



It May Be Incredibly Easy in the Digital Age, but Secretly Recording Conversations Is Still Illegal

By Lindsay A. LaSalle

INTRODUCTION

Scott Gerber, the Communications Director for California Attorney General Jerry Brown, resigned in early November after it was revealed that he had secretly recorded telephone conversations with reporters. Neither Brown nor any other attorneys in the office were aware Gerber was recording the calls without permission.¹ Gerber explained in his resignation letter: “My purpose wasn’t to play gotcha but simply to have an accurate record of official, on-the-record statements about matters of public concern.”² Whatever Gerber’s purpose, however, recording private conversations without the consent of all parties is illegal under California law and violators are subject to both criminal and civil liability.

This Commentary provides an overview of the federal and state regulations governing the legality of monitoring confidential conversations and the measures that employers should take to ensure compliance. Special attention is paid to California privacy law. While no action has yet been taken against employees in the Attorney General’s office, Gerber’s misstep provides a stark reminder to employers of the privacy rights implicated by monitoring or recording workplace conversations.

FEDERAL PRIVACY LAW

The Electronic Communications Privacy Act (ECPA) of 1986 prohibits the real-time interception, by mechanical or electronic means, of telephone conversations (wireless or wireline), emails, and other employee communications that take place in or by means of an employer’s facilities. All employers, whether public or private, commercial or nonprofit, are subject to the ECPA restrictions.³

ECPA contains two exceptions that are of particular importance to employers, but the benefit of those exceptions can be lost if they are not well understood.

The first is the “business extension” exception, which permits employers to monitor an employee’s communications in the ordinary course of the employer’s business. This exception does not apply when the employer records or listens to an employee’s private conversations, and only covers monitoring accomplished with “telephone or telegraph” instruments or components ordinarily provided by the telephone company or other service provider.

This second qualification to the business extension exception is a bit of an

anachronism today: it dates from a time when telecommunications service was provided by licensed monopolies that were the exclusive source of the telephones and related equipment furnished to their customers. In that environment, there was a clear distinction between an extension telephone that fell within the exception because the telephone was provided by the telephone company under tariff, and a recorder or other device that fell outside the business extension exception because the device had to be obtained elsewhere. Today, with rapidly evolving communications technologies and multiple sources of every kind of equipment, the distinction is harder to make. Businesses that intend to rely on the business extension exception are well advised to confine their monitoring, literally, to the use of extension telephones.⁴

The second exception is far more useful. Under the “prior consent” exception, an employer may monitor electronic communications where *one* party to the communication has consented to the monitoring.⁵ The prior consent exception has been narrowly interpreted in the employment context: consent is unlikely to be implied and cannot be given on behalf of the employee by the employer. However, consent may be expressly given in employment contracts as a condition of employment or through company-wide policies addressing electronic monitoring. The employer must announce its policy concerning monitoring employees’

phone conversations in advance of implementing the policy. Once the policy has been announced, employees generally are considered to have consented to the monitoring by continuing to work for the employer.⁶

The EPCA provides a civil cause of action to anyone whose communications are unlawfully intercepted. Successful plaintiffs may recover actual or statutory damages (the greater of \$10,000 or \$100 a day for each day of violation), punitive damages, and attorney’s fees. The EPCA also makes the unlawful interception, or the attempted interception, of an oral, wire, or electronic communication a felony punishable by fine and/or imprisonment.⁷

STATE PRIVACY LAWS

Most states have enacted legislation prohibiting electronic monitoring and surveillance of workplace conversations.⁸ The District of Columbia and 38 states follow the federal model and are therefore referred to as “single-party consent states.” As previously detailed, an employer may lawfully intercept and record a workplace conversation when one of the parties to the conversation has given prior consent.

California, on the other hand, is one of 12 states that have taken a more protective stance than the federal government in favor of greater personal privacy. These states require notification and consent of *all* parties before a private conversation

may be recorded. In addition to California, these states include Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

For employers in these states, it is important to stress that federal law does not preclude the application of state standards that apply more restrictive rules. In *People v. Conklin*, 12 Cal. 3d 259 (Cal. 1974), for example, the California Supreme Court addressed the question of whether the provisions of the federal Omnibus Crime Control and Safe Streets Act of 1968, later amended by the EPCA, preempted the application of the more stringent provisions embodied in California’s invasion of privacy law. Reviewing the legislative history of the federal regulation, the court determined that “Congress intended that the states be allowed to enact more restrictive laws designed to protect the right of privacy,” pointing out that a legislative committee report observed that “[t]he proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation.”

CALIFORNIA’S INVASION OF PRIVACY ACT

The California Legislature enacted the Invasion of Privacy Act, Sections 630 to 638 of the California Penal Code, to protect the right of privacy of the people of California, declaring that advances

in science and technology had led to the development of new devices and techniques for eavesdropping on private communications and that the invasion of privacy resulting from the increasing use of such devices had created a serious and intolerable threat to the free exercise of personal liberties.⁹ Under Section 632 of the California Penal Code, it is unlawful for any person to intentionally record a confidential communication without the consent of all parties in the communication. This prohibition applies whether the communication is carried on among the parties within the presence of one another or by telephone. As such, this provision effectively prohibits an employer from recording employee telephone conversations or other confidential communications and also prohibits employees from recording their own conversations with other co-workers or clients unless all parties have consented.

For purposes of this prohibition against eavesdropping, a “person” under Section 632(b) is generally any individual, business association, partnership, corporation, limited liability company, or other legal entity, as well as any individual acting on behalf of any government or government subdivision. However, an individual known by all parties to a confidential communication to be overhearing or recording the communication is not

considered a person subject to the prohibition against eavesdropping. A “confidential communication” under Section 632(c) includes any communication carried on in circumstances that reasonably indicate that any party to the communication desires it to be confined to the parties to the communication. Thus, a communication made in a public gathering or in any circumstances in which the parties may reasonably expect that the communication may be overheard or recorded is not considered a confidential communication. The California Supreme Court in *Flanagan v. Flanagan*, 27 Cal. 4th 766 (Cal. 2002), addressed the question of when a communication is “confidential” within the meaning of this provision, holding that “a conversation is confidential under Section 632 if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded.” The court further explained that the statutory scheme protects against recordings “regardless of the content of the conversation.”

The language of Section 632 does not explicitly address whether the statute was intended to apply when one party to a telephone call is in California and another party is outside California. However, the California Supreme Court in *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95 (Cal. 2006), determined that the purpose of the Invasion of Privacy Act supported the application of the statute in a setting in which a person outside

of California records, without the Californian’s knowledge or consent, a telephone conversation of a California resident who is within California.

The facts of the case involved employees of a Georgia brokerage firm who regularly recorded conversations with customers located in California without disclosing to the customers that the calls were being recorded. Though it complied with Georgia law, which permitted a conversation to be recorded where one party to the conversation consents, the practice violated California Penal Code Section 632. The court explained that “the privacy interest protected by the statute is no less directly and immediately invaded when a communication *within California* is secretly and contemporaneously recorded from outside the state than when this action occurs within the state.” As such, the court concluded that “Section 632 applies when confidential communication takes place in part in California and in part in another state.” Thus, employers located in “single-party consent states” may still be liable for recording confidential conversations without the consent of *all* parties, if one of those parties is in California. Consequently, even employers outside California should immediately consider whether their current policy of recording telephone calls complies with California’s statutory scheme—and, if needed, change their call monitoring systems to ensure

This newsletter addresses recent employment law developments. Because of its generality, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

Editor: Lloyd W. Aubry, Jr., (415) 268-6558

San Francisco

Lloyd W. Aubry, Jr. (415) 268-6558
laubry@mofocom

James E. Boddy, Jr. (415) 268-7081
jboddy@mofocom

Karen Kubin (415) 268-6168
kkubin@mofocom

Linda E. Shostak (415) 268-7202
lshostak@mofocom

Eric A. Tate (415) 268-6915
etate@mofocom

Palo Alto

Christine E. Lyon (650) 813-5770
clyon@mofocom

Joshua Gordon (650) 813-5671
jgordon@mofocom

David J. Murphy (650) 813-5945
dmurphy@mofocom

Raymond L. Wheeler (650) 813-5656
rwheeler@mofocom

Tom E. Wilson (650) 813-5604
twilson@mofocom

Los Angeles

Timothy F. Ryan (213) 892-5388
tryan@mofocom

Janie F. Schulman (213) 892-5393
jschulman@mofocom

New York

Miriam H. Wugmeister (212) 506-7213
mwugmeister@mofocom

Washington, D.C./Northern Virginia

Daniel P. Westman (703) 760-7795
dwestman@mofocom

San Diego

Craig A. Schloss (858) 720-5134
cschloss@mofocom

Denver

Steven M. Kaufmann (303) 592-2236
skaufmann@mofocom

London

Ann Bevitt 44-20-7896-5841
abevitt@mofocom

If you wish to change an address, add a subscriber, or comment on this newsletter, please write to:

Wende Arrollado
Morrison & Foerster LLP
12531 High Bluff Drive, Suite 100
San Diego, California 92130
warrollado@mofocom

www.mofocom

©2009 Morrison & Foerster LLP. All Rights Reserved.

that California residents are properly advised of any recording. (See Legal Update for more information at <http://www.mofocom/news/updates/files/update02224.html>)

A violation of the statutory prohibition on eavesdropping on or recording confidential communications is punishable by a fine of up to \$2,500, by imprisonment in the county jail for up to one year, by imprisonment in state prison, or by both the fine and imprisonment. Section 637.2 of the California Penal Code also provides for a civil remedy of the greater of \$5,000, or three times the amount of any damages, to any person who has been injured under the Invasion of Privacy Act. The person injured need not have sustained or be threatened with actual damages. In addition, an action for injunctive relief may be joined with an action for damages.¹⁰

CONCLUSION

In order to ensure compliance with all-party consent laws, including California's Invasion of Privacy Act, employee or client conversations should never be monitored or recorded without the explicit consent of all parties. Many employers may choose to notify their employees in advance, through employment contracts or handbooks, that their activities may be monitored. While this ensures compliance as to conversations between employees, it would not allow an employer to monitor conversations between an employee and a client or other third party. In these cases, the employer

must adequately advise all parties at the outset of the conversation of its intent to record. The third party then has the choice to continue the conversation or not. Scott Gerber opined in his resignation letter that had he simply asked the reporters' permission to record the conversation, they likely "would have readily said yes." Hopefully an awareness of the federal and state privacy laws governing the monitoring and recording of private conversations will help others avoid the same mistake. ■

¹ Joe Carofoli, *Jerry Brown Spokesman on Leave for Secret Tapes*, SAN FRANCISCO CHRONICLE, Oct. 31, 2009, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/10/30/MN0D1AD74H.DTL>.

² <http://www.sacbee.com/static/weblogs/capitolalert/latest/Gerber.pdf>.

³ 18 U.S.C. §§ 2510 *et seq.* (2009) When employers acquire the contents of employee communications in electronic storage rather than in real time (for example, when employers review stored email messages), they are subject to the less stringent requirements of the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.*

⁴ 18 U.S.C. § 2510(4), (5)(a).

⁵ 18 U.S.C. § 2511(2)(d).

⁶ See *Ali v. Douglas Cable Communs.*, 929 F. Supp 1362 (D. Kan. 1996) (explaining that consent will be found where the party knows of the monitoring); see also Kevin J. Conlon, *The Kenneth M. Piper Lecture: Privacy in the Workplace*, 72 CHI.-KENT L. REV 285, 287-88 (1996).

⁷ 18 U.S.C. §§ 2520(a)-(c), 2511(4)(a), (5)(a).

⁸ South Carolina is the only state without such legislation.

⁹ CAL. PENAL CODE § 630 (Deering 2009).

¹⁰ CAL. PENAL CODE §§ 632(a), 637.2.

Lindsay A. LaSalle is an associate in our San Francisco office and can be reached at (415) 268-6079 and llasalle@mofocom.