ARTICLE

EMERGING WORKPLACE PRIVACY RIGHTS AND THE IMPLICATIONS FOR LITIGATORS

David Chaumette[*]
Brian A. Schaffer[**]

TABLE OF CONTENTS

---

* David A. Chaumette is a named partner of the boutique litigation law firm, De la Rosa and Chaumette. Mr. Chaumette represents corporations in numerous industries on litigation matters pending across the United States. Those matters have included oil and gas, securities, software licensing, and employment-related disputes. He has tried several cases to jury verdict and he has prosecuted appeals. Mr. Chaumette is also a leading lawyer on issues related to electronic discovery and data management.

** Brian A. Schaffer is an associate with De la Rosa and Chaumette. Mr. Schaffer specializes in complex commercial litigation, labor and employment matters, corporate law, and profesional responsbilitity issues.

I. INTRODUCTION

Typically, an employer has broad discretion to "invade" a worker's "privacy" in the workplace. An employer generally has the right to monitor the worker's communications (traditionally by e-mail or telephone), especially when the means of communication is supplied by the employer and the nature of the communication is work related.

However, is the employer's broad discretion to monitor communication limited when a worker uses her personal, web-based Internet e-mail account? Does the analysis change if the communication would otherwise be privileged, as between the employee and her lawyer? What if the nature of the communication is about a potential lawsuit the employee wants to bring against her employer? And does it matter if such communication was done on company time and with company equipment?

These are the questions addressed recently by the New Jersey Supreme Court in *Stengart v. Loving Care Agency, Inc.*[1] This Article takes the position that, at least in New Jersey, an employer cannot rely upon its electronic communications policy to justify reviewing the content of an employee's personal e-mail, even when stored on the employer's electronic resources—at least when it is arguably a privileged, private, or personal communication. Paradoxically, this Article suggests that social networking sites (such as Facebook, MySpace, Twitter, and LinkedIn) are open to review by an employer.

Part II of this Article will explore the general right of an employer to review an employee's communication. Part III then explores the competing expectation of privacy in the workplace. Part IV reviews how an employer may learn of employee communication through e-discovery and other means. Part V then reviews the recent case law addressing the tension between

1. Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

monitoring or discovering "private" communications occurring in the workplace and workplace "privacy." Part VI addresses the ethical constraints that lawyers may have in probing too deeply for ostensibly privileged communications, even though the communication was made in the workplace. Last, Part VII proposes how an employer should structure its electronic communications policy to avoid running afoul of invasion of privacy or ethics complaints.

II. AN EMPLOYER'S RIGHT TO REVIEW EMPLOYEE COMMUNICATION

In general, an employee should not expect to have much privacy in the workplace, especially if the company has an electronic communications policy that notifies the workforce that its communications may be monitored or otherwise discovered.[2] This is particularly the case when the communications are work related, made during work time, and while using company equipment.[3] However, new technology has increased the tension between an employer's right to monitor employee communications created using company equipment and an employee's intrinsic right to privacy in personal communications.

Much of the debate centers on the definition of "electronic communication" and which means of communication fall within the purview of an employer to monitor. For instance, there is the quintessential computer–server communication—e-mail. There seems to be no debate that e-mails created on a company's computer and transmitted over the company's network are subject to monitoring and discovery.[4] We will see in our review of *Stengart*, though, that an employer's purview to monitor becomes murky when that employee sends e-mail

---

2. *See* O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (noting that an employee's expectation of privacy "may be reduced by virtue of actual office practices and procedures or by legitimate regulation").

3. *See, e.g.*, Alamar Ranch, L.L.C. v. County of Boise, No. CV-09-004-S-BLW, 2009 WL 3669741, at *3 (D. Idaho Nov. 2, 2009) (citing Kaufman v. SunGard Inv. Sys., No. 05-cv-1236, 2006 WL 1307882, at *4 (D.N.J. May 10, 2006); Thygeson v. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at *21 (D. Or. Sept. 15, 2004)) (listing cases in which prior courts ruled in favor of employers where the files in question were stored on office computers or the communication was made over the work e-mail system); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 440 (N.Y. Sup. Ct. 2007) ("[T]he effect of an employer e-mail policy . . . is to have the employer looking over your shoulder each time you send an e-mail.").

4. *See Stengart*, 990 A.2d at 662 (reviewing several cases that found employees should have a "lesser expectation of privacy when . . . using a company e-mail system").

using her company-issued computer through her personal, password-protected, web-based e-mail account.

Next, there are Internet-based social networking sites, such as Facebook, MySpace, Twitter, and LinkedIn. As more individuals and businesses tap into these sites, the line between professional and personal networking becomes more blurred. Generally, employees have no reasonable expectation of privacy in publicly available material. However, there are no bright-line rules for situations in which an employee has used her sites' privacy settings to restrict public access or she has used a nonwork computer.

Then, there are third-party mobile phone platforms, such as text messaging. Typically, these are seen as personal communications. But what if the messages are sent using devices purchased by the employer for business use? Alternatively, what if the messages are sent using devices purchased by the individual but "synced" with the workplace system to provide a seamless transition between personal and business use?

As noted in the discussion below, all the cases involving employee use of e-mail and text messaging have different nuances. There has yet to be a broad ruling on the scope of employee privacy expectations in the use of employer equipment.[5] However, the single most important component in determining an employer's right to review and use an employee's information is notice to the workforce that when using company equipment, their activities—whether social or work related—are subject to review.

III. THE SPECIAL NATURE OF ATTORNEY–CLIENT COMMUNICATION

The attorney–client privilege prevents disclosure of confidential communications between an attorney and a client that are made for the purpose of seeking or rendering legal services.[6] The protections afforded by the privilege are intended to "encourage full and frank communication" between an attorney and her client.[7]

---

5. *See* Donald H. Nichols, *Window Peeping in the Workplace: A Look into Employee Privacy in a Technological Era*, 27 WM. MITCHELL L. REV. 1587, 1595–96 (2001) (characterizing *Ortega* as "the leading Supreme Court decision" regarding employer liability for monitoring employee e-mail).

6. *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (describing "sound legal advice or advocacy" as part of the "confidential communications" protected by attorney–client privilege).

7. *Id.*

In 1999, the American Bar Association Standing Committee on Ethics and Professional Responsibility issued a formal opinion providing that unencrypted e-mail sent through the Internet was an acceptable means of transmitting confidential information.[8] The Committee reasoned that the Internet afforded the same reasonable expectation of privacy as any other mode of communication. However, the Committee's opinion was rendered before the expansion of technology that took place after the new century. In particular, the opinion did not contemplate an employer's ability to monitor the transmission of e-mail communications through a third party's e-mail system.[9]

Drawing the line between those communications deemed privileged and those subject to disclosure becomes even more difficult when information contained in a group of e-mails serves business, legal, and personal purposes. Disclosure to a third party who lacks a common legal interest with the party asserting the privilege may be construed as a voluntary waiver of the privilege. The recent court decisions discussed below require that lawyers regard the methods and means for client communication with a heightened sense of scrutiny.

IV. E-DISCOVERY

The Federal Rules of Civil Procedure provide that all relevant, nonprivileged, electronically stored information may be subject to a discovery request.[10] The reference to electronically stored information includes any data or data compilations, stored in any medium. Many employers create a forensic image of the hard drive of a work-issued computer to preserve potential evidence in litigation. This is particularly so when the employer suspects that the employee has been 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 saves a picture of nearly every website visited by the employee on the computer.[11]

Any time a computer is used to access the Internet, the computer automatically creates and saves on its hard drive a

---

8. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).
9. *See id.*
10. FED. R. CIV. P. 34(a).
11. *See* Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 393 (N.J. Super. Ct. App. Div. 2009).

separate, temporary file for each web page that a person views.[12] Each temporary file, known as a .html file, is a copy of the web page visited. These .html files are created by standard software that is part of the computer's operating system. In the case of Internet-based e-mail accounts, the .html file will contain the content of any e-mail viewed on the computer.[13] 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.[14] Thus, as a result of the computer's ordinary operation, the content of a person's "private" communications is stored on a separate and routinely created file. By using the employer's computer, the employee, therefore, significantly increases the likelihood that the employer will find the employee's communications, particularly when litigation ensues and the employer has an obligation to preserve and collect electronically stored information. The cases analyzed in Part V attempt to address the competing interests between an employer's right to discover and use such information in litigation and an employee's expectation of privacy in the workplace.

V. WHAT THE COURTS ARE SAYING ABOUT THESE ISSUES

A. In re Asia Global Crossing, Ltd.

In *In re Asia Global Crossing*, several executives used their employer's e-mail system to communicate with their personal attorney concerning actual or potential litigation with the employer, who owned the e-mail system.[15] These e-mails were left behind on the company's e-mail servers subsequent to the employees' departure from the company.[16] Because a bankruptcy trustee sought discovery of these e-mails, the court had to decide whether the employees' use of the company e-mail system to communicate with their personal attorney destroyed the attorney–client privilege.[17]

The court began with an analysis of the confidentiality of

---

12. Rebecca Michaels, *The Insufficiency of Possession in Prohibition of Child Pornography Statutes: Why Viewing a Crime Scene Should Be Criminal*, 30 W. NEW ENG. L. REV. 817, 833 (2008).

13. Bill Nelson, AMELIA PHILLIPS & CHRISTOPHER STEWART, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS 466 (3d ed. 2010).

14. Michaels, *supra* note 12, at 833.

15. *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 252, 256 (Bankr. S.D.N.Y. 2005).

16. *Id.* at 252.

17. *Id.* at 253, 256, 258–61.

e-mail communication in general, noting that "[a]lthough e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, the prevailing view is that lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy."[18] Because the court could not locate any decisions discussing the confidentiality of an employee's e-mail in the context of the attorney–client privilege, the court looked to case law pertaining to an "employee's expectation of privacy in his office computer and the company e-mail system" for guidance.[19] In making this determination, the court considered four factors:

> (1) [D]oes the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[20]

With respect to access, the court found that anyone who had lawful access to the company's e-mail system could read the employees' e-mails because they were sent over the system and were stored on the company's server.[21] With respect to the other factors, however, "[t]he evidence [was] equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring employee e-mails."[22] Therefore, the court was unable to determine as a matter of law whether the employees' use of the company e-mail system to communicate with their attorney eliminated any existing attorney–client privilege, and thus the trustee was not entitled to the e-mails.[23]

B. Curto v. Medical World Communications, Inc.

In *Curto v. Medical World Communications, Inc.*, an employee was assigned company-owned equipment by her employer to use in the employee's home office for business purposes.[24] After the employee was terminated, the employer

---

18. *Id.* at 256.
19. *Id.*
20. *Id.* at 257.
21. *Id.* at 259.
22. *Id.*
23. *Id.* at 261.
24. Curto v. Med. World Commc'ns, Inc., 99 Fair Empl. Prac. Cas. (BNA) 298, 299 (2006).

hired a forensic consultant to inspect the computer. The consultant restored portions of the computer files and e-mails that the employee had attempted to delete. Some of these documents were communications between the employee and her attorney. In discovery, employer's counsel produced these documents to employee's counsel, who claimed that these documents were subject to the attorney–client privilege and must be returned to the employee.

The court recognized that (1) the company had a computer usage policy that prohibited the personal use of company computers, (2) the employee signed a handbook containing the policy, and (3) the employee used the computer for personal matters regardless.[25] "[However,] this did 'not end the issue' because the lack of [the company's] enforcement . . . of its computer usage policy created a 'false sense of security' which 'lull[ed]' employees into believing that the policy would not be enforced."[26] Moreover, the court noted that the employee took "reasonable precautions to prevent inadvertent disclosure" by sending the e-mail using her personal AOL account, which did not go through the company's servers.[27]

The court's holding appears to be "limited to the question of whether an employee's personal use of a company-owned computer in her home waives any applicable attorney–client privilege . . . that may attach to the employee's computer files and/or e-mails."[28] The court answered that the privilege is not waived in this scenario. However, the decision "does not purport to address an employee's right to privacy in an office computer in general."[29] In fact, the lesson of *Asia Global* and *Curto* appears to be that each case should be given an individualized look to see if the party requesting the protection of the privilege was reasonable in its actions.[30]

C. National Economic Research Associates, Inc. v. Evans

In *National Economic Research Associates, Inc. v. Evans*, an employee communicated with his attorney regarding his

---

25. *Id.*
26. *Id.* (third alteration in original) (quoting Jan. 18, 2006 Order).
27. *Id.* at 301.
28. *Id.* at 305.
29. *Id.*
30. *See* O'Connor v. Ortega, 480 U.S. 709, 718 (1987) ("Given the great variety of work environments . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.").

impending departure from his company.[31] "Many of these attorney–client communications were conducted by e-mail, with [the employee] sending and receiving e-mails from his personal, password-protected e-mail account with Yahoo rather than his [company] e-mail address."[32] However, the employee often used the computer issued to him by the company, which recorded the messages on its hard drive. After the employee's resignation, the company hired a computer forensic expert to search the hard drive of the computer.[33] The expert retrieved from the hard drive various attorney–client communications between the employee and his attorney.

The company's employee manual permitted personal use of e-mail but warned that computer resources were the property of the company, that e-mails were not confidential, and that these messages could be read during routine checks. However, the court noted that "the Manual did not expressly declare, or even implicitly suggest, that [the company could or] would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet."[34] Nor did the manual warn the workforce that "the content of such Internet e-mail communications is stored on the hard [drive] of a [company]-issued computer" and can, therefore, be read by the company. Therefore, the court denied the company's application to allow disclosure of the e-mail recovered by the forensic expert because the court found the employee's expectation of privacy in e-mail communication with his attorney to be reasonable.[35]

The court rendered the following advice to employers:

> The bottom line is that, if an employer wishes to read an employee's attorney–client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, the employer must plainly communicate to the employee that:
>
> 1. all such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and

---

31. Nat'l Econ. Research Assocs., Inc. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, at *1 (Mass. Super. Ct. Aug. 3, 2006).

32. *Id.*

33. *Id.* at *2.

34. *Id.* at *3.

35. *See id.* at *4 (finding that the e-mail communications were "protected by the attorney–client privilege").

> 2. the company expressly reserves the right to retrieve those temporary files and read them.
>
> Only after receiving such clear guidance can employees fairly be expected to understand that their reasonable expectation in the privacy of these attorney–client communications has been compromised by the employer.[36]

D. Scott v. Beth Israel Medical Center Inc.

The plaintiff in *Scott v. Beth Israel Medical Center Inc.*, a former employee of a medical center, moved the court for a protective order requiring the medical center to return all e-mail correspondence between the plaintiff and his attorney.[37] The e-mails in question were written using the e-mail account assigned to the employee by the medical center and were sent using the medical center's e-mail server.[38] In addition, the medical center's e-mail policy provided that employees were forbidden from using the e-mail system for non-business-related, personal reasons; that employees had no privacy right to e-mail sent using the medical center's e-mail system; and that the medical center retained the right to access or disclose any e-mail sent or received, at any time, without notice.

The *Scott* court used the test created in *Asia Global* to render its decision.[39] The court concluded that the medical center's policy clearly banned personal use of the center's electronic resources and that this prohibition was communicated to the plaintiff and enforced by the center.

Thus, this case is distinguishable from the cases previously cited because the medical center's policy was abundantly clear—the plaintiff had no reasonable expectation of privacy in any e-mail communication using company electronic resources.[40] The court actually held that the attorney–client privilege never came into existence because—as provided in the medical center's policy—the plaintiff had no reason to expect that personal e-mail would remain confidential.[41]

---

36. *Id.* at *5.
37. Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 438 (N.Y. Sup. Ct. 2007).
38. *Id.* at 439.
39. *Id.* at 441–43.
40. *Id.*
41. *See id.* at 444 (concluding that the attorney's notice of confidentiality within the text of an e-mail "might be sufficient to protect a privilege if one existed").

E. Convertino v. U.S. Department of Justice

In *Convertino v. U.S. Department of Justice*, the plaintiff used his DOJ-provided e-mail account to communicate with his private counsel.[42] The DOJ obtained these e-mails from its e-mail server. The plaintiff then claimed an attorney–client privilege over the documents. The court first concluded that the plaintiff's disclosure of the e-mail communication was "inadvertent."[43] The plaintiff did not intend to allow the DOJ to read the e-mails that he was sending to his personal attorney, despite their transmission through the Department's e-mail system. The court noted that the DOJ's policy did not ban personal use of the Department's electronic resources.[44] Last, although the DOJ had access to personal e-mail sent using the Department-supplied e-mail account, the plaintiff was unaware that the Department could—or would—access and retain these e-mails. Therefore, the court ruled that the plaintiff had a reasonable expectation that the e-mail communication with his personal attorney would be confidential.[45]

F. City of Ontario v. Quon

Everyone with an interest in the topic of this Article expected the U.S. Supreme Court to provide clear parameters on the scope of employee privacy expectations in the use of employer equipment in *City of Ontario v. Quon*.[46] However, the Court declined to make a broad ruling and it merely affirmed that employers have a right to conduct reasonable searches in furtherance of legitimate workplace objectives.[47] The Court determined that any broader ruling would be premature because society's expectation of privacy in technology is still evolving.[48]

In *Quon*, the Ontario Police Department outfitted its officers with pagers equipped with text messaging capability for work-related use.[49] Quon, a police officer, spent a significant amount of time sending sexually explicit text messages to his wife and girlfriend.[50] Department policy did not specifically

---

42. Convertino v. U.S. Dep't of Justice, 674 F. Supp. 2d 97, 108 (D.D.C. 2009).
43. *Id.* at 109.
44. *Id.* at 110.
45. *Id.*
46. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
47. *Id.* at 2630–32.
48. *Id.* at 2629–30.
49. *Id.* at 2625.
50. *Id.* at 2626.

address text messages, but the Department had a detailed policy regarding e-mail use.[51] The Department's e-mail policy gave the Department the right to monitor and log all network activity—including e-mail and Internet use—and prohibited inappropriate or suggestive language. The Department issued a memorandum advising its officers that the e-mail policy applied to the text messages sent by officers. In performing an internal audit of the Department's text message use to determine whether the Department was properly using the system, the Department sought copies of the text messages from the service provider, who turned over text messages sent by Quon.[52] Upon review of the text messages, the Department disciplined Quon for the inappropriate nature of the messages.

Although the Court recognized that the case touched issues of far-reaching significance, the Court concluded that it could resolve the case by settled principles to determining when a search is reasonable.[53] The Court avoided the critical privacy issue by assuming arguendo that Quon had a reasonable expectation of privacy.[54] In dicta, the Court opined on Quon's privacy expectation:

> Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.
>
> [E]mployer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.[55]

Ultimately, the Court determined that the Department had not violated Quon's Fourth Amendment rights, primarily because the Department had a legitimate purpose behind its investigation of the police officers' text messages and because

---

51. *Id.* at 2625.
52. *Id.* at 2626.
53. *Id.* at 2624.
54. *Id.* at 2630.
55. *Id.* at 2629–30.

the Department had put its officers on notice that the text messages were subject to audit.[56] The Court also observed that the kind of search conducted by the Department would be "regarded as reasonable and normal in the private-employer context" as well.[57]

G. Stengart v. Loving Care Agency

In *Stengart*, the New Jersey Supreme Court looked at many of the same factors as the *Quon* Court in concluding that an employee's right to confidential communications with her attorney was preserved, notwithstanding the employer's recovery of e-mail communications between the employee and her attorney from a laptop that the employer provided to the employee.[58] Many commentators have focused on the attorney–client privilege issue.[59] However, the *Stengart* decision is significant beyond the privilege issue because of what it says about employer policies and about an attorney's ethical obligations during discovery. As such, *Stengart* deserves close scrutiny.

Stengart was a director-level employee of Loving Care, a provider of home-care services.[60] Stengart resigned from Loving Care in December 2007, and within two months she filed a lawsuit alleging sex discrimination against the company.[61] Shortly after Stengart resigned, Loving Care took custody of Stengart's company-issued computer and created a forensic image of the computer's hard drive.[62] Investigation of this forensic image revealed that Stengart had used the computer to send and receive e-mails to and from her attorney regarding

---

56. *Id.* at 2631–32.

57. *Id.* at 2633 (quoting O'Connor v. Ortega, 480 U.S. 709, 732 (1987)).

58. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 662 (N.J. 2010) (discussing factors in determining the reasonableness of an employee's expectation of privacy, including whether the employee used company e-mail or a web-based personal e-mail and whether company policy bans personal e-mail); Stengart v. Loving Care Agency, Inc., No. BER-L-858-08, 2009 WL 798044, at *3 (N.J. Super. Ct. Feb. 5, 2009), *rev'd*, 973 A.2d 390 (N.J. Super. Ct. App. Div. 2009), *aff'd in part*, *modified in part*, 990 A.2d 650 (N.J. 2010).

59. *See, e.g.*, John Gergacz, *Employees' Use of Employer Computers to Communicate with Their Own Attorneys and the Attorney–Client Privilege*, 10 COMPUTER L. REV. & TECH. J. 269, 274–75 (2007) (comparing the attorney–client privilege to the right to privacy when an employee uses an employer's computer); Richard L. Marcus, *The Electronic Lawyer*, 58 DEPAUL L. REV. 263, 297–98 (2009) (noting the potential for future problems regarding the application of the attorney–client privilege to information stored on an employee's computer).

60. *Stengart*, 990 A.2d at 655.

61. *Id.* at 655–56; *Stengart*, 2009 WL 798044, at *3.

62. *Stengart*, 990 A.2d at 656.

Stengart's lawsuit against Loving Care.[63] These e-mails were sent using Stengart's private, password-protected, Internet-based Yahoo! e-mail account.

During the litigation, Loving Care disclosed that it had found evidence of Stengart's communication with her attorney.[64] Stengart invoked the protections of the attorney–client privilege and demanded the immediate return or destruction of every e-mail.[65] Loving Care refused, arguing that Stengart waived any protection by using Loving Care's computer, Internet access, and servers to communicate with her attorney.[66] Stengart responded by filing a motion asking the trial court to order Loving Care to comply with Stengart's requests.[67] The trial court denied Stengart's motion, which was reversed by the appellate court. Loving Care then appealed to the New Jersey Supreme Court, which carefully analyzed the extent of an employee's expectation of privacy and confidentiality in personal e-mails with her attorney when that correspondence was sent and received using an employer-owned computer.[68]

The court focused its analysis on two principal areas: "the adequacy of the notice provided" by Loving Care's electronic communications policy and "the important public policy concerns raised by the attorney–client privilege."[69] Both considerations concern the reasonableness of an employee's expectation of privacy. Regarding, first, the meaning and scope of Loving Care's policy, the court noted that the policy reserves to Loving Care the right to review and access "all matters on the company's media systems and services at any time" and that e-mail is "considered part of the company's business . . . records."[70] However, the court also noted that "[i]t is not clear from that language whether the use of personal, password-protected, web-based e-mail accounts via company equipment is covered."[71] The policy also did not "warn employees that the contents of such e-mails are stored on a hard drive and can be forensically retrieved and read by

---

63. *See id.* at 655–56.

64. *Id.* at 656–57.

65. *Stengart*, 2009 WL 798044, at *3–4.

66. *Id.* at *4.

67. *Stengart*, 990 A.2d at 657.

68. *See id.* at 660–64 (reviewing precedent and outlining various factors that inform reasonable expectation of privacy).

69. *Id.* at 659.

70. *Id.* (alteration in original).

71. *Id.*

Loving Care."[72] Thus, as written, the policy "creates ambiguity about whether personal e-mail use is company or private property. The scope of the written Policy, therefore, is not entirely clear."[73]

The court then discussed the policies underlying the attorney–client privilege, which the court recognized is meant to foster free and full disclosure of information between client and attorney. The court set out to evaluate whether Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney and, if so, whether she had waived the privilege.[74]

The court reviewed previous decisions that addressed this issue, including *Asia Global*, *Curto*, *Evans*, *Scott*, and *Convertino*.[75] The court noted that these previous decisions appear to grant an employee "a lesser expectation of privacy when [the employee] communicate[s] with an attorney using a company e-mail system as compared to a personal, web-based account" like the one Stengart used—even when the e-mails are sent using a company-owned computer.[76] The court also noted that the previous decisions appear to have found that "the existence of a clear company policy banning personal e-mails can also diminish the reasonableness of an employee's claim to privacy in e-mail" with her attorney.[77] Last, the court noted that "[t]he location of the company's computer may also be a relevant consideration."[78]

Specifically, the court cited *Curto*, noting that the employee sent e-mails to her attorney using a company-owned notebook computer via her personal AOL e-mail account while working from her home office.[79] Those messages did not go through the company's servers, but were retrievable nonetheless. Notwithstanding the company's policy banning personal use, the *Curto* court found that the e-mails were privileged.[80] In sum, the *Stengart* case considered all the previous related decisions and concluded that a multitude of different facts can affect the

---

72. *Id.*
73. *Id.*
74. *Id.* at 659–64.
75. *Id.* at 660–63.
76. *Id.* at 661–62.
77. *Id.* at 662.
78. *Id.* at 663.
79. *Id.* (citing Curto v. Med. World Commc'ns, Inc., 99 Fair Empl. Prac. Cas. (BNA) 298, 299, 301 (2006)).
80. *Curto*, 99 Fair Empl. Prac. Cas. (BNA) at 305.

outcome in a given case, and that no one factor is dispositive.[81]

Applying the above considerations to the facts before it, the *Stengart* court determined that Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's notebook computer.[82] The court noted that Stengart took steps to protect the privacy of the e-mails by using "a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer."[83] In addition, Loving Care's electronic communications policy did not specifically "address the use of personal, web-based e-mail accounts accessed through company equipment."[84] In fact, the policy did not address personal accounts at all. Nor did the policy warn the workforce that the contents of e-mail sent via personal accounts could be retrieved forensically and read by the company.[85] Thus, the court determined that the e-mail communications were protected by attorney–client privilege and that Stengart did not waive the privilege.[86]

Most notably, in dicta the court opined that even a clearly crafted electronic communications policy would not allow a company to read an otherwise privileged communication.[87] Nonetheless, the court conceded that employers may monitor and regulate the use of workplace computers, and that companies may adopt computer use policies to protect their assets, reputation, and productivity. The court noted:

> But employers have no need or basis to read the specific *contents* of personal, privileged, attorney–client communications in order to enforce corporate policy. Because of the important public policy concerns underlying the attorney–client privilege, even 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

81. *Stengart*, 990 A.2d at 660–63.

82. *Id.* at 663.

83. *Id.* at 663. The Court also considered the fact that Stengart did not save the password to her personal e-mail account on the company-owned computer. *Id.*

84. *Id.*

85. *Id.*

86. *Id.* at 664.

87. *Id.* at 665.

enforceable.[88]

This broad pronouncement should alert employers who may have previously relied on their policy statements to defeat an employee's privacy expectations with respect to both business and personal e-mail stored on company equipment.

The *Stengart* court next examined whether Loving Care's law firm's review and use of the privileged e-mail violated any ethical rules. The court referred to Rule 4.4 of New Jersey's Rules of Professional Conduct, which provides that "[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."[89] Although the court recognized that Loving Care "legitimately attempted to preserve evidence" within the context of a civil lawsuit, "[i]ts error was in not setting aside the arguably privileged messages once it realized they were attorney–client communications, and failing either to notify its adversary or seek court permission before reading further."[90]

Notably, Rule 4.04(a) of the Texas Disciplinary Rules of Professional Conduct is unclear whether Texas lawyers would be under the same obligation. Rule 4.04(a) requires that "[i]n representing a client, a lawyer shall not . . . use methods of obtaining evidence that violate the legal rights of [a third] person."[91] The current comments to Rule 4.04 do not address a *Stengart* situation.[92] However, under the recently unsuccessful amendments to the Rules, Comment 1 stated, "For example, if a lawyer receives a document relating to the lawyer's representation of a client and knows that the document was sent inadvertently, the lawyer should promptly notify the sender."[93] In any case, it would behoove the prudent litigator to segregate any arguably privileged communication and seek an expeditious court ruling regarding the nature of the communication.

---

88. *Id.*

89. *Id.* (alteration in original) (quoting N.J. RULES OF PROF'L CONDUCT R. 4.4 (2004), *available at* http://www.judiciary.state.nj.us/rules/apprpc.htm).

90. *Id.* at 666.

91. TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 4.04(a) (2010).

92. *See* TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 4.04 cmt. (2010) ("Although in most cases a lawyer's responsibility to the interest of his client is paramount . . . , a lawyer should avoid the infliction of needless harm.").

93. PROPOSED AMENDMENTS TO TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 4.04 cmt. 1 (2010), *available at* http://www.supreme.courts.state.tx.us/rules/pdf/ProposedTDRPCAndComments.pdf.

VI. IMPLICATIONS OF *STENGART*

Although the *Stengart* court did not expressly address nonprivileged personal e-mails accessed and sent using company computers, its analysis implies that these messages may be afforded less protection. In *Stengart*, the strong public policy reasons for protecting confidential attorney–client communications are given significant weight in balancing Stengart's interests against those of Loving Care. However, whether an employee has a reasonable expectation of privacy in nonprivileged communications from a personal, password-protected, web-based e-mail service may depend on the adequacy of the employer's policy to provide notice that the content of such e-mail communication could be monitored and read. Thus, employers should treat the decision as a warning that other courts may carefully scrutinize, narrowly interpret, and give reduced weight to electronic communications policies previously used to justify an employer's regulation of communications stored on corporate equipment.

Employers cannot predict how courts will react to this new and potentially far-reaching decision. As such, employers should review their electronic resources policies—both in terms of how they are distributed and how clearly they are written—to ensure that the policy places them in the strongest position when monitoring communications stored on their equipment. Even a company that takes all possible precautions should recognize that it might still face a ruling that an employee's communications with personal counsel are privileged despite the policy. Therefore, the company and its counsel must be aware of their ethical obligations should arguably privileged communications be discovered.

VII. AN EFFECTIVE ELECTRONIC COMMUNICATIONS POLICY

The foundation of an employer's right to monitor and discover employee communication is an effective electronic communication policy. Initially, the employer should state the goal of the policy—to establish a clear line between purely personal communication and communication in which the employer has a right to review. Next, the policy must explicitly delineate the types of data and information that are to be transferred and stored on the company's systems, which must be for legitimate business reasons only. For example, the policy should explain that it encompasses company-issued equipment, such as laptops, desktops, servers, personal digital assistants, printers, and cell phones. The policy should also encompass all

electronic communications and files (such as e-mails, instant messages, and text messages) stored on, or transmitted by or through, any of the employer's equipment or network, regardless of whether employees use a third-party service provider to convey the message.

As part of that policy, an employer should inform the workforce that the employer will, in its discretion, review any communication or files stored on any company-owned device, whether or not the communication concerns the employer's business, either during or after the end of the employee's tenure. Critically, the policy should expressly advise the workforce that the employer's monitoring may encompass any communication or other information stored on—or transmitted by or through—its electronic resources, regardless of whether a personal e-mail or text message facilitated the transmission.

An employer should also prohibit its workforce from using personal accounts to conduct any company business and consider going one step further and prohibit its workforce from accessing accounts through personal, third-party service providers using company electronic resources. Such a policy, however, could only be enforced by using blocking software. In addition, such a policy could generate significant employee disgruntlement. To address this concern, an employer could advise its workforce that incidental personal use of company computer equipment or its network is permitted only during nonworking time, such as before or after the workday or during lunch. In addition, the policy should unambiguously state that any such personal use is not private and is subject to all of the provisions of the electronic resources policy.

Last, the company's managers should be trained to follow and enforce the policy. Enforcement should be clearly stated in the policy to include discipline, up to and including termination, for a violation of the policy. And each employee should sign a receipt acknowledging dissemination of the policy.

In sum, the workforce should be told clearly that they have no expectation of privacy in any business or personal communications transmitted through or stored on corporate electronic resources. Yet, it may be the case after *Stengart* that an employer may not monitor, review, or use an employee's communication with personal counsel even when such communication clearly violates the company's stringent electronic communications policy.

VIII. CONCLUSION

During the past decade, e-mail has become ubiquitous because of the growth of the Internet, the plethora of communications devices, and the widespread availability of wireless networks. Naturally, this has resulted in attorneys and clients communicating more frequently and in nontraditional forms. However, recent court decisions, particularly *Stengart*, counsel that attorneys and clients regard the nature, form, and use of their communication with a heightened sense of scrutiny and security.