Bloomberg Law Reports® Privacy & Information

2010 Is Not *1984:* *Stengart v. Loving Care Agency, Inc.* and Cyber Privacy in the Workplace

Contributed by Brent A. Cossrow, Fisher & Phillips LLP

"There was of course no way of knowing whether you were being watched at any given moment," explained Winston Smith, the protagonist of George Orwell's masterpiece, *1984*. Smith and his fellow employees worked and lived under the assumption that every sound they made was overheard, every utterance recorded, and every movement scrutinized by their employer, a government agency. As an ever-increasing number of employers provide their employees with work-issued computers and Internet access, life appears to be imitating art. While computers, the Internet and e-mail have resulted in unprecedented efficiencies and greater ease of communication, computers record voluminous information about how they are used. This means when employees use work-issued computers for personal matters, and employers find the records of this use, employees can feel as though 2010 has become *1984*.

But looks can be deceiving, as demonstrated by one widely followed appellate decision, *Stengart v. Loving Care Agency, Inc*.[1] Awaiting a decision on further appeal to the New Jersey Supreme Court, *Stengart* involves an employee's use of a work-issued computer to access her Internet-based, password-protected personal e-mail account to communicate with her attorney about her upcoming lawsuit against her employer. This article discusses how the intermediate appellate court in *Stengart* neglected to explain and address the role of one of the computer's ordinary, default operations – the production of .html files when a web page is viewed on the computer – in recording the content of the e-mails between the employee and her attorney. Omitting this explanation created a dramatic misimpression that the employer was an Orwellian nightmare: rummaging through, prying into, and seizing its employee's most private communications. This article explains how the failure to address the role of .html files undermined the appellate court's legal analysis, and discusses how the New Jersey Supreme Court can cure this deficiency.

Employee Defection

Stengart v. Loving Care Agency, Inc. underscores the importance of understanding not only how computers work, but also the context in which these cases originate. The Petri dish of workplace cyber privacy conflicts is employee defection, where the resignation, firing, raiding, or termination of employees results in key employees

accepting new employment in competition with his or her former employer. When an employee defects, in many industries it is a best practice for the former employer to retrieve any company property that was issued to the employee. Frequently this involves retrieving documents, files, and a work-issued computer as soon as the employment is terminated.

While the rationale for retrieving work-issued computers ranges from the need to re-assign a scarce asset to another employee to taking custody of evidence of a possible crime, it is inside the hard drives of these computers that Orwell's fears spring to life – or may appear to do so. Many employers create a forensic image of the hard drive of a work-issued computer, particularly when the employer suspects the employee was involved in improper activity such as corporate espionage, trade secrets theft, or misuse of the computer to visit inappropriate websites. Evidence of such wrongdoing frequently resides on the hard drive, which can record almost every keystroke made by the employee on the computer and saves a picture of nearly every web site visited by the employee on the computer.

Stengart v. Loving Care Agency, Inc.

An employer's ability to discover how its employee used a work-issued computer is far from the total surveillance that haunted Winston Smith, and the facts at issue in *Stengart* crystallize the differences between the two scenarios.

Stengart was a director-level employee of Loving Care, which provided home care services for children and adults. Stengart resigned from Loving Care in December 2007, and within two months filed a lawsuit alleging Loving Care discriminated against her because she was a woman. Shortly after Stengart resigned, Loving Care took custody of Stengart's work-issued computer and created a forensic image of its hard drive. Investigation of the forensic image revealed that Stengart used the computer to send and receive e-mails to and from her attorney regarding Stengart's lawsuit against Loving Care. Importantly, these e-mails were sent through Stengart's private, password-protected, Internet-based Yahoo! e-mail account.

During the litigation, Loving Care disclosed that it found evidence of Stengart's communications with her attorney. Indignant that Loving Care could have obtained private and password-protected e-mails, Stengart invoked the protections of the attorney client privilege and demanded the immediate return and destruction of every e-mail. Loving Care refused, arguing Stengart waived any protection provided by using Loving Care's computer, Internet access, and servers to make the communications. Stengart responded by filing a motion that asked the trial court to order Loving Care to comply with Stengart's requests.

This motion was denied by the trial court. It noted that the forensic image of Stengart's work computer contained temporary Internet files, which contained the content of e-mails sent from Stengart's Yahoo! account. The court also observed that Loving Care implemented employment policies regarding use of Loving Care's computers and Internet connections. These policies informed Loving Care's employees that their Internet use and e-mails transmitted on work-issued computers were not private and were considered part of the company's business.

The court concluded that although communications between attorneys and their clients normally are protected by the attorney-client privilege, Loving Care's employment policies put Stengart on notice that she did not have a reasonable expectation of privacy in her Internet-based communications made through office computers. Under these circumstances, the trial court concluded, Stengart waived the protections of the privilege by choosing a method of communication with her attorney – through her work-issued computer – that carried a risk that the communications would be disclosed and found.

This holding was reversed by the appellate court. It concluded that the attorney-client privilege "substantially" outweighed the employer's interest in enforcing its employment policies. The appellate court rejected the employer's "claimed right to rummage through and retain the employee's e-mails to her attorney."[2] The appellate court also rejected the employer's argument that it owned Stengart's e-mails because the computer used to make the communications was owned by the employer. The appellate court found this problematic because Loving Care's employee policy manual allowed for "occasional personal use" of the corporate computers.[3] Given this permissive use, it did not make sense that anything flowing from the use of the computer became corporate property because it could be found on the computer. The court was especially critical of an employment practice that would essentially transform an employer's right to inspect its employee's property into a right to seize ownership of that property.

The appellate court also discussed the "gray areas," wherein an employer has a legitimate interest in accessing its employees' personal communications from a company computer – such as when an employee uses a work-issued computer to access child pornography or misappropriate company property.[4] But according to the appellate court, such interests are different from monitoring an employee's use of a work-issued computer, seizing, and claiming ownership of the employee's personal communications:

> When an employee, at work, engages in personal communications via a company computer, the company's interest – absent circumstances the same or similar to . . . [employee theft or child pornography] is not in the content of those communications; the company's legitimate interest is in the fact that the employee is engaging in business other than the company's business. Certainly, an employer may monitor whether an employee is distracted from the employer's business and may take disciplinary action if an employee engages in personal matters during work hours; that right to discipline or terminate, however, does not extend to the confiscation of the employee's personal communications. . . .
>
> We thus reject the philosophy buttressing the trial judge's ruling that, because the employer buys the employee's energies and talents during a certain portion of each workday, anything that the employee does during those hours becomes company property. . . . [T]he employer's interest in enforcing its unilateral regulations wanes when the employer attempts to reach into purely private

matters that have no bearing on the employer's legitimate interests.[5]

The Deficiencies in the Appellate Court's Opinion

The appellate court's opinion is under review by the New Jersey Supreme Court, and it has an opportunity to explain how it was the ordinary operation of the computer systems – not Stengart's employer – that compromised Stengart's expectations of privacy. But such an explanation will require the New Jersey Supreme Court to more fully address the following three deficiencies:

First, the appellate court did not explain how Stengart's private Yahoo! e-mails came to reside on Loving Care's computer. The reality is that Stengart's e-mails did not *reside* on Loving Care's computer, and the absence of this explanation is even more unusual because it was part of the trial court's record and opinion. As the trial court explained, Loving Care found temporary internet files. Any time a computer is used to access the Internet, the computer automatically creates and saves on its hard drive a separate, temporary file for each web page that a person views. Each temporary file, known as an .html file, is a copy of each web page visited. These .html files are created by standard software that is part of the computer's operating system. These files are not the result of surveillance or monitoring initiated by an employer – it is simply how computers work.

In the case of Internet-based e-mail accounts, the .html file will contain the content of any e-mail viewed on the computer. And the process that creates and saves .html files does not have a content filter. In other words, no matter how private or confidential the content of the e-mail that one drafts on his or her Internet-based personal e-mail account, the computer on which it was viewed will create and save an .html file that records the e-mail's content. The .html files will remain on the computer's hard drive unless they are intentionally deleted or overwritten through the subsequent use of the computer. Thus, as a result of the computer's ordinary operation, the content of a person's most private communications can be stored on a separate and routinely created file that could be just a click away from anyone who uses the computer on which the Internet-based e-mail was viewed. It should be noted that this phenomenon is hardly a secret: the risk of losing privacy of e-mail on a computer that others can access is a staple of online privacy discussions and advice.[6]

The absence of any explanation of the role of .html files from the appellate court's opinion has profound implications for the appellate court's analysis, Stengart's privacy rights, and the attorney-client privilege. While Stengart undeniably has an expectation of privacy in the e-mails she sent to and received from her attorney, there are legitimate questions as to what extent Stengart had any expectation of privacy in the .html files. Significantly, Loving Care never obtained the e-mails between Stengart and her attorney. Loving Care obtained only the .html files created by the computer, which contained images of the content of Stengart's e-mails. And the .html files are not communications between an attorney and its client; the .html files are evidence of such communications – they are copies. The appellate court concluded that Stengart's decision to use her private, password protected, Internet based e-mail account reflected Stengart's intent to protect the privacy of the e-mails with her attorney. This begs the question that the appellate court did not ask: if it is

so important that Stengart chose her Yahoo! e-mail account to protect the privacy of privileged communications from her employer, why is not equally important that Stengart used one of the only computers that would compromise the privacy she was trying to protect?

Using her employer's computer significantly increased the likelihood her employer would find copies of Stengart's e-mails to her attorney. Perhaps Stengart did not know that the computer automatically created .html files of her personal communications; or perhaps Stengart knew this full well. Either way, Stengart's understanding of .html files and their role is too important to have been omitted from the appellate court's discussion of whether she had a reasonable expectation of privacy in these communications with her attorney.

Second, the appellate court's descriptions do not accurately capture the reality of Loving Care's actions. There is a disconnect between what the trial court's opinion reveals about what Loving Care did, and how the appellate court described Loving Care's behavior. There is suggestion of the sinister, and of intentional breaking-and-entering in the descriptions: "rummage through and retain the employee's e-mails to her attorney"; "pry into and retain plaintiff's communications with her attorney"; "the confiscation of the employee's personal communications"; "reach into an employee's private life"; and "prying into an employee's private affairs."[7] The appellate court concluded, "we reject the employer's claimed right to rummage through and retain the employee's e-mails to her attorney."[8] In its most dramatic flourish, the appellate court analogized Loving Care's conduct to "reach[ing into Stengart's] pockets" and seizing her property.[9]

As a matter of advocacy, these descriptions certainly help support the appellate court's decision. But, for such a consequential opinion, they are far too removed from the actual conduct as reflected in the trial court record. Setting aside the appellate court's failure to mention that Loving Care never obtained the e-mails themselves, Loving Care did not rummage through or pry into any file, folder, compartment, container, or other package that belonged to Stengart. Loving Care did not conduct surveillance on Stengart. Loving Care did not use spy-ware or other programs to real-time monitor, hack into, or access Stengart's Yahoo! account. Indeed, Loving Care never even entered into Steingart's Yahoo! account. Nor did Loving Care open an area of the work-issued computer that Stengart had designated "personal" or "confidential." And Loving Care did not reach into Stengart's pockets — Loving Care did not have to do any of that to *see* copies of Steingart's e-mails: the .html files containing the content of Stengart's communications with her attorney were sitting in plain sight on the hard drive of Loving Care's computer because of Stengart's decision to use this computer.

Third, we cannot determine what an e-mail says until we read it. The appellate court also focused on whether the employment policy at issue – here, a policy that said any files residing on Loving Care's computer were the property of Loving Care – furthers a legitimate business interest of the employer. The appellate court acknowledged that determining whether an employee used a work computer to access child pornography or to steal corporate property would implicate a legitimate interest. But the appellate court did not explain how an employer can determine whether the employee is using the computer to steal trade secrets without investigating the employee's use of the computer. If the employee is using an

Internet-based e-mail account to steal trade secrets, this cannot be confirmed until the employer reviews e-mails, .html files, and USB registries. But according to the appellate court, if during the course of such a review, the employer were to find the employee's personal communications, this probably would constitute an invasion of privacy. This rule of law is unworkable, because there is no way for an employer to know whether an e-mail or .html file was created as a result of a personal communication until the e-mail or .html file has been reviewed.

2010 Is Not 1984

Another interesting aspect of the appellate court's opinion is that the stated basis for reversal was a procedural issue that did not involve Stengart's privacy rights or the attorney-client privilege. The appellate court's holding was that the trial court committed reversible error by failing to hold hearings on what the appellate court believed was conflicting evidence (none of which concerned .html files). So the reality is that it probably was not even necessary to invoke the specter of an Orwellian workplace here – regardless of whether it really existed or not. This leaves open the possibility that the New Jersey Supreme Court could chose to narrowly decide the appeal, by vacating the appellate court's opinion and remanding the matter back to the trial court to hold hearings without addressing the cyber privacy and privilege questions that the appellate court ruled on in dicta.

Such a narrow decision would be unfortunate. *Stengart* represents the rare opportunity for a state's supreme court to define the difference between a client's Internet-based e-mails to her attorney and the .html files created by the computer used to send these e-mails. Hopefully, the New Jersey Supreme Court's opinion will determine whether an employee like Stengart has a reasonable expectation of privacy in these .html files. Such a ruling would help both employers and employees to better understand the cyber privacy boundaries in the workplace, and demonstrate the importance of knowing how computers operate.

New Jersey Supreme Court Finds Reasonable Expectation of Privacy in E-mails

On March 30, 2010, the New Jersey Supreme Court unanimously affirmed the appellate court's holding that Stengart had a reasonable expectation of privacy in her e-mails to and from her attorney. The Supreme Court held that Stengart could reasonably expect that the e-mails sent and received through her personal, password protected Yahoo! account would remain private, and that sending and receiving them via the employer's company laptop did not waive the protection of the attorney-client privilege. The Supreme Court recognized employers can monitor and regulate their employees' use of work-issued computers, but concluded that employers "have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy."[10]

Brent A. Cossrow is an attorney with Fisher & Phillips LLP, a national labor and employment law firm. He can be reached at bcossrow@laborlawyers.com

---

1 408 N.J. Super. 54, 973 A.2d 390 (Super. Ct. App. Div. 2009).
2 *Id.* at 59.
3 *Id.* at 60.

[4] *Id.* at 70.

[5] *Id.* at 72–73.

[6] *See, e.g.*, Microsoft Online Safety: 5 Safety Tips for Using a Public Computer, available at www.microsoft.com/protect/mobile/public/publicpc.aspx (last visited Mar. 24, 2010); Kris Littlejohn, "10 things you should do to protect yourself on a public computer," *TechRepublic*, available at http://blogs.techrepublic.com.com/10things/?p=322 (last visited Mar. 24, 2010).

[7] *Stengart*, 408 N.J. Super at 59, 60, 72, 73.

[8] *Id.* at 59.

[9] *Id.* at 69.

[10] *Stengart v. Loving Care Agency, Inc.*, No. A-16 September Term 2009, 2010 BL 69532 at 28 (N.J. Mar. 30, 2010).