

By: Chris W. McCarty
Lewis, King, Krieg & Waldrop, P.C.



Why Does Your Jacket Echo? Identifying and Understanding the ECPA

We all know the scene. Two guys with mustaches fasten what looks like a Sony Walkman¹ to the chest of a rather sullen looking man. He whines about possible death while they joke about his predominantly hairless torso. We soon find our mustachioed buddies sitting in a van and listening intently to large earphones. It seems a stereotypical Russian mobster is about to confess numerous crimes into our hero's hairless chest.

As a lawyer, have you ever asked this question while watching that scene: don't they need a warrant? Surprisingly, the answer is, "No." Exceptions and exemptions to the Electronic Communications Privacy Act ("ECPA") often allow law enforcement and private employers to bypass individual privacy protections.²

I. ECPA

"Electronic surveillance law is largely governed by the [ECPA]."³ Legislators divide the ECPA into three (3) titles. Title I prohibits the intentional interception of wire, oral, or electronic communications (unless authorized by court order). Title II proscribes unauthorized access to stored wire or electronic communications. Finally, Title III pertains to pen registers and trap/trace devices.

When reading the word "surveillance" many of us think of a cops and robbers scenario much like the one previously described. But Webster's Dictionary paints "surveillance" with a broader brush: "close watch kept over someone or something." That means electronic surveillance encompasses everything from a cop wearing a wire to your firm's IT person reading a coworker's e-mail.

II. CRIMINAL

The ECPA finds its most obvious application in criminal matters. Both policemen and prosecutors rely on the Act to guide their use of electronic surveillance. In turn, a defense attorney may harness the ECPA to exclude that pesky audio-recording of her client buying stolen microwaves from guys named Vinny and Sal.

Yet the ECPA should be viewed as more map than barrier. That map still points toward the Fourth Amendment and probable cause when an officer wants to tap your phone line. When looking again at our Russian mobster's confession, however, we discover that our hairless hero may tape that confession without a warrant.

Under one (1) of many ECPA exceptions, "[i]t shall not be unlawful . . . for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication[.]"⁴ That means the Fourth Amendment shall not be offended "where one of the parties to the communication consents to have the communication electronically monitored[.]"⁵ So, as long as our hairless hero remains a party to his conversation with the Russian mobster, the ECPA will allow their conversation to be recorded and later introduced.

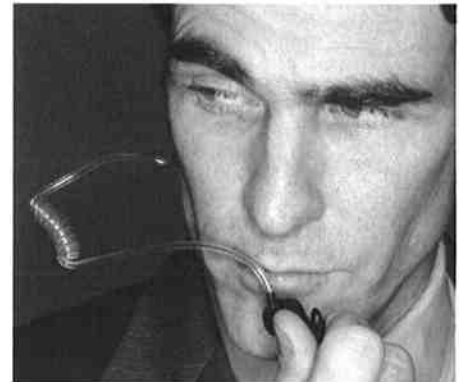
III. CIVIL

Surprisingly, the ECPA also finds application outside the criminal realm. The Act commands a very real presence in Corporate America. In fact, many employers now view the ECPA as yet another batch of lawsuits waiting to happen.

Under the ECPA, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used . . . may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."⁶ Put simply, though "[t]he ECPA is primarily a criminal statute, [it also] authorizes recovery for civil damages."⁷ That can even mean awards for both punitive relief and attorneys' fees.⁸

Those damages, however, remain lofty goals when faced with the ECPA's so-called business extension exemption.⁹ This "exemption operates without regard to consent." Employers, for example, may lawfully monitor employee telephone calls under the ECPA "so long as the requisite business connection is demonstrated."¹⁰

Courts originally interpreted the business extension exemption to include any calls, e-mails or other electronic communications stemming from company equipment. In other words, you would possess no ECPA privacy protections while using a work-based e-mail



account. Yet as our society grows more protective of its electronic communications, our courts seem more willing to recognize previously nonexistent ECPA protections.¹¹ That places employers on alert and their attorneys on the lookout.

IV. CONCLUSION

Unlike the surveillance scene referenced throughout this article, the ECPA cannot be easily described. It remains a complex statute whose borders and applications grow with each passing day. The ECPA comes into play while defending a banker whose emails infer embezzlement; and yet the same statute will also rear its head during a divorce proceeding in which the husband taped his wife admitting to a fling with the mailman. As more and more of our clients depend on and utilize electronic communications, the ECPA must be something that we all learn to identify and navigate. If not, like our Russian comrade, we may be in for an unwelcome surprise.

¹ For the Y Generation reader, the Sony Walkman was a pre-iPOD portable listening device.

² See 18 U.S.C. §§ 2510, et seq. Tennessee's largely parallel version of the ECPA can be found at: Tenn. Code Ann. § 39-13-601, et seq.

³ In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

⁴ 18 USCS § 2511(2)(c).

⁵ United States v. Vasquez, No. 98 CR 795, 1999 U.S. Dist. LEXIS 13301, *22 (N.D. Ill. 1999), citing United States v. White, 401 U.S. 745, 751-754 (1971), see also 18 USCS § 2511(2)(c).

⁶ 18 USCS § 2520(a).

⁷ Eves v. Henry County, No. 1: 05-cv-3216-GET, 2006 U.S. Dist. LEXIS 48573, *3 (N.D. Ga. 2006).

⁸ 18 USCS § 2520(b).

⁹ 18 USCS § 2510(5)(a)(i).

¹⁰ Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).

¹¹ See Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) (Ninth Circuit recognized an employee's privacy interests as to text messages from an employer-provided pager).