of "electronic communication," 18 U.S.C. 2510(12)(C), excludes "any communication from a tracking device (as defined in section 3117 of this Title)" and thereby removes such tracking device communications from Title III coverage. Assuming, moreover, that the defendant is correct in his assertion that his phone was used as a tracking device, § 3117 does not provide a suppression remedy. See U.S. v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000), where the court observed that, in contrast to other statutes governing electronic surveillance, § 3117 "does not *prohibit* the use of a tracking device in the absence of conformity with the section.... Nor does it bar the use of evidence acquired without a section 3117 order." (Emphasis in original.) The Court finds Gbemisola to be persuasive and likewise concludes that § 3117 does not provide a basis for suppressing the cell-site data. Defendant attempted to distinguish his case from Smith v. Maryland, 442 U.S. 735 (1979) in that he did not voluntarily convey his cell-site data to anyone, and did not in fact use his cell phone. The agent dialed defendant's cell phone and the dialing caused the phone to send signals to the nearest cell tower. The Court, however, finds that the distinction between the cell-site data and the defendant's location is not legally significant under the particular facts of this case. The cell-site data is simply a proxy for the defendant's visually observable location as to which the defendant has no legitimate expectation of privacy. The Supreme Court's decision in Knotts is controlling. The DEA agents did not conduct a search within the meaning of the Fourth Amendment when they obtained the defendant's cell-site data. U.S. v. Forest, 355 F.3d 942 (6th Cir. 2004).

Two magistrate judges have recently issued opinions rejecting use of the pen/trap statute and 2703 in applications seeking court orders for prospective acquisition of cell-site information. See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 2005 WL 2656621 (S.D. Tex. Oct. 14, 2005); In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 2005 WL 2739208 (E.D.N.Y. Oct. 24, 2005). The government maintains that the magistrate judges are wrong to assert that cell-site information is not "dialing, routing, addressing, or signaling information" under the Pen/Trap Statute. They are wrong to assert that cell-site information is not "a record or other information pertaining to a subscriber or customer" of an electronic communication service provider under ECPA. They are wrong to assert that the tracking device statute, 18 U.S.C. § 3117, requires a warrant based on probable cause to compel disclosure of cell-site information. They are wrong to assert that cell-phone users have a reasonable expectation of privacy in cell-site information.

Wire or Electronic Communications in Storage and Transactional Records Access

Stored Wire and Electronic Communications (Contents)

18 U.S.C. 2703(a) permits a governmental entity to obtain the contents of wire or electronic communications that are in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal procedure by a court with jurisdiction over the offense under investigation (single warrant effective nationwide) or equivalent State warrant. The contents of communications in storage for longer than 180 days may be obtained by any of the means available under 18 U.S.C. 2703(b).

2703(b) permits a governmental entity to gain access to wire or electronic communications held or maintained by a remote computing service without required notice to the subscriber or customer if a warrant issued using the procedures described in the Federal Rules of Criminal procedure by a court with jurisdiction over the offense under investigation (single warrant effective nationwide) or equivalent State warrant is used, and with prior notice if a Federal or State administrative, grand jury or trial subpoena is used, or a court order under 18 U.S.C. 2703(d) is used, except that delayed notice may be given pursuant to section 2705. The provisions of 2703(b) are applicable to any wire or electronic communication held or maintained by the remote computing service on behalf of, and received by means of electronic transmission from a subscriber or customer of such remote computing service; and solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(If the remote computing service has uncontrolled access to the contents of the electronic communications, it should be treated as any other third party record custodian.)

Section 2703(f)requires that a service provider or remote computing service, upon the request of a governmental entity, shall preserve records, and other evidence in its possession pending the issuance of a court order or other process.

Police officer making record retention request under 2703(f)(1) need not limit the request to a certain number of days. U.S. v. Bach, 2001 WL 1690055 (D. Minn.).

Subscriber Information (Transactional Records)

18 U.S.C. 2703(c)(1) states that a provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal procedure by a court with jurisdiction over the offense under investigation (single warrant effective nationwide) or equivalent State warrant; obtains a court order pursuant to 18 U.S.C. 2703(d)(see below); or

has the consent of the subscriber or customer. Notice to the customer or subscriber is not required.

In early 1992, narcotics officers of the Omaha, Nebraska, Police Department obtained authority from a state court to install pen registers for 60 days on telephone lines. The state court also authorized the telephone company to supply subscriber information and caller identification service for the phones to which the pen registers were attached. The Court said that "[w]ith respect to the subscriber information, this information does not satisfy the definition of a pen register, trap and trace device, or a wiretap . . . ." Citing Smith v. Maryland, 442 U.S. 735 (1979), and without mentioning 18 U.S.C. 2703(c), the Court held that "acquisition and use of the subscriber information did not violate federal law." U.S. v. Fregoso, 60 F.3d 1314 (8th Cir. 1995).

Emergency Need for Telecommunications Records or Contents

During the government's investigation of a kidnapping for ransom, a telecommunications service provider provided records to the government without a court order. The government's application for a nunc pro tunc 2703(d) order retroactively authorizing the disclosure of the records to the government was denied because there is no provision for the issuance of such an order, and furthermore, such an order would not provide the immunity set forth in 18 U.S.C. 2703(e) because the disclosure when made was not authorized by a court order. However, a kidnapping for ransom is the type of emergency situation which involves "immediate danger of death or serious physical injury to a person. . ." Thus, a provider who discloses records or other information pursuant to the statutory authorization in 18 U.S.C. 2702(c)(4) (added by the Patriot Act of 2001) in emergency circumstances has the same protection from lawsuits as a provider who discloses the records pursuant to a court order. The Homeland Security Act of 2002 added an authorization (18 U.S.C. 2702(b)(8)) to disclose the contents of telecommunications in the same circumstances. In the Matter of the Application of the United States for a Nunc Pro Tunc Order for Disclosure of Telecommunications Records, 352 F. Supp.2d 45 (D. Mass. 2005).

2701, 2703 (c) and (d)

Under 18 U.S.C. 2703(c)(2), the government may obtain by Federal or State administrative, grand jury or trial subpoena (as well as the means available under 2703(c)(1)(see above)), the subscriber or customer's name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number).

To obtain more than this limited information, the government must use a 2703(d) court order, a search warrant, or have the consent of the subscriber or customer. To obtain a 2703(d) order the government must offer specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation. See U.S. v. Kennedy, 81 F. Supp.2d 1103 (D. Kan. 2000).

FTC'S pre-trial discovery subpoena pursuant to FRCP 45 seeking Netscape subscriber information relating to two e-mail addresses does not constitute a "trial subpoena" as contemplated by 2703(c)(1)(C)[now 2703(c)(2)]. Federal Trade Commission v. Netscape Communications Corp., 2000 WL 1277641 (N.D. Cal.).

There is no violation of 2701 or 2703(a),(b), or (c) if access is pursuant to a warrant. Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

18 U.S.C. 2701 does not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor does it proscribe authorized access for unauthorized or illegitimate purposes. International Association of Machinists and Aerospace Workers v. Werner-Masuda, et al. 390 F. Supp.2d 479 (D. Md. 2005).

"Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances. [18 U.S.C. 2701(c)(1)] therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access." Because defendants used a subpoena that "transparently and egregiously violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it (subpoena ordered all copies of e-mails sent or received by anyone, with no limitation as to time or scope)," they are charged with knowledge of its invalidity. The subpoena was "deceptive. . . a piece of paper masquerading as legal process . . . The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused." Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

A St. Paul, Minnesota Police officer faxed a state search warrant to Yahoo! Inc. for execution by Yahoo employees in California. The police officer was not present and acting in the execution of the warrant when the Yahoo employees searched and seized information from the defendant's Yahoo account. The police officer's presence was required by Minnesota statutes, but this is a federal case and therefore state law violations do not warrant suppression so long as the search complied with the Fourth Amendment. The federal statute (18 U.S.C. 3105) requiring the executing officer to be present when civilians aid in the execution of the search warrant applies only to federal officials. Inquiries under Section 3105 and the Constitution are separate and distinct. Congress intended to create a statutory expectation of privacy in e-mail files, but it is less clear that an analogous expectation of privacy derives from the Constitution. The court declines to decide whether there is a constitutional expectation of privacy in e-mail files, but does find that Yahoo!'s execution of the search warrant in this case did not violate the defendant's Fourth Amendment rights. The Fourth Amendment does not explicitly require official presence during a warrant's execution, therefore it is not an automatic violation if no officer is present during a search. The Fourth Amendment is governed by a "reasonableness" standard. Official presence should simply be one of many factors considered in determining the reasonableness of the execution of a search warrant. Civilian searches are sometimes more reasonable than searches by officers. The court considers several factors in this case to determine whether the search and seizure of the defendant's e-mail from Yahoo!'s server by Yahoo! technicians violated the defendant's Fourth Amendment rights, including the fact that no warrant was physically "served," no persons or premises were searched in the traditional sense, and there was no confrontation between Yahoo! technicians and the defendant. Other factors crucial to the court's decision include: (1) the actual physical presence of an officer would not have aided the search (in fact may have hindered it); (2) the technical expertise of Yahoo!'s technicians far outweighs that of the officers; (3) the items "seized" were located on Yahoo!'s property; (4) there was a warrant signed by a judge authorizing the search; and (5) the officers complied with the provisions of 18 U.S.C. § 2701. All of these factors weigh in favor of the government and the court therefore finds that the search was constitutional under the Fourth Amendment's reasonableness standard. U.S. v. Bach, 310 F.3d 1063 (8th Cir. 2002).

Section 2709 National Security Letters

"The Court concludes that compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violates the Fourth Amendment, and that the non-disclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment. The Government is therefore enjoined from issuing NSLs [national security letters] under § 2709 or from enforcing the non-disclosure provision in this or any other case, but enforcement of the Court's judgment will be stayed pending appeal, or if no appeal is filed, for 90 days." Doe v. Ashcroft, 334 F. Supp.2d 471 (S.D.N.Y 2004). See also, Doe v. Gonzales, 386 F. Supp.2d 66 (D. Conn. 2005).

Reimbursement of Service Provider for Reasonable Costs

Other than the regulations promulgated to facilitate the government's reimbursement of service providers for CALEA compliance, no regulations have been issued concerning the government's payment of reasonable costs incurred by service providers responding to information and assistance requests under 18 U.S.C. 2518(4), 2706, 3124(c) or 3125(d).

Under 18 U.S.C. 2706, the telephone company did not "maintain" terminating automated message accounting (AMA) reports of calls received by a particular customer, within meaning of exemption in 18 U.S.C. 2706(c) for information maintained by telephone company that relates to toll records and telephone listings; provision of Act requiring governmental entities to pay for information demanded from telephone companies applied to state and local governments as well as federal government; and provision did not exceed Congeress' authority under Commerce Clause. Ameritech Corporation v. McCann, 403 F.3d 908 (7th Cir. 2005). See also Michigan Bell Telephone Co. v. Drug Enforcement Admin., 693 F. Supp. 542 (E.D. Mich 1988)(dealing with allegedly excessive aggregate level of requests by DEA).

Civil Liability of Governmental Entity

(Pre-Patriot Act)

In a civil action pursuant to 18 U.S.C. 2707 the plaintiff alleged that the City of Durham, through its police officers, violated 18 U.S.C. 2703(c) when the officers obtained subscriber information regarding her telephone service through the use of two improper subpoenas. The Fourth Circuit held that 18 U.S.C. 2707 authorizes a private cause of action against governmental entities that violate the ECPA, but the language of 18 U.S.C. 2703(c) only limits the circumstances under which service providers may disclose subscriber information and does not prohibit any governmental conduct. Thus, a governmental entity may not violate that subsection by simply accessing information improperly. The absence of language in 2703(c) "limiting the access of customer information by governmental entities indicates that Congress did not intend to authorize civil suits against governmental entities for improperly obtaining customer records." The Court notes further that the distinction between limiting access and limiting disclosure is apparent within section 2703 itself where sections (a) and (b) do focus on the conduct of governmental entities by providing that "a governmental entity may require the disclosure by a provider . . ." thereby making them civilly liable for violations of section (a) or (b). Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996); Guest v. Leis, 255 F.3d 325 (6th Cir. 2001)(citing Tucker). See also U.S. v. Charles, 1998 WL 204696 (D. Mass.)(also holding that violation of 2703 is nonconstitutional in magnitude and the only remedies for such violations are described in chapter 121 of Title 18).

(Post-Patriot Act)

On October 26, 2001, the USA Patriot Act "amended the ECPA and removed this textual distinction [see paragraph above]. Now, §§ (a) (b), and (c) all begin with identical language focusing on government conduct, providing that '[a] governmental entity may require . . .' 18 U.S.C. § 2703 (a)-(c). Therefore, Tucker does not foreclose government liability under § 2703(c), and in fact supports the conclusion that the government can be liable under the present text of § 2703(c). To conclude that the government may circumvent the legal processes set forth in the ECPA by merely requesting subscriber information from an ISP contradicts Congress's intent to protect personal privacy. In light of legal precedent, the framework of the statute, and the legislative intent, governmental entities can be liable under § 2703(c) for soliciting information from an ISP without complying with the legal processes specified in the statute." Freedman v. America Online, Inc., 303 F. Supp.2d 121 (D. Conn. 2004).

Internet Related Cases

Federal District Judge Sporkin thinks it unlikely that the Tucker v. Waddell (see above) analysis of 2703(c) liability would prevail where a Navy investigator, at the least, "solicited a violation of the ECPA by AOL" when the Navy investigator obtained plaintiff's subscriber information from AOL without a court order or subpoena and did not identify himself. McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

Internet service provider MindSpring supplied a police officer with defendant's name, address, credit card number, e-mail address, home and work telephone numbers, fax number, and the fact that the Defendant's account was connected to the Internet using a specific Internet Protocol (IP) address. At the hearing on the defendant's motion to suppress, the government conceded the invalidity of the New Hampshire state subpoena used to obtain the information from the defendant's ISP, Mindspring, located in Atlanta, Georgia. The question before the court was whether the court must suppress the information obtained from MindSpring, and all that flowed from it, because the government failed to obtain a proper subpoena. Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA does not represent a legislative determination of a reasonable expectation of privacy in non-content information released by ISPs. The ECPA does not even provide for the relief requested in this case (suppression). Section 2707 provides a civil remedy for aggrieved individuals and Section 2708 states that this is the only remedy for nonconstitutional violations of 18 U.S.C. 2701-2711. U.S. v. Hambrick, 2000 U.S. App. LEXIS 18665 (4th Cir) (unpublished); Freedman v. America Online, Inc., 2005 WL 1899381 (D. Conn.) (citing Hambrick).

Plaintiffs lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators. Guest v. Leis, 255 F.3d 325 (6th Cir. 2001)(citing Hambrick).

Section 2703(c)(1)(A) authorized AOL to disclose to a private individual the name of an AOL account holder. Jessup-Morgan v. America Online, Inc., 20 F. Supp.2d 1105 (E.D. Mich. 1998). See also Hill v. MCI Worldcom Communications, Inc., 2000 WL 1759605 (S.D. Iowa)(citing Jessup-Morgan).

The ECPA does not recognize a cause of action for aiding and abetting a primary violator, and the Act does not create any secondary liability on the part of the service provider. Motise v. America Online, Inc., 2005 WL 1667658 (E.D. Va..).

Under the Digital Millennium Copyright Act (17 U.S.C. 512(h)), a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity, not to an ISP acting only as a conduit for data transferred between two Internet users. Recording Industry Ass'n of America, Inc. v. Verizon, 351 F.3d 1229 (C.A. D.C. 2003); In re: Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005).

The United States Air Force, without a warrant or a court order, obtained from an ISP, electronic data stored by the ISP in the form of a log identifying the date, time, user, and detailed internet address of sites accessed by the appellant over several months. The U.S. Court of Appeals for the Armed Forces determined that, under the provisions of 18 U.S.C. 2703(c), the ISP's release of such information to the government does not require a warrant (no contents of communications) and may be released upon a court order issued under 2703(d). Although neither a warrant or order was obtained, there is no exclusionary rule relief under 2703. The court did not reach the constitutional issue of whether the type of information released in the instant case enjoys Fourth Amendment protection, because it agreed with the lower court that a warrant would have inevitably been obtained for these records. The court did state the information at issue lies somewhere between the type of subscriber information at issue in U.S. v. Hambrick, 2000 U.S. App. LEXIS 18665 (4th Cir.) (unpublished) (subscriber has no reasonable expectation of privacy in name, address, credit card number, and telephone number provided to the ISP and its employees) and U.S. v. Maxwell, 45 MJ 406 (1996) (limited expectation of privacy in e-mail messages sent or received through an ISP). The government agent asked the ISP if it needed a warrant and was informed by the ISP that corporate counsel advised management that no warrant was needed. The government acted in complete good faith in relying on the ISP's assertions that the ISP could release the records without a warrant. There was no seizure which could be said to be the result of a constitutional violation of such import as to bring into play any exclusionary rule. U.S. v. Allen, 2000 CAAF LEXIS 921.

Marine corporal whose e-mails sent and received over a Government computer network were seized with the aid of the network administrator (not pursuant to authorized system monitoring activity) acting solely at the behest of law enforcement officials, without a warrant, had a limited expectation of privacy in her e-mail communications via the Government network server. "Specifically, while the e-mails [of Marine corporal] may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a result of monitoring or when a search was conducted in accordance with the principles enunciated in the 4th Amendment. Under the circumstances presented in this case, the appellant had a subjective expectation of privacy in the e-mails sent and received on her Government computer vis-à-vis law enforcement and this expectation of privacy was reasonable." U.S. v. Long, 61 M.J. 539 (N.M.Ct.Crim.App. 2005) (citing O'Connor, Simons, Slanina (see "Workplace Search" chapter above), and Maxwell (see above)).

Internet site subscriber information not protected by Fourth Amendment. U.S. v. Ohnesorge, 60 M.J. 946 (2005) (citing Maxwell, Hambrick and Allen.)

In Steve Jackson Games v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), the Secret Service, in its pursuit of suspected "hackers," used a Rule 41 search warrant to seize computers, disks and other materials, including public and private e-mail and other documents stored on a computer bulletin board service. The court fined the Secret Service $50,000 for violating the

Privacy Protection Act by failing to return the "work product" of the plaintiff pertaining to a book it was about to publish. In addition, while the court found that the seizures were not "interceptions" within the contemplation of Title III (citing U.S. v. Turk, 526 F.2d 654 (5th Cir. 1976)), the court did find that the Secret Service had knowledge of the applicability of the stored wire and electronic communications provisions of Title 18. The court fined the Secret Service an additional $1,000 for each plaintiff for failing to apply the provisions of 18 U.S.C. 2703 (restrictions on government access to stored electronic communications). The court held that had the government based its search warrant on 18 U.S.C. 2703, the plaintiffs would have had the opportunity to contend, under 18 U.S.C. 2703(d), that the search was unduly burdensome. Finally, the court held that the government failed to utilize the provisions of 18 U.S.C. 2704 permitting the government to request that the service provider make back-up copies of the electronic communications being sought.

Affirming on appeal, the 5th Circuit held that the government's seizure of a computer on which is stored private e-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, is not an "intercept" proscribed by 18 U.S.C. 2511(1)(a) because, per the Court's interpretation of "intercept" in U.S. v. Turk, 526 F.2d 654 (5th Cir. 1976), the acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications. Steve Jackson Games, Incorporated v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

"We assume without deciding that an additional warrant in compliance with section 2703 would have been required for the law enforcement officials in the instant case to gain access to the contents of the seized e-mail." Section 2703 does not appear to address whether concomitant and incidental seizure of e-mail and software stored in computer hardware seized under warrant as instrumentality of crime of distribution of obscenity, standing alone, is a violation of the ECPA. Nevertheless, the officers qualified for the statutory good faith defense of section 2707(e) for reliance on the search warrant authorizing the seizure of the computer hardware. Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997).

Regarding AOL's assertion of a good faith defense under 2707(e), there is a genuine issue of fact as to the objective reasonableness of an AOL employee's subjective good faith belief that a warrant (unsigned by judge) was valid, and therefore the issue must be resolved at trial. Freedman v. America Online, Inc., 325 F. Supp.2d 638 (E.D. Va. 2004) (contains comprehensive discussion of "good faith defense" jurisprudence); Freedman v. America Online, Inc., 329 F. Supp.2d 745 (E.D. Va. 2004) (Defendant's motion for partial reconsideration denied).

A person's mere eligibility to use a website, without any findings of actual use, does not qualify that person, under the provisions 18 U.S.C. 2701(c)(2), as a "user" of the website's electronic communication service who can authorize a third party's access to the "user's" communications. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

An anonymous source used a Trojan Horse virus to hack into defendant's computer and download incriminating information from the defendant's hard-drive. The source e-mailed the evidence to law enforcement authorities. There was no Fourth Amendment violation because there was no state action and there was no violation of the ECPA because the source did not intercept electronic communications real-time and the defendant's computer was not a facility through which an electronic communication service is provided. Even if an "interception" had occurred in violation of the Wiretap Act, suppression is not a remedy under the Wiretap Act with respect to unlawfully seized electronic communications. U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003)(citing Konop and Steve Jackson Games).

The First Circuit held that Pharmatrak, Inc., a firm providing data collection software to various pharmaceutical internet sites, "intercepted," without the consent of its pharmaceutical client web sites, personal and identifying data of the pharmaceutical sites' web users. (This holding appears to be based on a misunderstanding of the technology of web browsers that caused the court to believe that Pharmatrak was wiretapping communications between web users and the pharmaceutical sites. In fact, the information collected by Pharmatrak was sent by the users' own browsers directly to Pharmatrak. The users' browsers were simply operating per the standard for HTTP code. When the users clicked on a link in the pharmaceutical webpage they communicated simultaneously with the pharmaceutical sites and with Pharmatrak and then both the pharmaceutical client's server and Pharmatrak's server contributed content for the succeeding webpage. The pharmaceutical sites had configured their systems so as to expose the users' data in the URLs of the sites' dynamically generated pages.) The case was remanded to determine if Pharmatrak's actions were "intentional" within the meaning of the ECPA. In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).

An individual Plaintiff's personal computer is not a "facility through which an electronic communication service is provided" for the purposes 18 U.S.C. 2701. The personal computers are analogous to telephones and televisions. They are necessary devices by which consumers access particular services such as telephone lines, cable television and the Internet. While it is possible for modern computers to perform server-like functions, there was no evidence that any of the Plaintiffs used their computers in this way. The relevant service is Internet access, and the service is provided through ISPs or other servers, not through Plaintiffs' PCs. In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp.2d 4 (D. Mass. 2002)(citing DoubleClick, 154 F. Supp.2d 497 (S.D.N.Y. 2001)). But see Chance v. Avenue A, Inc., 165 F. Supp.2d 1153 (W.D. Wash. 2001)(the court considered it a "strained interpretation," but possible to conclude that modern computers, which serve as conduits for web servers' communications, are "facilities" under 18 U.S.C. 2701).

ECPA and Cable Communications Policy Act Regarding Notice to Customers

The USA Patriot Act amends Title 47, section 551(c)(2)(D), to clarify that the ECPA and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services –- such as telephone and internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programming a customer chooses to purchase.

Violations of Title III

Constitutionality of 2511 as Applied to the Media

Notwithstanding the prohibition of 18 U.S.C. 2511(1)(c), the First Amendment protects the knowing disclosure of illegally intercepted communications if the person making the disclosure played no part in the illegal interception, lawfully obtained access to the communications, and the communications deal with a matter of public concern. Bartnicki v. Vopper, 121 S. Ct. 1753 (2001).

Mens Rea for Illegal Interception, Disclosure or Use

The ECPA changed the mens rea required for violations from "willful" to "intentional." This modification served to "underscore that inadvertent interceptions are not crimes under the Electronic Communications Privacy Act." S. Rep. No. 541, 99th Cong., 2d Sess. 23, reprinted in 1986 U.S. Code Cong. & Admin. News 3555, 3577. Sanders v. Robert Bosch Corporation, 38 F.3d 736 (4th Cir. 1994); Abraham v. County of Greenville, South Carolina, 237 F.3d 386 (4th Cir. 2001); Thompson v. Dulaney, 970 F.2d 744 (10th Cir. 1992); In re Pharmatrak, Inc. Privacy Litigation, 292 F. Supp.2d 263 (D. Mass. 2003); Bess v. Bess, 929 F.2d 1332 (8th Cir. 1991); Tapley v. Collins, 41 F. Supp.2d 1366 (S.D. Ga. 1999) (violation occurred when defendant knew what was being intercepted and continued listening to it); Anderson v. City of Columbus, Georgia, 374 F. Supp.2d 1240 (M.D. Ga 2005)(distinguishing Sanders).

A criminal violation of the federal wiretap statute only requires proof of general intent. Oliver v. WFAA-TV, Inc, 1998 U.S. Dist. LEXIS 21532 (N. D. Tex.); Peavy v. Harman, 37 F. Supp.2d 495 (N.D. Tex. 1999).

Initial intercept by hotel operator or clerk was not "willful" (pre-ECPA mens rea), and continued eavesdropping when distress or possible crime was overheard was not intended by Congress to be unlawful. U.S. v. Savage, 564 F.2d 728 (5th Cir. 1977); Adams v. Sumner, 39 F.3d 933 (9th Cir. 1994).

Switchboard operator's exception (2511(2)(a)(i)) is limited only to that moment or so during which the operator must listen to be sure the call is placed. Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).

Conviction for violation of 2511(1)(a) affirmed, but court suggests a better jury instruction defining "intentionally." U.S. v. Townsend, 987 F.2d 927 (2d Cir. 1993).

For Title III purposes, "[t]he word 'intentional' describes the mental attitude associated with an act that is being done on purpose." The amendment's legislative history indicates that whether or not defendant believed her actions to be blameless, on advice of counsel or otherwise, is irrelevant to the question of whether she "intentionally" intercepted and disclosed the conversations. The plaintiffs need only show that defendant acted "on purpose," that is, with the intent of listening to and disclosing their telephone calls. Sheinbrot, M.D. v. Pfeffer, M.D., 1995 WL 432608 (E.D.N.Y. 7/12/95).

The word "intentional" refers to an act that is being done on purpose. First v. Stark County Board of Commissioners, 2000 WL 1478389 (6th Cir. 10/4/00)(unpublished).

The ECPA legislative history pertaining to 18 U.S.C. 2511 "makes clear that a mistake of law or ignorance of the law is no longer a defense under Title III." Young v. Young, 1995 WL 361706 (Mich. App.).

There is no "ignorance of law" defense to violation of 18 U.S.C. 2511(1). Tapley v. Collins, 41 F. Supp.2d 1366 (S.D. Ga. 1999).
U.S. v. Dossey, 2003 U.S. App. LEXIS 6892 (6th Cir.) (unpublished).

Defendant (divorce lawyer) accused of intentional use of illegally intercepted communications in violation of 2511(1)(d), cannot be convicted unless the government proves that he knew or had reason to know that the communications were obtained in violation of the Act. U.S. v. Wuliger, 981 F.2d 1497 (6th Cir. 1992); See also Weeks v. Union Camp Corporation, 2000 WL 727771 (4th Cir.)(unpublished)(citing Wuliger).

"Clearly under §2511(1)(d) a person may use the contents of a conversation which was not acquired through an intentional interception." Bayges v. Southeastern Pennsylvania Transportation Authority, 144 F.R.D. 269 (E.D. Pa. 1992) (inadvertent radio transmission of private conversation).

A person has not committed a disclosure or use violation under Title III unless he knew or had reason to know that the interception itself was in violation of Title III. Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993) (citing Wuliger and Thompson).

Plaintiffs failed to raise a fact issue with respect to the requisite knowledge of the defendant TV station of the tape's illegality sufficient to hold it liable for use or disclosure in violation of the federal wiretap statute. Mayes v. LIN Television of Texas, Inc., 1998 WL 665088 (N.D. Tex.).

Because the plaintiffs failed to allege that defendant Verizon had the requisite knowledge of illegality under 18 U.S.C. 2511(1)(c) and (d), they have not stated a claim on which relief can be granted. Fernicola v. Specific Real Property in Possession, 2001 WL 1658257 (S.D.N.Y.).

The government's jailhouse nonconsensual taping of a prisoner's "confession" to a priest was a violation of the Religious Freedom Restoration Act (RFRA) (held unconstitutional by Supreme Court on 6/25/97) and the Fourth Amendment. Since the taping was done in the ordinary course of duty of the law enforcement officer (jailor) (18 U.S.C. 2510(5)(a)), the mens rea required for a violation of 2511 was not present and therefore the prosecutor's retention of the intercepted confession was not a violation of 2511. This case was remanded for appropriate injunctive relief barring any future interception of confidential communications between a prisoner and a member of the clergy in the member's professional capacity. Mockaitis v. Harcleroad, 104 F.3d 1522 (9th Cir. 1997).

Violations of 2511

Use and disclosure proscriptions of 2511(1)(c) and (d) are not unconstitutionally vague and overbroad. Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000).

Congressman McDermott knowingly disclosed the contents of illegally intercepted communications in violation of 2511(1)(c). When McDermott received the illegally intercepted communications directly from the illegal interceptors, he had present knowledge of the illegality of such disclosure by the interceptors, and thus "unlawfully" obtained the information. Therefore, the Supreme Court's holding in Bartnicki does not provide a First Amendment shield for

Congressman McDermott's violation of 18 U.S.C. 2511. Although not necessary to a determination of the instant case, Judge Hogan chose to discuss the "duty of confidentiality" and its consequent limitation on First Amendment protection that might have been otherwise enjoyed by the federal judge in U.S. v. Aguilar, 515 U.S. 593 (1995) (judge disclosed wiretap information to the subject of the surveillance). Boehner v. McDermott, 332 F. Supp.2d 149 (D. D.C. 2004).

New and discrete cause of action for violation of 18 U.S.C. 2511(1)(c) accrues each time a recording of an unlawfully intercepted communication is played to a third party who has not yet heard it. Fultz v. Gilliam, 942 F.2d 396 (6th Cir. 1991);
Fields v. Atchison, Topeka, and Santa Fe Railway Company, 985 F. Supp. 1308 (D. Kan. 11/25/97).

Because contents of illegal interceptions had become part of the public record during divorce proceedings, additional disclosures in the course of ensuing litigation do not constitute separate violations of Title III. Lombardo v. Forbes, 192 F. Supp.2d 893 (N.D. Ind. 2002)(citing legislative history for 18 U.S.C. 2511(1)(c)and(d)).

Recording and disclosure are separate violations of 2511 for which plaintiff may receive damage awards under 2520(c). Bess v. Bess, 929 F.2d 1332 (8th Cir. 1991); Deal v. Spears, 780 F. Supp. 618 (W.D. Ark. 1991); Biton v. Menda, 812 F. Supp. 283 (D.P.R. 1993).

Neither the number of discrete violations of the Act committed by the "person or entity engaged in that violation" on any one day,
nor, in our view, the different types of violations committed on any one day (interception, or disclosure, or intentional use), are relevant in calculating the liquidated damages to be awarded under Section 2520(c)(2)(B). Desilets v. Wal-Mart Stores, Inc., 171 F.3d 711 (1st Cir. 1999).

The $10,000 in 2520(c)(2)(B)is designed to compensate a plaintiff for all of the transgressor's misdeeds under the wiretapping statute arising out of a closely related course of conduct that takes place over a relatively short period of time. Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999).

Listening to tape recording of known illegal interception constitutes illegal "use" under 2511(1)(d). Thompson v. Dulaney, 838 F. Supp. 1535 (D. Utah 1993).

Listening alone is insufficient, under 2511(1)(d), to impose liability for "using" illegally intercepted communications. Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999); Reynolds v. Spears, 93 F.3d 428 (8th Cir. 1996). Fields v. Atchison, Topeka, and Santa Fe Railway Company, 985 F. Supp. 1308 (D. Kan. 1997); Peavy v. Harman, 37 F. Supp.2d 495 (N.D. Tex. 1999).

Twenty-two hours of automatically recorded calls from telephone extension on line serving business and residence where business owner suspected employee of participation in burglary was not exempted under 2510(5)(a)(i) as use in the ordinary course of business. The recording device, not the extension phone, was the instrument used to intercept the calls and does not fall within the statutory exemption. The defendant disclosed enough of the "contents" of the taped conversations to incur liability under 2511(1)(c). No implied consent here. Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); Peavy v. Harman, 37 F. Supp.2d 495 (N.D. Tex. 1999); see also Sanders v. Robert Bosch Corporation, 38 F.3d 736 (4th Cir. 1994) (round-the-clock secret telephone monitoring to intercept bomb threats).

Summary judgment granted for wife in suit against husband for illegally intercepting her telephone calls. Husband had no "good faith" defense, the wife did not impliedly consent to the

interceptions and there were no parent conversations with a minor child on behalf of whom the husband could assert vicarious consent. Milke v. Milke, 2004 U.S. Dist. LEXIS 11199 (D. Minn.).

Qualified Immunity

Prosecutors are entitled only to qualified immunity for acts related to investigations or the giving of legal advice. Burns v. Reed, 500 U.S. 478 (1991).

Qualified immunity does not apply broadly to Title III claims because complete defense is provided in 2520(d). Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).

"The court concludes as a matter of law that a defendant is entitled to assert the defense of qualified immunity for an alleged violation of the Wiretap Act." Peavy v. Dallas Independent School District, 57 F. Supp.2d 382 (N.D. Tex. 1999).

"Congress did not intend to deprive public officials of their defense of qualified immunity when it enacted Title III." Blake v. Wright, 179 F.3d 1003 (6th Cir. 1999); Tapley v. Collins, 211 F.3d 1210 (11th Cir. 2000)(citing Blake); Conner v. Tate, 130 F. Supp.2d 1370 (N.D. Ga. 2001).

Although defendant police officer's interception of the cordless telephone communications of plaintiff during a drug investigation in 2000 violated federal law (cordless telephone exemption removed from Title III in 1994), the good faith defense in 18 U.S.C. 2520(d) excuses the defendant from liability because he relied in good faith on a Tennessee court order issued in accordance with state law, and he received verification of its propriety from a local assistant district attorney. Because the law regarding Fourth Amendment applicability to cordless telephone communications is not "clearly established" (neither the Supreme Court nor the Sixth Circuit has specifically addressed the issue), and because he was acting pursuant to a court order under state law, and with the endorsement of an assistant district attorney, the defendant has qualified immunity from liability if there was a Fourth Amendment violation. Frierson v. Goetz, 2004 U.S. App. LEXIS 10037 (6th Cir.) (unpublished).

No qualified immunity for chief of police who secretly taped a police line used for personal calls and which had been announced by the chief to be free from taping. Abbott v. The Village of Winthrop Harbor, 1998 U.S. Dist. LEXIS 11897 (N.D. Ill. 7/29/98).

Absolute Immunity

The prosecutor is absolutely immune for acts taken in preparing for the initiation of judicial proceedings or for trial, including the professional evaluation of evidence assembled by the police. Buckley v. Fitzsimmons, 509 U.S. 259 (1993).

Prosecutors have absolute immunity in their review of evidence in anticipation of prosecution. Whether the prosecutors are right or wrong in their evaluation of their right to use illegally recorded tape as evidence is of no moment. Davis v. Zirkelbach, 149 F.3d 614 (7th Cir. 1998).

Prosecutors have absolute immunity in turning over tape recordings in discovery pursuant to Rule 16 because such action is clearly related to a prosecutorial function. Lanier v. Bryant, 332 F.3d 999 (6th Cir. 2003).

Good Faith Reliance Defense [2520(d)]

Defendants who relied on attorney's advice were protected by "good faith reliance" defense under § 2520(d) even though cases upon which attorney relied were later overruled. Rice v. Rice, 951 F.2d 942 (8th Cir. 1991).

Government officials who are sued for alleged violations of the Constitution or of the Omnibus Crime Control and Safe Streets Act in the performance of their official duties may offer as an affirmative defense that they had reasonable grounds to believe their actions were legal and that there is no evidence that they acted in bad faith. Zweibon v. Mitchell, 606 F.2d 1172 (D.C. Cir. 1979).

In Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993), the court stated that "nothing in § 2520(d) supports a conclusion that the good faith defense applies where a defendant mistakenly believes that there exists a statutory authorization for the wiretapping. See Campiti, 611 F.2d at 394-95 (mistaken belief that statutory exceptions apply does not give rise to a good faith defense); see also Heggy v. Heggy, 944 F.2d 1537, 1542 (10th Cir. 1991) (§ 2520(d) does not embrace mistake of law); Ferrara v. Detroit Free Press, Inc., 1998 U.S. Dist. LEXIS 8635 (E.D. Mich.); Fultz v. Gilliam, 942 F.2d 396 (6th Cir. 1991) (ignorance of the law is not a defense under the federal wiretap law); Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000)(rejecting ignorance or mistake of law defense for disclosure or use in violation of 2511(1)(c) and (d)).

Defendant says that because she believed in good faith that her actions did not violate Title III, she is not liable for them. But it is "self-evident that the good faith defense simply does not apply to actions (civil or criminal) against persons not engaged in law enforcement" because "there exists no statutory procedure whereby such persons can secure official authorization of interceptions they wish to make." Citron v. Citron, 539 F. Supp. 621, 626 (S.D.N.Y. 1982). See also Heggy v. Heggy, 944 F.2d 1537, 1542 (10th Cir. 1991) (good faith reliance on mistake of law not a defense); Campiti v. Walonis, 611 F.2d 387, 394-95 (erroneous belief that statute did not apply to extension phone not a defense). Sheinbrot, M.D. v. Pfeffer, M.D., 1995 WL 432608 (E.D.N.Y. 7/12/95).

Civil Action Under 2520

Notwithstanding the prohibition of 18 U.S.C. 2511(1)(c), the First Amendment protects the knowing disclosure of illegally intercepted communications if the person making the disclosure played no part in the illegal interception, lawfully obtained access to the communications, and the communications deal with a matter of public concern. Bartnicki v. Vopper, 121 S. Ct. 1753 (2001).

Defendants' use, in the preparation and filing of a lawsuit, of illegally intercepted cordless telephone communications concerning purely private matters was not protected First Amendment activity under the theory applied in Bartnicki. Quigley v. Rosenthal, 327 F.3d 1044 (10th Cir. 2003).

Congressman McDermott knowingly disclosed the contents of illegally intercepted communications in violation of 2511(1)(c). When McDermott received the illegally intercepted communications directly from the illegal interceptors, he had present knowledge of the illegality of such disclosure by the interceptors, and thus "unlawfully" obtained the information. Therefore, the Supreme Court's holding in Bartnicki does not provide a First Amendment shield for Congressman McDermott's violation of 18 U.S.C. 2511. Although not necessary to a

determination of the instant case, Judge Hogan chose to discuss the "duty of confidentiality" and its consequent limitation on First Amendment protection that might have been otherwise enjoyed by the federal judge in U.S. v. Aguilar, 515 U.S. 593 (1995) (judge disclosed wiretap information to the subject of the surveillance). Boehner v. McDermott, 332 F. Supp.2d 149 (D. D.C. 2004).

Section 2520 does not permit recovery for procurement of another to intercept covered communications. Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000); Gunderson v. Gunderson, 2003 WL 1873912 (W.D. Mo.); Hurst v. Phillips, 2005 WL 2436712 (W.D. Tenn.).

Section 2520(a) does not create a private right of action against a person who possesses a device in violation of section 2512(1)(b). Directv, Inc. v. Treworgy, 373 F.3d 1124 (11th Cir. 2004); Flowers v. Tandy Corp., 773 F.2d 585 (4th Cir. 1985) (no private cause of action lies under 18 U.S.C. 2520 for violations of 18 U.S.C. 2512); See Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000) (holding, in context of action for procurement under § 2511(1)(a), that "that violation" in § 2520 clearly refers only to illegal interception, disclosure, or use); Walker v. Darby, 911 F.2d 1573 (11th Cir. 1990) ("In order to recover under § 2520, plaintiff must show that defendants violated § 2511 . . . ."); Directv, Inc. v. Smith, 2004 U.S. Dist. LEXIS 5199 (S.D. Ohio)(excellent review of cases on either side of the issue).

A civil action under 18 U.S.C. 2511 and 2520 may be brought against one who intercepts encrypted satellite transmissions. Directv, Inc. v. Nicholas, 403 F.3d 223 (4th Cir. 2005).

A civil action may be brought under 2520 whether or not defendant has been prosecuted and convicted for acts complained of. Peavy v. Harman, 37 F. Supp.2d 495 (N.D. Tex. 1999) (citing legislative history).

A civil action may be brought under 18 U.S.C. 2520 for an alleged violation of 18 U.S.C. 2512. Directv, Inc. v. Kitzmiller, 2004 U.S. Dist. LEXIS 5263 (E.D. Pa.); Directv, Inc. v. Dougherty, 2003 U.S. Dist. LEXIS 23654 (D. N.J.).

Section 2520(a) does not provide a cause of action against aiders and abettors. In re Toys R US, Inc., Privacy Litigation, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal.).

The ECPA does not recognize a cause of action for aiding and abetting a primary violator, and the Act does not create any secondary liability on the part of the service provider. Motise v. America Online, Inc., 2005 WL 1667658 (E.D. Va..).

Section 2520 of the Wiretap Act expressly precludes relief against the United States. The exclusive remedy against the United States for violation of the Wiretap Act is contained in 18 U.S.C. 2712. Ellis v. Bazetta Police Department, 2005 WL 1126731 (N.D. Ohio); Marshall v. Johnson, 2005 U.S. LEXIS 9620 (W.D. Ky.).

Under 47 U.S.C. 230(c), ISPs are indifferent to the content of information they host or transmit: whether they do or do not take precautions, there is no liability under either state or federal law. Nor is an ISP liable under 18 U.S.C. 2511 and 2520 merely because a customer violates 18 U.S.C. 2511 through use of the ISP's internet hosting services. Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

Claims under 18 U.S.C. 2520 were barred by two year statute of limitations set forth in 2520(e). Lanier v. Bryant, 332 F.3d 999 (6th Cir. 2003); Sparshott v. Feld Entertainment, Inc., 311 F.3d 425 (D.C. Cir. 2002)(no requirement that person actually be aware of the violation, only that the person had a "reasonable opportunity" to discover the wiretapping); Bristow v. Clevenger, 80 F.

Supp.2d 421 (M.D. Pa. 2000); Perkins v. Napieralski, 2001 U.S. Dist. LEXIS 12570 (D. Or.); Menard v. Board of Trustees of Loyola University of New Orleans, 2004 WL 856641 (E.D. La.).

Disclosure of tape recordings by United States Attorney during discovery in plaintiff's criminal prosecution is not a prohibited disclosure under the Wiretap Act. Rule 16 requires the Government upon request by the defendant to disclose certain items for inspection by the defendant, and since the recordings were of the defendant, and the defendant presumably requested their disclosure during discovery, the defendant and his attorney cannot be considered third parties. In any event, the prosecutors are entitled to absolute immunity because turning over tape recordings in discovery pursuant Rule 16 is an action clearly related to a prosecutorial function. Lanier v. Bryant, 332 F.3d 999 (6th Cir. 2003).

Connecticut's fraudulent concealment doctrine was applicable in determining whether claims for alleged wiretapping of plaintiff's workplace telephone were time-barred. Schmidt v. Devino, 106 F. Supp.2d 345 (D. Conn. 2000).

Title III does not preempt a 42 U.S.C. 1983 action based on a claimed Constitutional violation. PBA Local No. 38 v. The Woodbridge Police Department, 832 F. Supp. 808 (D. N.J. 1993); Amati v. The City of Woodstock, 829 F. Supp. 998 (N.D. Ill. 1993).

Under 18 U.S.C. 2520(a), government entities can be held liable for violations of Title III. Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001); Dorris v. Absher, 959 F. Supp. 813 (M.D. Tenn. 1997); PBA Local No. 38 v. The Woodbridge Police Department, 832 F. Supp. 808 (D. N.J. 1993); Conner v. Tate, 130 F. Supp.2d 1370 (N.D. Ga. 2001).

"Title III does not allow for suits against municipalities. 18 U.S.C. 2510(6)." Amati v. City of Woodstock, 176 F.3d 952 (7th Cir. 1999); Abbott v. Village of Winthrop Harbor, 205 F.3d 976 (7th Cir. 2000); Anderson v. City of Columbus, Georgia, 374 F. Supp.2d 1240 (M.D. Ga 2005) (citing Abbott).

Municipalities are exempt from punitive damages under 18 U.S.C. 2520. Lewis v. Village of Minerva, 934 F. Supp. 268 (N.D. Ohio 1996).

District court enjoined defendant's pursuit of a claim against plaintiff based on the defendant's apparent nonconsensual tape recording of plaintiff's participation in a union meeting. 18 U.S.C. 2520(b)(1). Earley v. Smoot, 846 F. Supp. 451 (D. Md. 1994).

The $10,000 liquidated damages amount under § 2520(c)(2)(B) is designed to compensate a claimant for all of a transgressor's misdeeds under the Act, unless that transgressor has violated the Act on more than one hundred separate days, in which case compensation is $100 for each such day. Smoot v. United Transportation Union, 246 F.3d 633 (6th Cir. 2001).

The court has discretion under 2520(c)(2) to award no damages. Directv, Inc. v. Brown, 371 F.3d 814 (11th Cir. 2004); Reynolds v. Spears, 93 F.3d 428 (8th Cir. 1996); Morford v. City of Omaha, 98 F.3d 398 (8th Cir. 1996); Nalley v. Nalley, 53 F.3d 649 (4th Cir. 1995); Culbertson v. Culbertson, 143 F.3d 825 (4th Cir. 1998); Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999); Directv, Inc. v. Griffin, 290 F. Supp.2d 1340 (M.D. Fla. 2003); Leach v. Byram, 1999 U.S. Dist. LEXIS 7832 (D. Minn.); Romano v. Terdik, 939 F. Supp. 144 (D. Conn. 1996); Goodspeed v. Harman, 39 F. Supp.2d 787 (N. D. Tex. 1999).

Despite the use of the term "may," the court has no discretion under 2520(c)(2) to decline to impose damages. Rodgers v. Wood, 910 F.2d 444 (7th Cir. 1990).

An interception violates the statute if the authorization to make it was obtained by material false statements, and "we cannot think of any reason why the damages remedy (under 2520) would be unavailable." Apampa v. Layng, 157 F.3d 1103 (7th Cir. 1998).

Circuit court remands a dismissed 2520 invasion of privacy complaint involving a video recording of consensual sexual activity. The Court finds the complaint not legally deficient, and mentions some facts the plaintiff will have to prove under 2511(1), 2510(2) , 2510(4) and 2511(2)(d). Doe v. Smith, 2005 U.S. App. LEXIS 25051 (7th Cir.).

Civil Action Under 2707

Governmental entity may be held liable under Section 2707(a).
Organization JD Ltda. v. U.S. Dept. of Justice, 18 F.3d 91 (2d Cir. 1994); Conner v. Tate, 130 F. Supp.2d 1370 (N.D. Ga. 2001).

The 1996 amendment to 18 U.S.C. 2707(a), providing a civil cause of action for certain violations of the ECPA to "any provider of electronic communication service, subscriber, or other person aggrieved," does not apply to actions pending at the time of its enactment. Organizacion JD Ltda. v. U.S. Dept. of Justice, 124 F.3d 354 (2d Cir. 1997).

Cause of action was time-barred by two year limitation in 18 U.S.C. 2707(f). Reyna v. City of Coppell 2001 WL 220143 (N.D. Tex.).

Section 2702(a)(3) requires that the plaintiff prove that defendant “knowingly divulged” plaintiff’s subscriber information to establish a statutory violation. An ISP acts knowingly if it has knowledge of the factual circumstances that constitute the alleged offense. Section 2702(a)(3) does not require that the defendant understand the legal significance of these factual circumstances or that the defendant have the specific intent to violate the statute. Freedman v. America Online, Inc., 325 F. Supp.2d 638 (E.D. Va. 2004); Freedman v. America Online, Inc., 329 F. Supp.2d 745 (E.D. Va.. 2004) (denying Defendant’s motion for partial reconsideration)(Section 2707(a) makes clear that a plaintiff may establish civil liability for an ECPA violation by showing either that a defendant violated the statute knowingly **or** intentionally –- an ISP acts intentionally provided only that its acts are not inadvertent).

Cellular and Cordless Telephone Violations

The radio portion of a cordless telephone communication is a protected wire or electronic communication under Title III. Pub.L. No. 103-414 (10/25/94), amending 18 U.S.C. 2510(1) & (12).

Illegal interception of the radio portion of a cordless telephone communication is penalized under the same scheme as that applied to the illegal interception of the radio portion of a cellular telephone communication. The offense is considered to be an "infraction" (subject to a fine of not more than $5000; 18 U.S.C. 3559(a)(9) and 3571(b)(7)) if it is a first offense not for a tortious or illegal purpose, not for commercial advantage or private commercial gain, and the intercepted radio communication was not encrypted, scrambled 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. 18 U.S.C. 2511(4)(b).

Although defendant police officer's interception of the cordless telephone communications of plaintiff during a drug investigation in 2000 violated federal law (cordless telephone exemption removed from Title III in 1994), the good faith defense in 18 U.S.C. 2520(d) excuses the defendant from liability because he relied in good faith on a Tennessee court order issued in accordance with state law, and he received verification of its propriety from a local assistant district attorney. Because the law regarding Fourth Amendment applicability to cordless telephone communications is not "clearly established" (neither the Supreme Court nor the Sixth Circuit has specifically addressed the issue), and because he was acting pursuant to a court order under state law, and with the endorsement of an assistant district attorney, the defendant has qualified immunity from liability if there was a Fourth Amendment violation. Frierson v. Goetz, 2004 U.S. App. LEXIS 10037 (6th Cir.) (unpublished).

Descramblers

Section 2512 prohibits modification, sale, or possession of descramblers knowing or having reason to know that the design of such device renders it primarily useful for the purpose of surreptitious interception of satellite television transmissions. Whether the design of the device renders it primarily useful for the purpose of surreptitious interception is a question of fact that will in virtually every case have to go to trial. U.S. v. Herring, 993 F.2d 784 (11th Cir. 1993)(en banc); U.S. v. One Macom Video Cipher II, 985 F.2d 258 (6th Cir. 1993); U.S. v. Harrell, 983 F.2d 36 (5th Cir. 1993); U.S. v. Splawn, 982 F.2d 414 (10th Cir. 1992) (en banc); U.S. v. Shriver, 989 F.2d 898 (7th Cir. 1992) (also, section 2511 applies to manufacture and sale of modified descramblers); U.S. v. Davis, 978 F.2d 415 (8th Cir. 1992)(en banc); U.S. v. Lande, 968 F.2d 907 (9th Cir. 1992).

Because of ambiguities as to whether "electronic communications" in the form of scrambled cable transmissions are clearly protected by 2512, defendant (an electronic components supplier) was held not to have violated 2512(1)(b). U.S. v. Hochman, 809 F. Supp. 202 (E.D.N.Y. 1992).

Cable television programming transmitted over a cable network is not a "radio communication" as defined in 47 U.S.C. 153(b), and thus its unlawful interception must be prosecuted under 553(a) and not 605. Congress intended for 47 U.S.C. 605 to apply to the unlawful interception of cable programming transmitted through the air, while it intended for 47 U.S.C. 553 to apply to the unlawful interception of cable programming while it is actually being transmitted over a cable system. U.S. v. Norris, 88 F.3d 462 (7th Cir. 1996); TKR Cable Company v. Cable City Corporation, 267 F.3d 196 (3d Cir. 2001); TCI Cablevision of New England v. Pier House Inn, Inc., 930 F. Supp. 727 (D. R.I. 1996); CSC Holdings, Inc. v. Kimtron, Inc., 47 F. Supp.2d 1361 (S.D. Fla. 1999).

Surreptitious Interception Devices

Section 2512 is not unconstitutionally vague. U.S. v. Biro, 143 F.3d 1421 (11th Cir. 1998).

Section 2512, as applied to these defendants, is not unconstitutionally vague, notwithstanding the legality of one party consensual monitoring under 2511(2)(d). U.S. v. The Spy Factory, Inc., 951 F. Supp. 450 (S.D.N.Y. 1997).

Parental Interception of Child on Home Telephone

(extension phone exemption)

Custodial parent's interception of telephone conversations of minor child within the custodial parent's home, without the child's knowledge or consent, is not prohibited by Title III. Newcomb v. Ingle, 944 F.2d 1534 (10th Cir. 1991); Anonymous v. Anonymous, 558 F.2d 677 (2d Cir. 1977); Scheib v. Grant, 22 F.3d 149 (7th Cir. 1994).

(vicarious consent)

Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998) (custodial parent's objectively reasonable exercise of "vicarious consent" to protect minor child qualifies for consent exception under 2511(2)(d)); Thompson v. Dulaney, 838 F. Supp. 1535 (D. Utah 1993); Campbell v. Price, 2 F. Supp.2d 1186 (E.D. Ark. 1998); Wagner v. Wagner, 64 F. Supp.2d 895 (D. Minn. 1999).

Husband/Wife Interceptions

Title III provides no exception for interspousal wiretapping. Glazner v. Glazner, 347 F.3d 1212 (11th Cir. 2003); Heggy v. Heggy, 944 F.2d 1537 (10th Cir. 1991); Kempf v. Kempf, 868 F.2d 970 (8th Cir. 1989); Pritchard v. Pritchard, 732 F.2d 372 (4th Cir. 1984); U.S. v. Jones, 542 F.2d 661 (6th Cir. 1976); Lombardo v. Lombardo, 192 F. Supp.2d 885 (N.D. Ind. 2002); Walker v. Carter, 820 F. Supp. 1095 (C.D. Ill. 1993). Gaubert v. Gaubert, 1999 WL 10384 (E.D. La.)(no interspousal immunity where separated husband affixed taping device to telephone in marital residence occupied by wife).

The Second Circuit holds that Title III does not apply to interspousal wiretaps. Anonymous v. Anonymous, 558 F.2d 677 (2d Cir. 1977).

Home Telephone Extension Exception

Unrecorded eavesdropping on home extension telephone by family member concerned about the safety of her sister was not an "intercept" under Title III or Massachusetts law because such telephone extension use, in the residential context, qualifies as use within the ordinary course of business under 18 U.S.C. 2510(5)(a)(i). Commonwealth v. Vieux, 671 N.E.2d 989 (Mass. App. Ct. 1996) (comprehensive review of case law concerning residential telephone interceptions). [Affirming the federal district court's rejection of a habeas petition, the First Circuit held that the Massachusetts Appeals Court holding in Vieux was not "contrary to" or "an unreasonable application" of federal law in light of a healthy debate among a number of courts. Vieux v. Pepe, 184 F.3d 59 (1st Cir. 1999)]

Other Offenses

Criminal Disclosures

Disclosure of a wiretap after its authorization expires violates 18 U.S.C. 2232(c) [now 2232(d)]. The offense is complete at the time the notice is given, when it often cannot be known whether any interception will take place. U.S. v. Aguilar, 515 U.S. 593 (1995).

18 U.S.C. 2232(d) provides:

> (d) Notice of certain electronic surveillance.--Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

18 U.S.C. 2511(1)(e) provides that any person who:

> (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) to (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).

18 U.S.C. 1503

This is an issue of first impression in the federal courts. The Third Circuit concluded that a wiretap is part of an investigation conducted by agents of the executive branch and does not constitute the "administration of justice" within the meaning of 18 U.S.C. 1503. U.S. v. Davis, 197 F.3d 662 (3d Cir. 1999).