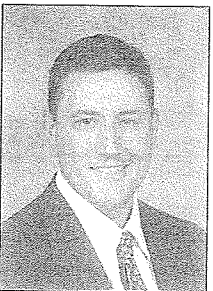


MICHAEL NEWMAN AND SHANE CRASE

What in the World is the Electronic Communications Privacy Act? An Overview of the ECPA Hurdles in the Context of Employer Monitoring

Employers have a myriad of legitimate reasons to monitor their employees. Not only do employers face considerable liability problems, but they must also keep track of employees' productivity in order to run their businesses successfully.¹ Nevertheless, the law must provide a balance between an employer's right to monitor employees and an employee's right to privacy. Fortunately, the Electronic Communications Privacy Act (ECPA) attempts to strike such a balance. Congress enacted the ECPA to provide greater protection of an individual's privacy from emerging communication technologies in the private sector.² Yet, even with this federal statutory protection, employees still have difficult hurdles to overcome before recovering damages under the ECPA.



The ECPA "prohibits the intentional or willful interception, accession, disclosure, or use of one's electronic communication."³ The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act—known as the Federal Wiretap Act—and, most significantly, inserted the term "electronic communication" into the language (whereas Title III previously protected only wire and oral communications).⁴ The ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part of a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."⁵

The ECPA mandates criminal punishment⁶ for violating the act and also provides a civil cause of action allowing damages.⁷

The ECPA contains three exceptions that are applicable to employers' monitoring of employees in the private sector: monitoring communications used for business, used by service providers, and used with the consent of the party being monitored.⁸ This column will discuss how various federal courts have interpreted the ECPA and its exceptions and will illustrate

some of the potential pitfalls for employers, employees, and attorneys practicing in this area of the law.

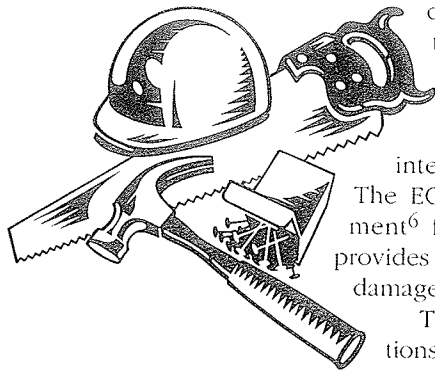
The Business Use Exception

The "business use" exception asserts that any equipment or component used in the ordinary course of business is not considered an electronic device, and therefore an employer who uses such a device is exempt under the ECPA.⁹ The determining factor is whether the interceptor device is used in the ordinary course of business.¹⁰ Courts often use two methods when applying the business use exception: the content approach and the context approach.¹¹

The content approach allows employers to monitor "business-related" communications but not personal communications.¹² When applying this approach, the courts focus primarily on the subject matter of the intercepted communication.¹³ For example, in *Watkins v. L.M. Berry & Co.*, the U.S. Court of Appeals for the Eleventh Circuit ruled that the employer's conduct—intercepting an employee's personal call discussing a job interview with a prospective employer—was unlawful.¹⁴ The court held that employers must prove a "business interest" in the employee's communication and that personal calls are never made or received "in the ordinary course of business ... except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not."¹⁵

In a differing opinion—*Briggs v. American Air Filter Co.*—the U.S. Court of Appeals for the Fifth Circuit decided that it is in the ordinary course of business for an employer to intercept a call if the employer suspects that the employee is disclosing confidential business information.¹⁶ Similarly, in *Epps v. St. Mary's Hospital of Athens Inc.*, the Eleventh Circuit held that an employer's interception of a telephone conversation between employees who criticized the company's supervisors was lawful.¹⁷ The Eleventh Circuit found that the conversation was a "business call" because it transpired during office hours and the employer had a legitimate interest in keeping a stable work environment.

The content approach concentrates on the subject of the interception, whereas the context approach focuses on the circumstances of the interception that is being challenged.¹⁸ The context approach centers on



the workplace environment as opposed to the content of the conversation and takes into account certain factors in order to determine the employer's reasoning for monitoring the communication.¹⁹ The ultimate test the courts use when applying the context approach is whether the employer had a legitimate business interest that justified the interception.²⁰

In *United States v. Harpel*, the U.S. Court of Appeals for the Tenth Circuit established that, at a minimum, employers must sufficiently inform employees of the possibility that their communication could be intercepted.²¹ Reiterating the importance of notice, the Tenth Circuit, in *James v. Newspaper Agency Corp.*, upheld a monitoring system after the employer proved that the purpose of the interception system was to protect employees from abusive calls and to help supervisors train employees in customer communication.²² The court also found it significant that employees had prior notice of the system.²³

More recently, in *Deal v. Spears*, the Eighth Circuit articulated a two-pronged test for the context approach.²⁴ The court required that "the intercepting equipment must be furnished to the user by the phone company or connected to the phone line, and it must be used in the ordinary course of business."²⁵ Because the employer had purchased the monitoring device separately from the firm's communications system, the court found that the monitoring did not meet the ordinary business use exception. The court also concluded that the employer's asserted justification for business use of the device—to catching burglars—was insufficient because the employer had monitored the employee's calls even when they were clearly personal and unrelated to the employer's business interest.²⁶

The Service Provider Exception

Along with the business use exception, the ECPA also establishes a "service provider" exception, which exempts employers from the law when they provide "electronic communication service."²⁷ This exception permits network providers to intercept an employee's communications that are conducted during the ordinary course of business that are "necessary to the rendition of service," or "necessary to protect the rights or property" of the company.²⁸ This exception is broad, because most employers provide electronic communications to their employees; therefore, employers may almost always meet the service provider exemption.²⁹

The Consent Exception

Another exception to the ECPA is the consent exception, which provides that an interception is lawful if one of the parties to the communication gives prior consent to the interception.³⁰ Employers may gain consent either by publishing a monitoring policy or

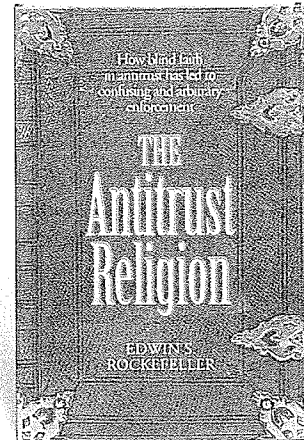
LABOR continued on page 14

NEW BOOKS FROM THE CATO INSTITUTE

"It is not surprising that antitrust law enforcement, grounded on such precise concepts as 'unreasonable' and 'unfair,' has allowed policy-making prosecutors and judges to careen crazily across the legal landscape for generations."

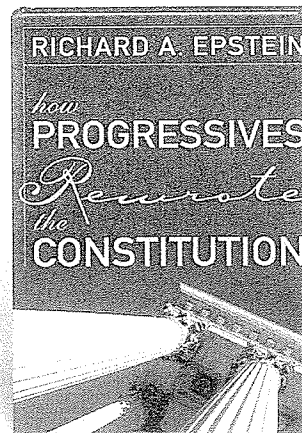
—DANIEL OLIVER
former chairman
Federal Trade Commission

Drawing on 50 years of experience with U.S. antitrust laws, attorney Edwin S. Rockefeller sheds light on why lawmakers, bureaucrats, academics, and journalists use arbitrary and irrational laws and enforcement mechanisms to punish businesses rather than promote competition.



\$16.95 • hardcover • 978-1-933995-09-0

Now in paperback!



\$10.95 • paperback • 978-1-933995-06-9

\$15.95 • hardcover • 978-1-930865-87-7

"Epstein provides an astonishingly detailed account of the reformation of the U.S. Constitution in surprisingly few pages. He highlights every major court case that altered the original ideals of the Constitution ever so slightly, but that turned out in the end to land America drastically far from the sound political ideals with which it had begun."

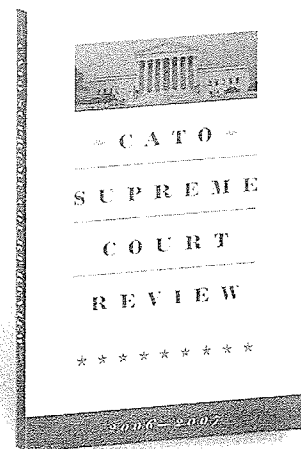
—ECONOMIC AFFAIRS

University of Chicago professor of law Richard Epstein explores the fundamental shift in political and economic thought in the Progressive Era and how the Supreme Court used those ideas to undermine the Constitution.

"In view of so many Americans' alarming lack of knowledge of why we are Americans, the *Cato Supreme Court Review* is essential reading."

—NAT HENTOFF
syndicated columnist
Village Voice

Published every September, the *Cato Supreme Court Review* brings together leading legal scholars to analyze key cases from the Court's most recent term, plus cases coming up. Now in its sixth edition, the *Review* is the first scholarly journal to appear after the term's end and the only one to critique the Court from a Madisonian perspective, grounded in the nation's first principles, liberty and limited government.



\$15.00 • paperback • 978-1-933995-08-3

Buy your copy at bookstores nationwide, by calling 800-767-1241,
or by visiting www.cato.org

by adequately informing employees of the policy.³¹ Moreover, actual consent may be implied from the circumstances.³² However, knowledge of the possibility of interception does not always imply employee consent.³³ Furthermore, the employer must not have a criminal or tortious purpose for the interception, such as extortion, blackmail, or intent to cause emotional distress.³⁴

In *Watkins v. L.M. Berry & Co.*, the Eleventh Circuit ruled that consent cannot be systematically implied because it would negate the purpose of the ECPA's consent exception.³⁵ Similarly, in *Deal v. Spears*, the Eighth Circuit concluded that an employer must prove more than a mere capability of monitoring to meet the consent exception. In *Deal*, the employer told employees that the business "might" need to intercept calls to deter the increasing amount of personal calls, and the court determined this justification was insufficient to meet the consent exemption.

"Contemporaneous" Exception

In addition to the three exceptions enumerated by the ECPA, there is a judge-made "contemporaneous" exception for "electronic communications."³⁶ In *Steve Jackson Games Inc. v. United States Secret Service*, the Fifth Circuit ruled that a violation under the ECPA requires the interception to be contemporaneous with the transmission. In other words, in order to violate the ECPA, an employer must intercept an e-mail at the time it was sent and before it was stored in the employer's e-mail system. The court found that Congress had not intended for the word "intercept" to apply to "electronic communications" when those communications are located in "electronic storage." In *Konop v. Hawaiian Airlines Inc.*, the Ninth Circuit held that "for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."³⁷

In contrast, in *United States v. Councilman*, the First Circuit disagreed with the *Konop* ruling when the court concluded that e-mail in temporary storage can still be "intercepted" within the meaning of the ECPA and is not required to be "in transmission" when it was intercepted.³⁸ According to the *Councilman* court, "we doubt that Congress contemplated the existential oddity that Councilman's interpretation creates: messages ... briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again."

Conclusion

The ECPA attempts to strike a balance between an employer's right to monitor employees and an employee's concerns about privacy. By prohibiting the intentional interception, accession, disclosure, or use

of electronic communications, the ECPA attempts to alleviate employees' concerns about their privacy. On the other hand, the ECPA addresses the needs of employers by establishing three exceptions to this general rule. Whether they represent employers or employees, attorneys practicing in this area of the law need to understand how various federal courts have interpreted the ECPA and its exceptions and be aware of the potential pitfalls employers and employees as well as their attorneys can encounter in cases involving monitoring of employees' electronic communications. TFL

Michael Newman is a partner in the Labor and Employment Department of the Cincinnati-based firm, Dinsmore & Shohl LLP, where he serves as chair of the Labor and Employment Appellate Practice Group. He is a vice president of the FBA's Sixth Circuit. Shane Crase is an associate in the same department and treasurer of the Cincinnati-Northern Kentucky Chapter of the FBA. They may be reached at michael.newman@dinslaw.com and shane.crase@dinslaw.com, respectively.

Endnotes

¹See Louise Ann Fernandez and Jennifer Rappoport, WORKPLACE CLAIMS: BEYOND DISCRIMINATION, LITIGATION AND ADMINISTRATIVE PRACTICE COURSE HANDBOOK SERIES, 662 PLI/Lit 1221, 1224 (2001).

²Sarah DiLuzio, Comment, *Workplace E-mail: It's Not as Private as you Might Think*, 25 DEL. J. CORP. L. 741, 745 (2000) (citing 18 U.S.C. § 2511 (1994)).

³18 U.S.C. §§ 2510–2520 (2006).

⁴18 U.S.C. § 2522(1)(a). Furthermore, Congress banned the illegal access and disclosure of electronically stored wire and electronic communications under Title II of the ECPA, which is also referred to as the Stored Communications Act. See 18 U.S.C. §§ 2701–2711 (2002). Even though the ECPA does not explicitly mention "e-mail," the legislative history indicates that Congress intended to include e-mail within the definition of "electronic communication." See Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. LAW 115, 130–131 (2005).

⁵18 U.S.C. § 2510(12).

⁶18 U.S.C. §§ 2511(4)–(5).

⁷18 U.S.C. § 2520. The ECPA provides "appropriate relief [that] includes: such preliminary and other equitable or declaratory relief as may be appropriate, damages under subsection (c) and punitive damages in appropriate cases, and a reasonable attorney's fee and other litigation costs reasonably incurred."

⁸18 U.S.C. § 2510(5)(a); 18 U.S.C. § 2511(2)(a)(i); 18 U.S.C. § 2511(2)(d).

⁹18 U.S.C. § 2510(5)(a).

¹⁰Alexander I. Rodriguez, Note, *All Bark, No Byte*:

Employee E-mail Privacy Rights in the Private Sector Workplace, 47 EMORY L.J. 1439, 1452-1453 (1998).

¹¹*Id.*

¹²*See id.*, at 1455-1456 (citing *Briggs v. American Air Filter Co.*, 630 F.2d 414, 420 (5th Cir. 1980)).

¹³*Id.*

¹⁴704 F.2d 577, 581 (11th Cir. 1983).

¹⁵*Id.* at 582-583. The court also determined that an employer should stop intercepting a communication as soon as the employer verifies the call is personal.

¹⁶630 F.2d at 419-420. The court stated: "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."

¹⁷802 F.2d 412, 416-417 (11th Cir. 1986).

¹⁸*See* Dan McIntosh, *E-Monitoring@Workplace.Com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 HAMLINE L. REV. 539, 550 (2000).

¹⁹*See* Rodriguez, *supra* note 10, at 1453-1454 (citing *United States v. Harpel*, 493 F.2d 346 (10th Cir. 1974); *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979); *Deal v. Spears*, 980 F.2d 1153, 1158 (8th Cir. 1992); and *Sanders v. Robert Bosch Corp.*, 38 F.3d 736 (4th Cir. 1994)).

²⁰*See* McIntosh, *supra* note 19.

²¹*Harpel*, 493 F.2d at 351.

²²*James*, 591 F.2d at 581; *See also Arias v. Mutual Cent. Alarm Serv. Inc.*, 202 F.3d 553, 559 (2d Cir. 2000) (finding a valid business justification for the employer's monitoring system).

²³*Id.*

²⁴*Spears*, 980 F.2d at 1157.


²⁵*Id.*; *See also Sanders*, 38 F.3d at 741.

²⁶*Id.*; but *see O'Sullivan v. Nynex Corp.*, 426 Mass. 261, 687 N.E.2d 1241 (1997) (applying federal case law regarding the ECPA in order to determine claims under the Massachusetts wiretap statute).

²⁷18 U.S.C. § 2511(2)(a)(i); *See* Hornung, *supra* note 4 at 138; *see also United States v. Mullins*, 992 F.2d 1472 (9th Cir. 1992). 18 U.S.C. § 2511(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 necessary incident to the

LABOR continued on page 23

THERE IS A BETTER WAY TO KEEP THE WHEELS OF JUSTICE TURNING...



... WITHOUT MAKING ATTORNEYS TRAVEL TO COURT FOR A BRIEF APPEARANCE.

CourtCall®
TELEPHONIC COURT APPEARANCES

Find out how COURTCALL® can offer your Court a simple and innovative Solution for TELEPHONIC APPEARANCES at no Cost or Expense to the Court.

Join the hundreds of other Courts that trust CourtCall® to handle their Telephonic Appearances.

Enhance courtroom efficiency • Program tailored to individual Judge
State of the art technology provided to the Court at no charge
No change in Judge's schedule • No burden on courtroom staff
Reduce travel time and save money

YOUR COURT'S SOURCE FOR TELEPHONIC APPEARANCES

Federal, Bankruptcy and State Courts Nationwide

Enron PG&E United Worldcom Aldephia

PUT OUR EXPERIENCE TO WORK FOR YOUR LEGAL COMMUNITY!
Just a few representative cases

Call for Details:
888.882.6878

www.courtcall.com

rendition of his service or to the protection of rights or property of the provider of that service.”

²⁸*Id.*

²⁹*Id.*; Hornung, *supra* note 4, at 138.

³⁰18 U.S.C. § 2511(2)(d).

³¹DiLuzio, *supra* note 2, at 748; *see also Campiti v. Walonis*, 611 F.2d 387 (1st Cir. 1979).

³²*Deals*, 980 F.2d at 1157.

³³*Watkins*, 704 F.2d at 580; but *see United States v. Rittweger*, 258 F. Supp. 2d 345, 354–55 (S.D.N.Y. 2003) (finding consent when the plaintiff knew that the lines

were continuously taped, that the employer reserved the right to listen to those tapes, and the employee handbooks made employer monitoring clear).

³⁴*Id.*; *see McIntosh, supra* note 19, at 556–557 (citing *Roberts v. Americable Internat'l Inc.*, 883 F. Supp. 499, 502 (E.D. Cal. 1995)).

³⁵*McIntosh, supra* note 19, at 577.

³⁶*See Steve Jackson Games v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994).

³⁷302 F.3d 868, 878–879 (9th Cir. 2002).

³⁸418 F.3d 67, 79–81 (1st Cir. 2005).

INSIGHT continued from page 19

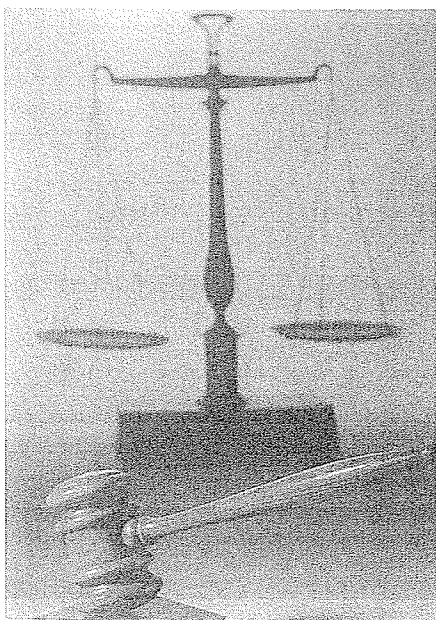
the licensor upon the licensee, it is likely that the licensor will be burdened with the defense and indemnity for design defects—both alleged and actual defects. Defects interjected by negligence in manufacturing (including lack of quality control and defective or improper materials) are typically made the responsibility of the manufacturing licensee. Breaches of implied or express warranties are generally founded on product labeling, and these may revert to the product approval process or a licensee's promotional program; therefore, liability between the licensor and licensee will rest as it was negotiated by the parties to the agreement.

In the United States, insurance covering losses associated with such injuries may be costly or difficult to obtain. If one of the licensing parties does not have liability insurance to cover the licensed property, the indemnity provisions of the license agreement may become meaningless in the event that this party also does not have the financial resource to bear the costs of litigation and indemnity. In such a case, it may be incumbent on the other party to prescribe some additional security to protect its investment.

Conclusion

The licensing process is a business tool used to commercialize intellectual property. As long as the property can be quantified—either in a registered document such as a patent, trademark, or set of specifications or sequential steps in a manufacturing process—it is capable of being sold, leased, or traded. The approach to licensing begins with the recognition and evaluation of the respective needs of the parties in reaching agreement. The task concludes with the adoption of assurances, guarantees, and alternative obligations in the event the commercial situation should change or go awry. In the middle remains the continuing interest of the licensor and licensee to maintain the value of the licensed property in order to continue (or expand) the commercial return on the investment. TFL

H. Roy Berkenstock is a patent and trademark attorney in the Memphis, Tenn., office of Wyatt, Tarrant & Combs LLP. He can be reached at (901) 537-1108 or rberkenstock@wyattfirm.com. © 2007 H. Roy Berkenstock. All rights reserved.



Judicial Profile Writers Wanted

The Federal Lawyer is looking to recruit current law clerks, former law clerks, and other attorneys who would be interested in writing a Judicial Profile of a federal judicial officer in your jurisdiction. A Judicial Profile is approximately 1,500–2,000 words and is usually accompanied by a formal portrait and, when available, personal photographs of the judge. Judicial Profiles do not follow a standard formula, but each profile usually addresses personal topics such as the judge's reasons for becoming a lawyer, his/her commitment to justice, how he/she has mentored lawyers and law clerks, etc. If you are interested in writing a Judicial Profile, we would like to hear from you. Please send an e-mail to Stacy King, managing editor, sking@fedbar.org.