



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 10, NO. 5

REPORT

APRIL 15, 2010

Reproduced with permission from Digital Discovery & e-Evidence, 10 DDEE 05, 04/15/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

BNA INSIGHTS

New Jersey Supreme Court Rules That Employees Retain Privacy And Privilege of Attorney-Client Communications Made From Work



By **FERNANDO M. PINGUELO** AND **LAURA J. TYSON**

The New Jersey Supreme Court March 30 announced that after an employee sends or receives e-mails to her attorney via her personal e-mail account from an employer-provided computer, the employer cannot pierce the attorney-client privilege to access the contents of those communications. (*Stengart v. Loving Care Agency, Inc.*, N.J., A-16-09, 3/30/10)

In *Stengart*, the court held that an employee could “reasonably expect that e-mail communications with her attorney through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them.”

The court also held that the company’s attorneys violated an ethics rule by reading the “arguably privi-

leged” e-mails and by failing to alert the employee that they had them.

New Jersey Privacy Protections. The Court’s 7-0 opinion reinforces New Jersey’s commitment to providing broader privacy protections to her citizens than those that are typically available under federal law.¹ Thus, its conclusion that upheld the privilege as attaching to

¹ See, e.g., *State v. McAllister*, 875 A.2d 866, 875 (N.J. 2005) (reasonable expectation of privacy in bank records); *State v. Hemepele*, 576 A.2d 793, 810 (N.J. 1990) (reasonable expectation of privacy in garbage left for collection at curb); *State v. Reid*, 945 A.2d 26, 37 (N.J. 2008) (reasonable expectation of privacy in subscriber information provided to ISPs).

communications made in the workplace was not a complete surprise.

But the court did unleash at least one surprise by announcing that even a seemingly bulletproof company policy on workplace computer use that claims attempts to defeat the attorney-client privilege *would not be enforceable* if the employee accessed the privileged communication through a personal, password-protected e-mail account.

This ruling thus establishes a nearly impenetrable firewall through which employers must pass when they seek to pierce an employee's attorney-client privilege attached to a personal e-mail.

The Facts. As plenty of other employees at work often do, Marina Stengart used her employer's computer to briefly access the Internet for personal use. Stengart worked as Executive Director for Nursing for Loving Care Agency, Inc., a home health-care and nursing services provider.

While still employed by Loving Care, Stengart anticipated filing an employment discrimination case against it. On several occasions prior to her resignation, Stengart used her company-issued laptop computer to access e-mail from her attorney via her personal, password protected Yahoo e-mail account. By that time, Loving Care had already distributed an employee handbook containing an "Electronic Communication [P]olicy" that outlined the company's policies on computer use at work. The Policy specifically provided:

The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice.

...

E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.

The principal purpose of electronic mail (e-mail) is for company business communications. Occasional personal use is permitted

The Policy further detailed types of personal use for which the internet should not be used, including "solicit[ing] for outside business ventures, charitable organizations, or for any political or religious purpose"

Despite the wording of the Policy, Stengart used the company-issued laptop computer to access her private, password protected Yahoo e-mail account. Stengart was unaware that the computer was automatically saving web-page images in a temporary internet file cache folder on the computer's hard drive. After Stengart formally resigned and returned the laptop, Loving Care had the hard drive forensically imaged and discovered files containing the content of the e-mails Stengart exchanged with her attorney.

Rather than promptly returning the e-mail to Stengart, Loving Care's attorneys concluded that she had waived privilege claims in light of Loving Care's computer use Policy, which explained that Internet use and communication were "not to be considered private or personal to any individual employee."

Believing no privilege attached, Loving Care cited one of the e-mails in an interrogatory answer. Sten-

Fernando M. Pinguelo, a trial lawyer and partner of Norris McLaughlin & Marcus, co-chairs the firm's Response to Electronic Discovery and Information group. Fernando handles a variety of cases that implicate electronic documents and their impact on lawsuits and on businesses. Notably, Fernando was involved in New Jersey's first case addressing its new electronic discovery rule amendments, and has lectured numerous times on the topic, including at the Judicial College of New Jersey. Recently, the Fulbright Program, the U.S. government's flagship international exchange program, designated Fernando a Fulbright Specialist for his work in e-discovery; and he will engage in a collaborative project at Mackenzie University in São Paulo, Brazil. He founded the award-winning *eLessons Learned* (www.eLL-blog.com), a blog focused on how technology impacts the law.

Laura J. Tyson currently handles e-discovery issues as part of a litigation team at Stern & Killcullen while she completes her law degree at Seton Hall Law School in Newark, New Jersey. Following graduation in May 2010, Laura will serve as Law Clerk to the Honorable William J. McGovern III, Superior Court, Civil Division, Sussex County, New Jersey. Before attending law school, Laura was a product specialist for Roland Corporation's digital audio recording products.

gart's attorneys immediately sought return of the e-mails, but the trial judge held for Loving Care after concluding that Stengart waived the privilege. The Appellate Division reversed, holding that preserving attorney-client privilege outweighed the employer's interest in enforcing its Policy.

High Court's Holding. On challenge to New Jersey's highest court, Loving Care argued that the attorney-client privilege did not attach to the e-mails because its company policy regarding computer and Internet use at the workplace removed any expectation of privacy that Stengart may have had; and that she waived the privilege because she accessed her e-mail via the company's computer and server.

The Supreme Court of New Jersey disagreed. After first concluding that Loving Care's Policy was "not clear" and created "ambiguity about whether personal e-mail use is company or private property," the court evaluated case law from other jurisdictions, giving particular attention to (and ultimately following) a Massachusetts case with nearly identical facts.²

Relevant Factors. The court considered factors by which an employee could be found to have a lesser expectation of privacy in attorney communications.

First, the court distinguished between the use of a company e-mail system as compared to a personal, web-based e-mail account (such as Yahoo or Gmail.)

² See *Nat'l Econ. Research Assocs. v. Evans*, Mass. Super. Ct., No. 04-2618 (2006).

E-mails transmitted via an employer's e-mail account might be subject to less privacy than those sent via a personal web-based account.

Second, the court noted that the physical location of the company's computer might make a difference in the analysis, suggesting that an employee who works from a home office may be entitled to greater privacy than an employee whose communication is made via the company's servers.

Third, the court recognized that other jurisdictions have held that the existence of a clear company policy that prohibits personal computer use may diminish an employee's expectation of privacy; but, as explained below, the New Jersey Court refused to consider the sufficiency of a company policy as a determination of whether the employer can pierce the attorney-client privilege.

In holding that Stengart's e-mails were protected by the attorney-client privilege because she could reasonably expect them to remain private, the court outlined three reasons.

First, the court noted that Stengart had both a subjective and an objectively reasonable expectation of privacy in the e-mails because she had used a password-protected account to access the messages and had not given her password to anyone at Loving Care.

The court also noted that Stengart had not used the computer to conduct illegal activities.

Third, the court recognized that the e-mails were clearly labeled as attorney-client communications and warned the reader that the messages were personal and confidential. (The e-mails included a paragraph warning the reader "THE INFORMATION CONTAINED IN THIS EMAIL COMMUNICATION IS INTENDED ONLY FOR THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENT NAMED ABOVE.")

Privilege Trumps Policy. Addressing Loving Care's argument that no privilege attached to Stengart's e-mails because Stengart "brought a third person into the conversation from the start—watching over her shoulder," the court explained that the "Policy did not give Stengart, or a reasonable person in her position, cause to anticipate that Loving Care would be peering over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account."

In fact, the effectiveness of Loving Care's Policy was not dispositive. As noted above, the court determined that the Policy was ambiguous, lacked clarity, and failed to warn employees that even web-based e-mails could be forensically retrieved. But, as the court explained, even if the Policy were perfectly drafted, it would not be enough to pierce the attorney-client privilege:

[E]mployers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy. . . . [E]ven a more clearly written company manual—that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney client communications, if accessed on a personal, password protected e-mail account using the company's computer system—would not be enforceable.

Declining to rely on other states' case law holding that a clear company policy banning personal e-mails could diminish an employee's expectation of privacy in attorney-client communications, the court added that a

"zero-tolerance policy can be unworkable and unworkable in today's dynamic and mobile workforce and [we] do not seek to encourage that approach in any way."

Implications of Ruling on Workplace Practices. The court's ruling does not mean that employers cannot monitor or regulate Internet use in the workplace. The court made it clear that employers may still establish and enforce workplace policies relating to computer use. Indeed, an employer may "discipline employees and, when appropriate, terminate them, for violating proper workplace rules . . ." But it cannot use a workplace violation as a reason to pierce an employee's attorney-client privilege.

Ethical Considerations. The *Stengart* court also considered whether Loving Care's attorneys violated professional ethics rules. New Jersey's Rules of Professional Conduct prohibits a lawyer from reading a document that the lawyer has a reasonable cause to believe was disclosed inadvertently.³ The court ruled that the attorneys were at fault for "not setting aside the arguably privileged messages once [they] realized they were attorney-client communications" and by "failing either to notify [their] adversary or seek court permission before reading further." Noting the absence of an appearance of bad faith, the Court reiterated that the attorneys "should have promptly notified opposing counsel when it discovered the nature of the e-mails."

Does Technology Defeat Privacy? The Future of Workplace Privacy The court's holding in *Stengart* depended heavily on its recognition that "[i]n the modern workplace . . . occasional, personal use of the Internet is commonplace." But its holding was limited to finding a privacy in attorney-client communications. *Stengart* did not address whether the contents of other types of highly confidential communications found in personal e-mails might be off-limits to an employer in light of an ambiguous employee policy, or whether a reasonable expectation of privacy attaches to communications that are simply marked "personal" or "confidential" that an employee accesses while at work via a personal password protected web site. Does simply labeling an e-mail communication as "confidential" and only using a password protected personal web-based e-mail account to access it from work prevent an employer from reading its contents?

Additionally, *Stengart* involved only conduct by private—not state—actors; thus Fourth Amendment protections were not implicated. Yet it is not likely that the New Jersey Supreme Court would allow government employers to more easily overcome the attorney-client privilege (and Fourth Amendment privacy protections) in order to read the contents of a privileged communication sent or received via a government employer's computer.

Although the United States Supreme Court has ruled that government employers may conduct warrantless searches for work-related purposes or because of work-related misconduct, even where the employee retains a

³ See RPC 4.4(b) ("A lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender.").

reasonable expectation of privacy,⁴ the New Jersey Supreme Court would be more likely to provide citizens with broader privacy protections. And a pending ruling from the U.S. Supreme Court⁵ could potentially throw a wrench into the whole mix. In a case that does not in-

⁴ *O'Connor v. Ortega*, 480 U.S. 709, 725–26 (1987).

⁵ See *City of Ontario v. Quon*, 130 S. Ct. 1011 (2009) (granting a writ of certiorari to review the Ninth Circuit's decision in

volve attorney-client privilege, the Supreme Court will soon answer the question of whether a government employer is required to use less intrusive methods when reviewing the contents of an employee's private text messages sent using a employer-issued pager.

Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008)).