LEWIS AND ROCA LLP LAWYERS

CLIENT Alert

June 2009

Electronic Communication Monitoring: Tips To Avoid Liability

By Edwin A. Barkel and Emily S. Cates

Technological innovation has drastically changed the way businesses communicate with their customers and prospective clients, supplementing, and in some cases replacing, traditional modes of communication with more-convenient, electronic means, like e-mail and instant messages. Recognizing this shift, FINRA now requires broker-dealers to monitor, review, and preserve electronic communications with the public, like e-mail correspondence. New software is making it more affordable for firms to electronically monitor e-mail correspondence and causing many firms to shift from manual review of printed e-mail. However, doing so without taking certain precautions may put your firm at risk of violating the Electronic Communications and Privacy Act ("ECPA"). *See* 18 U.S.C. § 2510, *et seq.*, and 18 U.S.C. § 2701, *et seq.*

Lewis and Roca is familiar with the ECPA and offers several tips to help your firm engage in or transition to electronic monitoring without violating the ECPA. We begin with a brief overview of the ECPA and why it could pose a threat to your business.

Brief Overview of the ECPA

Passed in 1986 to protect the privacy of electronic communications, the ECPA primarily regulates when and how law enforcement can intercept and access electronic communications, including e-mail, text messages, instant messages, phone calls, etc. Importantly though, it provides for possible civil liability against a "person or entity" that has intercepted another's electronic communications or a service provider that has accessed stored communications without authorization.

The ECPA permits monetary damages starting at $10,000 for an interception and $1,000 for accessing stored communications, injunctive relief, and, in the appropriate case, punitive damages. The ECPA also provides reasonable attorneys' fees and litigation costs for the prevailing plaintiff, but not for a defendant that successfully defeats an ECPA claim. Defending against an ECPA action can, therefore, be expensive. Indeed, a recent article about the ECPA compiled a list of representative damage awards ranging from $1,000 to $100,000 in statutory, compensatory damages and up to $400,000 in one case for punitive damages, plus attorneys' fees.

The primary defense to an ECPA claim is prior, express consent. For example, there is no violation where "one of the parties to the communication has given prior

MEMBERS OF LEWIS AND ROCA'S SECURITIES GROUP INCLUDE:

Edwin Barkel • Emily Cates • Thomas Gilson • Todd Hale • Michael Hammer • Lisa Lackland • Adele Ponce • Candida Ruesga • Thomas Ryan • Jesse Simpson

Still have questions or want help drafting or revising your policies/manuals? Please contact one of our Securities Practice Group Leaders and they will be happy to help answer your questions.

Edwin Barkel	Phoenix	602.262.5377	EBarkel@LRLaw.com
Jesse Simpson	Phoenix	602.262.5387	JSimpson@LRLaw.com

Interested in a particular topic or have an idea for our next Client Alert? Please contact Edwin Barkel or Jesse Simpson with your ideas.

consent to such interception." Similarly, there is no violation under the ECPA for accessing stored data "with the lawful consent of the originator or an addressee or intended recipient of such communication." Some cases have held that prior consent can be implied. That analysis, however, is fact-intensive, and therefore, a defendant is unlikely to establish an implied consent defense before trial on a motion for summary judgment.[1] The ECPA also provides a business exception defense where e-mail is transmitted using company property and e-mail review is something the company does in the ordinary course of its business. In addition, statute of limitations may also offer a defense where a claim has been filed more than two years after the plaintiff should have discovered the violation.

Determining what constitutes an improper "interception" and what constitutes "stored communications" is the subject of considerable debate and courts have repeatedly recognized that the ECPA is not a model of clarity. The plaintiffs in a case Lewis and Roca recently defended, for example, survived dismissal by arguing that a broker-dealer and several of its approved outside e-mail providers unlawfully "intercepted" their e-mails when the outside e-mail providers began automatically forwarding e-mails to the broker-dealer's compliance department for electronic review. The representatives made this claim despite the fact that by registering with FINRA they agreed to abide by FINRA rules, which require the broker-dealers to review their e-mails. In addition, the broker-dealer had simply implemented a new procedure for electronically monitoring the e-mail communications of its independent registered representatives who used e-mail through approved, outside vendors rather than through the firm's internal e-mail system. However, neither the broker-dealer nor the e-mail vendors obtained prior **express consent** from the representatives prior to implementing the new e-mail forwarding procedure. Although the vendors forwarded e-mails for only approximately 21 days and immediately suspended the forwarding when one representative complained, the plaintiffs eventually asserted a class action, which proved expensive to defend.

Tips to Help Avoid Liability

The following tips may help your firm implement electronic monitoring without violating the ECPA:

- Make sure your firm's policy manuals, handbooks, and procedures include language that the firm, with assistance from outside service providers, if applicable, will be monitoring, intercepting, and accessing all incoming, outgoing and stored e-mails. Include broad language so that the policy also covers text messages, instant messages, and any other modes of electronic communication.
- Enforce the policy manual or handbook as written. Do not permit supervisors or employees to create informal policies by suggesting that e-mails and other electronic communications are not actually being monitored, intercepted, or accessed.
- Distribute a consent form that all e-mail users, including employees and independent contractors, must sign, acknowledging and consenting to the monitoring, intercepting, and accessing of all electronic communications. Follow up to make sure all users have signed and returned the forms.
- Provide similar notice and consent forms in your firm's hiring documents for employees as well as independent contractors.
- Periodically remind e-mail users that their communications are being accessed, intercepted, stored, or monitored.
- Work with outside service providers to ensure that their service agreements authorize the providers to access, intercept and forward e-mail to your firm and to work directly with your firm to implement electronic monitoring.

Lewis and Roca can assist in the review and drafting of your policies, employment agreements and consent forms.

[1] Consent is also an important factor for invasion of privacy claims and serves as good evidence that a plaintiff lacks any expectation of privacy, a prerequisite under most states' privacy laws.