New Jersey Supreme Court Limits Employer's Review of Emails Sent Using Company Laptop

By Suhna Pierce and Christine Lyon

Does an employee have a reasonable expectation of privacy when accessing her personal, web-based email account from a company-owned computer? In *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court held that an employee could reasonably expect that emails she exchanged with her attorney via her personal Yahoo! Mail account using a company laptop would remain private.[1] This case demonstrates that public policy concerns may outweigh an employer's right to review some email communications sent using company computers, and provides important guidance to U.S. employers for drafting technology use policies.

Background

This case arose from a lawsuit filed by Marina Stengart against her former employer, Loving Care Agency, Inc. ("Loving Care"). In preparing to defend against Ms. Stengart's claims, Loving Care created a forensic image of the hard drive of the company laptop that had been assigned to her. This forensic image showed the contents of seven or eight email messages that Ms. Stengart had exchanged with her attorney, using her personal, web-based Yahoo! email account. While Ms. Stengart had wisely refrained from using her company email account to correspond with her attorney, she had used her company laptop to log in to her Yahoo! account to access and transmit these messages. Without her knowledge, the web browser of her company laptop had automatically saved a copy of Internet pages she viewed to a "cached" folder of temporary Internet files on the hard drive. As a result, these files were later viewable to Loving Care and its counsel.

Ms. Stengart's counsel objected to Loving Care's inspection and use of these email messages, based on the attorney-client privilege. In response, Loving Care argued that the email messages were not protected by the privilege because Ms. Stengart had no reasonable expectation of privacy in files on a company-owned computer, given Loving Care's written policy that it may access "all matters on the company's media systems and services at any time." The trial court agreed with Loving Care, but the Appellate Division reversed, finding that ambiguous language in the electronic communications policy supported a reasonable expectation of privacy in personal emails sent on a company computer.[2] The Appellate Division also concluded that Loving Care's counsel had violated professional conduct rules by failing to alert Ms. Stengart's attorneys that it possessed the email messages before reading them. The New Jersey Supreme Court agreed to hear the case on appeal.

The New Jersey Supreme Court's Decision

On March 30, 2010, the New Jersey Supreme Court affirmed the Appellate Division, holding that Ms. Stengart had a reasonable expectation of privacy in emails she exchanged with her lawyer using her personal, web-based account, and that Loving Care's counsel consequently violated the attorney-client privilege by reading the messages. An employee's expectation of privacy is reasonable, the court said, if she

Beijing

Paul D. McKenzie	86 10 5909 3366
Jingxiao Fang	86 10 5909 3382

Brussels

Karin Retzer	32 2 340 7364
Teresa V. Basile	32 2 340 7366
Antonio Seabra Ferreira	32 2 340 7367

Hong Kong

Gordon A. Milner	852 2585 0808
Nigel C.H. Stamp	852 2585 0888

Los Angeles

Mark T. Gillett	(213) 892-5289
Michael C. Cohen	(213) 892-5404
David F. McDowell	(213) 892-5383
Russell G. Weiss	(213) 892-5640

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Chris Coulter	44 20 7920 4012
Suzanne Horne	44 20 7920 4014

New York

Gabriel E. Meister	(212) 468-8181
Joan P. Warrington	(212) 506-7307
John F. Delaney	(212) 468-8040
Madhavi T. Batliboi	(212) 336-5181
Marian A. Waldmann	(212) 336-4230
Michiko Ito Crampe	(212) 468-8028
Miriam Wugmeister	(212) 506-7213
Sherman W. Kahn	(212) 468-8023

Northern Virginia

Daniel P. Westman	(703) 760-7795
Timothy G. Verrall	(703) 760-7306

Palo Alto

Bryan Wilson	(650) 813-5603
Christine E. Lyon	(650) 813-5770

San Francisco

Roland E. Brandel	(415) 268-7093
James McGuire	(415) 268-7013
William L. Stern	(415) 268-7637
Jim McCabe	(415) 268-7011

San Diego

Mark R. Wicker	(858) 720-7918

Tokyo

Daniel P. Levison	81 3 3214 6717
Jay Ponazecki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

Washington, D.C.

Andrew M. Smith	(202) 887-1558
Cynthia J. Rich	(202) 778-1652
Julie O'Neill	(202) 887-8764
Nathan David Taylor	(202) 778-1644
Obrea O. Poindexter	(202) 887-8741
Oliver I. Ireland	(202) 778-1614
Reed Freeman	(202) 887-6948
Richard Fischer	(202) 887-1566

subjectively expects her email communications to be private and if that expectation is objectively reasonable. Two principal concerns informed the court's subjective-objective analysis: (1) whether Loving Care's electronic communications policy provided sufficient notice that it covers personal, web-based emails; and (2) how the nature of the emails affects the balance between Stengart's interest in privacy and Loving Care's interest in inspecting messages stored on its systems.[3] To evaluate these concerns, the court considered factors that other jurisdictions had deemed relevant under similar facts, including: whether the employer's technology use policy explicitly warns or implicitly suggests that it covers personal, web-based accounts; whether the employee is aware of monitoring policies; whether the privacy claim involves illegal or inappropriate information that could harm the employer; whether the messages were transmitted using the employer's email system, as compared with the employee's personal, web-based account; and whether the computer was located in the employer's facilities or in the employee's home.[4]

The court found that Ms. Stengart met both the subjective and objective components of its privacy analysis. She had a subjective expectation of privacy because she took steps to ensure that the emails remained private, such as using her personal, web-based email account rather than Loving Care's email system, and not saving her ID and password on the laptop. Moreover, the court found her expectation of privacy to be objectively reasonable, concluding that Loving Care's policy failed to put Stengart on notice that her Yahoo! emails could be monitored and read, and because of the important public policy reasons for protecting privileged communications.[5] In light of the important public policy concerns behind privileging attorney-client communications, the court noted that even a technology use policy that unambiguously reserves the right for the employer to retrieve and read an employee's attorney-client communications with her attorney, accessed on her personal, web-based email account via the company's computer, would not be enforceable.[6]

Because of the steps Ms. Stengart took to keep her emails private, the shortcomings in Loving Care's electronic communications policy, and the public policy behind privileging attorney-client communications, the court held that Ms. Stengart's expectation of privacy was reasonable. The court further held that, once Loving Care's counsel identified the messages as potential attorney-client communications, they were obligated to notify Ms. Stengart's attorney that they possessed the emails or to seek court permission before reading further. By reading the emails, Loving Care's counsel was found to have violated New Jersey's rules of professional conduct.

THE NEW JERSEY SUPREME COURT CLARIFIED THAT ITS DECISION "DOES NOT MEAN THAT EMPLOYERS CANNOT MONITOR OR REGULATE THE USE OF WORKPLACE COMPUTERS."

Although the court did not expressly address non-privileged personal emails accessed and sent on company computers, its analysis implies that these messages may be afforded less protection.[7] In *Stengart*, the strong public policy reasons for protecting confidential attorney-client communications are given significant weight in balancing Ms. Stengart's interests against those of Loving Care.

In addition, the New Jersey Supreme Court noted that "courts might treat e-mails transmitted via an employer's e-mail account differently than they would web-based e-mails sent on the same computer."[8] While observing that some courts have attributed a "lesser expectation of privacy" to employees who communicate with their attorneys over company email, the court refrained from addressing how it would rule in such a case.[9]

Practical Implications for Employers

The New Jersey Supreme Court clarified that its decision "does not mean that employers cannot monitor or regulate the use of workplace computers."[10] *Stengart* confirms that a company can adopt and enforce technology use policies to protect its "assets, reputation, and productivity."[11] In light of this decision and evolving technology, U.S. employers should revisit their technology use policies to ensure they are current, considering the following:

- Technology use policies should accurately reflect your company's own monitoring practices. Your IT personnel may be a source of valuable input about the types of data that may be captured or stored by your company's computer systems. This information can help to identify other practices that may be appropriate to address in your policies.
- *Stengart* demonstrates the importance of providing sufficient detail about monitoring practices, so that employees can regulate their conduct accordingly. For instance, you will

want to consider explaining that website content accessed via company computers may be stored on the company's technology resources, and that these stored copies are subject to monitoring. Personal, web-based email accounts are one example, but the same issue may arise with other web-based content that an employee accesses using a company computer (*e.g.,* online accounts, external blogs or social media pages, etc.)

- Employers should maintain a clearly-stated policy that messages sent or received via the company's email system are subject to monitoring, in accordance with applicable law.
- Attorney-client privileged communications require special care. If you discover potential attorney-client communications between an employee and his or her personal attorney, consult with legal counsel about your potential obligations in that particular jurisdiction.
- Remember that monitoring of employee email or computer usage is subject to very different privacy regimes outside of the U.S.[12] Technology use policies and monitoring practices need to comply with the local requirements of the countries in which your company operates. ■

1 *Stengart v. Loving Care Agency, Inc.*, 2010 N.J. LEXIS 241 (N.J. Mar. 30, 2010).

2 *Stengart v. Loving Care Agency, Inc.*, 408 N.J. Super. 54, 973 A.2d 390 (App. Div., Jun. 26, 2009)

3 *See Stengart* at *25, *37-38.

4 *Stengart* at *30-36.

5 *Stengart* at *38.

6 First, the court noted that Loving Care's policy neither addressed the use of personal, web-based email accounts on its equipment, nor warned employees that the contents of messages sent via such accounts were stored on the hard drive and could be retrieved by the company. Not only did the policy fail to address external web-based email, the court also found the language of the policy unclear as to emails sent over the company's internal email system. Second, the court considered the nature of the messages at issue. They did not involve illegal or inappropriate activity that could put the company at risk; rather they were confidential attorney-client communications, which are "historically cloaked in privacy" for the purpose of fostering candid exchanges between client and counsel. *Stengart* at *43.

7 Whether or not an employee has a reasonable expectation of privacy in *non-privileged* communications from a personal, password-protected, web-based email service may depend on the adequacy of the employer's policy to provide notice that the content of such emails could be monitored and read. *See, e.g., Stengart* at *25-26 (finding the scope of Loving Care's written policy unclear when it failed to give employees "express notice" that personal, web-based accounts were subject to monitoring). The employer's reasons for accessing the emails may also be relevant. *See Stengart* at *30-31 (discussing New Jersey cases where courts rejected privacy claims based on employers' investigation of employees' use of company computers in illegal activity); *Stengart* at *44-45 (contrasting Loving Care's lack of "bad faith" in its "legitimate[ ] attempt[ ] to preserve evidence" with a scenario in which an employer might "hack into [an employee's] personal account," "maliciously seek out attorney-client documents," and "rummage through an employee's personal files out of idle curiosity"). The court did not expressly reach this issue in its decision, however.

8 *Stengart* at *35.

9 *Stengart* at *34.

10 *Stengart* at *42.

11 *Id.*

12 Examples of restrictions on employee monitoring activity in other countries may be found in prior Legal Updates, including "German Data Protection Landscape is Changing" (http://www.mofo.com/German-Data-Protection-Landscape-is-Changing-07-09-2009) and "Comparing the U.S. and EU Approach to Employee Privacy" (http://www.mofo.com/pubs/xpqPublicationDetail.aspx?xpST=PubDetail&pub=8182). For more detailed information, please refer to Chapter 3, "Email and Internet Monitoring/ Video and Physical Surveillance," of GLOBAL EMPLOYEE PRIVACY AND DATA SECURITY LAW, Morrison & Foerster LLP (editors Miriam H. Wugmeister and Christine E. Lyon), BNA 2009.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, Fortune 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last six years, we've been included on *The American Lawyer*'s A-List. *Fortune* named us one of the "100 Best Companies to Work For." We are among the leaders in the profession for our longstanding commitment to pro bono work. Our lawyers share a commitment to achieving results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, 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.

www.mofo.com

©2010 Morrison & Foerster LLP