990 A.2d 650 (2010)
201 N.J. 300

Marina STENGART, Plaintiff-Respondent,
v.
LOVING CARE AGENCY, INC., Steve Vella, Robert Creamer, Lorena Lockey, Robert Fusco, and LCA Holdings, Inc., Defendants-Appellants.

A-16 September Term 2009.

Supreme Court of New Jersey.

Argued December 2, 2009.
Decided March 30, 2010.

654 *654 Peter G. Verniero, Newark, argued the cause for appellants (Sills Cummis & Gross and Porzio Bromberg & Newman, attorneys; Mr. Verniero and James M. Hirschhorn, of counsel; Mr. Verniero, Mr. Hirschhorn, Lynne Anne Anderson, and Jerrold J. Wohlgemuth, on the briefs).

Peter J. Frazza, Short Hills, argued the cause for respondent (Budd Larner, attorneys; Mr. Frazza and David J. Novack, of counsel; Mr. Frazza, Donald P. Jacobs, and Allen L. Harris, on the briefs).

Marvin M. Goldstein, Newark, submitted a brief on behalf of amicus curiae Employers Association of New Jersey (Proskauer Rose, attorneys; Mr. Goldstein, Mark A. Saloman, and John J. Sarno, of counsel and on the brief).

Jeffrey S. Mandel, Morristown, submitted a brief on behalf of amicus curiae Association of Criminal Defense Lawyers of New Jersey (PinilisHalpern, attorneys).

Richard E. Yaskin, Cherry Hill, submitted a brief on behalf of amicus curiae National Employment Lawyers Association of New Jersey (Mr. Yaskin and Resnick, Nirenberg & Cash, attorneys; Mr. Yaskin and Jonathan I. Nirenberg, on the brief).

Allen A. Etish, President, Haddonfield, submitted a brief on behalf of amicus curiae New Jersey State Bar Association (Mr. Etish, Stryker, Tams & Dill, Gibbons, and Scarinci Hollenbeck, attorneys; Mr. Etish, Douglas S. Brierley, Fruqan Mouzon, and Thomas Hoff Prol, on the brief).

Chief Justice RABNER delivered of the opinion of the Court.

In the past twenty years, businesses and private citizens alike have embraced the use of computers,
655 electronic communication devices, the Internet, and e-mail. As those and other forms of technology *655 evolve, the line separating business from personal activities can easily blur.

In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.

This case presents novel questions about the extent to which an employee can expect privacy and confidentiality in personal e-mails with her attorney, which she accessed on a computer belonging to her employer. Marina Stengart used her company-issued laptop to exchange e-mails with her lawyer through her

personal, password-protected, web-based e-mail account. She later filed an employment discrimination lawsuit against her employer, Loving Care Agency, Inc. (Loving Care), and others.

In anticipation of discovery, Loving Care hired a computer forensic expert to recover all files stored on the laptop including the e-mails, which had been automatically saved on the hard drive. Loving Care's attorneys reviewed the e-mails and used information culled from them in the course of discovery. In response, Stengart's lawyer demanded that communications between him and Stengart, which he considered privileged, be identified and returned. Opposing counsel disclosed the documents but maintained that the company had the right to review them. Stengart then sought relief in court.

The trial court ruled that, in light of the company's written policy on electronic communications, Stengart waived the attorney-client privilege by sending e-mails on a company computer. The Appellate Division reversed and found that Loving Care's counsel had violated *RPC* 4.4(b) by reading and using the privileged documents.

We hold that, under the circumstances, Stengart could reasonably expect that e-mail communications with her lawyer 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. By reading e-mails that were at least arguably privileged and failing to notify Stengart promptly about them, Loving Care's counsel breached *RPC* 4.4(b). We therefore modify and affirm the judgment of the Appellate Division and remand to the trial court to determine what, if any, sanctions should be imposed on counsel for Loving Care.

I.

This appeal arises out of a lawsuit that plaintiff-respondent Marina Stengart filed against her former employer, defendant-appellant Loving Care, its owner, and certain board members and officers of the company. She alleges, among other things, constructive discharge because of a hostile work environment, retaliation, and harassment based on gender, religion, and national origin, in violation of the New Jersey Law Against Discrimination, *N.J.S.A.* 10:5-1 to -49. Loving Care denies the allegations and suggests they are an attempt to escape certain restrictive covenants that are the subject of a separate lawsuit.

Loving Care provides home-care nursing and health services. Stengart began working for Loving Care in 1994 and, over time, was promoted to Executive Director of Nursing. The company provided her with a laptop computer to conduct company business. From that laptop, Stengart could send e-mails using her company e-mail address; she could also access the Internet and visit websites through Loving Care's server.
656 Unbeknownst to Stengart, certain browser software in place automatically *656 made a copy of each web page she viewed, which was then saved on the computer's hard drive in a "cache" folder of temporary Internet files. Unless deleted and overwritten with new data, those temporary Internet files remained on the hard drive.

On several days in December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop.

Not long after, Stengart left her employment with Loving Care and returned the laptop. On February 7, 2008, she filed the pending complaint.

In an effort to preserve electronic evidence for discovery, in or around April 2008, Loving Care hired experts to create a forensic image of the laptop's hard drive. Among the items retrieved were temporary Internet files

containing the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account.[1] Stengart's lawyers represented at oral argument that one e-mail was simply a communication he sent to her, to which she did not respond.

A legend appears at the bottom of the e-mails that Stengart's lawyer sent. It warns readers that

> THE INFORMATION CONTAINED IN THIS EMAIL COMMUNICATION IS INTENDED ONLY FOR THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENT NAMED ABOVE. This message may be an Attorney-Client communication, and as such is privileged and confidential. If the reader of[2] this message is not the intended recipient, you are hereby notified that you have received this communication in error, and that your review, dissemination, distribution, or copying of the message is strictly prohibited. If you have received this transmission in error, please destroy this transmission and notify us immediately by telephone and/or reply email.

At least two attorneys from the law firm representing Loving Care, Sills Cummis (the "Firm"), reviewed the e-mail communications between Stengart and her attorney. The Firm did not advise opposing counsel about the e-mails until months later. In its October 21, 2008 reply to Stengart's first set of interrogatories, the Firm stated that it had obtained certain information from "e-mail correspondence"—between Stengart and her
657 lawyer—from Stengart's "office computer on December 12, 2007 at 2:25 p.m." In response, Stengart's *657 attorney sent a letter demanding that the Firm identify and return all "attorney-client privileged communications" in its possession. The Firm identified and disclosed the e-mails but asserted that Stengart had no reasonable expectation of privacy in files on a company-owned computer in light of the company's policy on electronic communications.

Loving Care and its counsel relied on an Administrative and Office Staff Employee Handbook that they maintain contains the company's Electronic Communication policy (Policy). The record contains various versions of an electronic communications policy, and Stengart contends that none applied to her as a senior company official. Loving Care disagrees. We need not resolve that dispute and assume the Policy applies in addressing the issues on appeal.

The proffered Policy states, in relevant part:

> 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; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

The Policy also specifically prohibits "[c]ertain uses of the e-mail system" including sending inappropriate sexual, discriminatory, or harassing messages, chain letters, "[m]essages in violation of government laws," or messages relating to job searches, business activities unrelated to Loving Care, or political activities. The

Policy concludes with the following warning: "Abuse of the electronic communications system may result in disciplinary action up to and including separation of employment."

Stengart's attorney applied for an order to show cause seeking return of the e-mails and other relief. The trial court converted the application to a motion, which it later denied in a written opinion. The trial court concluded that the Firm did not breach the attorney-client privilege because the company's Policy placed Stengart on sufficient notice that her e-mails would be considered company property. Stengart's request to disqualify the Firm was therefore denied.

The Appellate Division granted Stengart's motion for leave to appeal. The panel reversed the trial court order and directed the Firm to turn over all copies of the e-mails and delete any record of them. *Stengart v. Loving Care Agency, Inc.*, 408 *N.J.Super.* 54, 973 *A.*2d 390 (App.Div. 2009). Assuming that the Policy applied to Stengart, the panel found that "[a]n objective reader could reasonably conclude. . . that not all personal emails are necessarily company property." *Id.* at 64, 973 *A.*2d 390. In other words, an employee could "retain an expectation of privacy" in personal e-mails sent on a company computer given the language of the Policy. *Id.* at 65, 973 *A.*2d 390.

The panel balanced Loving Care's right to enforce reasonable rules for the workplace against the public
658 policies underlying the attorney-client privilege. *Id.* at 66, 973 *A.*2d 390. The court rejected the notion *658 that "ownership of the computer [is] the sole determinative fact" at issue and instead explained that there must be a nexus between company policies and the employer's legitimate business interests. *Id.* at 68-69, 973 *A.*2d 390. The panel concluded that society's important interest in shielding communications with an attorney from disclosure outweighed the company's interest in upholding the Policy. *Id.* at 74-75, 973 *A.*2d 390. As a result, the panel found that the e-mails were protected by the attorney-client privilege and should be returned. *Id.* at 75, 973 *A.*2d 390.

The Appellate Division also concluded that the Firm breached its obligations under *RPC* 4.4(b) by failing to alert Stengart's attorneys that it possessed the e-mails before reading them. The panel remanded for a hearing to determine whether disqualification of the Firm or some other sanction was appropriate.

We granted Loving Care's motion for leave to appeal and ordered a stay pending the outcome of this appeal.

II.

Loving Care argues that its employees have no expectation of privacy in their use of company computers based on the company's Policy. In its briefs before this Court, the company also asserts that by accessing e-mails on a personal account through Loving Care's computer and server, Stengart either prevented any attorney-client privilege from attaching or waived the privilege by voluntarily subjecting her e-mails to company scrutiny. Finally, Loving Care maintains that its counsel did not violate *RPC* 4.4(b) because the e-mails were left behind on Stengart's company computer—not "inadvertently sent," as per the *Rule*—and the Firm acted in the good faith belief that any privilege had been waived.

Stengart argues that she intended the e-mails with her lawyer to be confidential and that the Policy, even if it applied to her, failed to provide adequate warning that Loving Care would save on a hard drive, or monitor the contents of, e-mails sent from a personal account. Stengart also maintains that the communications with her lawyer were privileged. When the Firm encountered the arguably protected e-mails, Stengart contends it should have immediately returned them or sought judicial review as to whether the attorney-client privilege applied.

We granted amicus curiae status to the following organizations: the Employers Association of New Jersey (EANJ), the National Employment Lawyers Association of New Jersey (NELA-NJ), the Association of Criminal Defense Lawyers of New Jersey (ACDL-NJ), and the New Jersey State Bar Association (NJSBA).

EANJ calls for reversal of the Appellate Division decision. It notes the dramatic, recent increase in the use of non-business-related e-mails at work and submits that, by allowing occasional personal use of company property as a courtesy to employees, companies do not create a reasonable expectation of privacy in the use of their computer systems. EANJ also contends that the Appellate Division's analysis— particularly, its focus on whether workplace policies in the area of electronic communications further legitimate business interests— will unfairly burden employers and undermine their ability to protect corporate assets.

NELA-NJ and ACDL-NJ support the Appellate Division's ruling. NELA-NJ submits that an employee has a substantive right to privacy in her password-protected e-mails, even if accessed from an employer-owned
659 computer, and that an employer's invasion of that privacy right must be narrowly tailored to the employer's *659 legitimate business interests. ACDL-NJ adds that the need to shield private communications from disclosure is amplified when the attorney-client privilege is at stake.

NJSBA expresses concern about preserving the attorney-client privilege in the "increasingly technology-laden world" in which attorneys practice. NJSBA cautions against allowing inadvertent or casual waivers of the privilege. To analyze the competing interests presented in cases like this, NJSBA suggests various factors that courts should consider in deciding whether the privilege has been waived.

III.

Our analysis draws on two principal areas: the adequacy of the notice provided by the Policy and the important public policy concerns raised by the attorney-client privilege. Both inform the reasonableness of an employee's expectation of privacy in this matter. We address each area in turn.

A.

We start by examining the meaning and scope of the Policy itself. The Policy specifically reserves to Loving Care the right to review and access "all matters on the company's media systems and services at any time." In addition, e-mail messages are plainly "considered part of the company's business . . . records."

It is not clear from that language whether the use of personal, password-protected, web-based e-mail accounts via company equipment is covered. The Policy uses general language to refer to its "media systems and services" but does not define those terms. Elsewhere, the Policy prohibits certain uses of "the e-mail system," which appears to be a reference to company e-mail accounts. The Policy does not address personal accounts at all. In other words, employees do not have express notice that messages sent or received on a personal, web-based e-mail account are subject to monitoring if company equipment is used to access the account.

The Policy also does not warn employees that the contents of such e-mails are stored on a hard drive and can be forensically retrieved and read by Loving Care.

The Policy goes on to declare that e-mails "are not to be considered private or personal to any individual employee." In the very next point, the Policy acknowledges that "[o]ccasional personal use [of e-mail] is permitted." 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.

B.

The policies underlying the attorney-client privilege further animate this discussion. The venerable privilege is enshrined in history and practice. *Fellerman v. Bradley,* 99 *N.J.* 493, 498, 493 *A.*2d 1239 (1985) ("[T]he attorney-client privilege is recognized as one of `the oldest of the privileges for confidential communications.'") (quoting 8 J. Wigmore, *Evidence* § 2290, at 542 (McNaughton rev.1961)). Its primary rationale is to encourage "free and full disclosure of information from the client to the attorney." *Ibid.* That, in turn, benefits the public, which "is well served by sound legal counsel" based on full, candid, and confidential exchanges. *Id.* at 502, 493 *A.*2d 1239.

The privilege is codified at *N.J.S.A.* 2A:84A-20, and it appears in the *Rules of Evidence* as *N.J.R.E.* 504. Under the *Rule,* "[f]or a communication to be privileged it must initially be expressed by an individual in his
660 capacity as a client in *660 conjunction with seeking or receiving legal advice from the attorney in his capacity as such, with the expectation that its content remain confidential." *Fellerman, supra,* 99 *N.J.* at 499, 493 *A.*2d 1239 (citing *N.J.S.A.* 2A:84A-20(1) and (3)).

E-mail exchanges are covered by the privilege like any other form of communication. *See Seacoast Builders Corp. v. Rutgers,* 358 *N.J.Super.* 524, 553, 818 *A.*2d 455 (App.Div.2003) (finding e-mail from client to attorney "obviously protected by the attorney-client privilege as a communication with counsel in the course of a professional relationship and in confidence").

The e-mail communications between Stengart and her lawyers contain a standard warning that their contents are personal and confidential and may constitute attorney-client communications. The subject matter of those messages appears to relate to Stengart's working conditions and anticipated lawsuit against Loving Care.

IV.

Under the particular circumstances presented, how should a court evaluate whether Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney?

A.

Preliminarily, we note that the reasonable-expectation-of-privacy standard used by the parties derives from the common law and the Search and Seizure Clauses of both the Fourth Amendment and Article I, paragraph 7 of the New Jersey Constitution. The latter sources do not apply in this case, which involves conduct by private parties only.[3]

The common law source is the tort of "intrusion on seclusion," which can be found in the *Restatement (Second) of Torts* § 652B (1977). That section provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Restatement, supra,* § 652B. A high threshold must be cleared to assert a cause of action based on that tort. *Hennessey, supra,* 129 *N.J.* at 116, 609 *A.*2d 11 (Pollock, J., concurring). A plaintiff must establish that the intrusion "would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object." *Restatement, supra,* § 652B cmt. d.

As is true in Fourth Amendment cases, the reasonableness of a claim for intrusion on seclusion has both a subjective and objective component. *See State v. Sloane,* 193 *N.J.* 423, 434, 939 *A.*2d 796 (2008) (analyzing Fourth Amendment); *In re Asia Global Crossing, Ltd.,* 322 *B.R.* 247, 257 (Bankr.S.D.N.Y.2005) (analyzing common law tort). Moreover, whether an employee has a reasonable expectation of privacy in her particular work setting "must be addressed on a case-by-case basis." *O'Connor v. Ortega,* 480 *U.S.* 709, 718, 107 *S.Ct.* 1492, 1498, 94 *L.Ed.*2d 714, 723 (1987) (plurality opinion) (reviewing public sector employment).

B.

661 A number of courts have tested an employee's claim of privacy in files stored on *661 company computers by evaluating the reasonableness of the employee's expectation. No reported decisions in New Jersey offer direct guidance for the facts of this case.[4] In one matter, *State v. M.A.,* 402 *N.J.Super.* 353, 954 *A.*2d 503 (App.Div.2008), the Appellate Division found that the defendant had no reasonable expectation of privacy in personal information he stored on a workplace computer under a separate password. *Id.* at 369, 954 *A.*2d 503. The defendant had been advised that all computers were company property. *Id.* at 359, 954 *A.*2d 503. His former employer consented to a search by the State Police, who, in turn, retrieved information tied to the theft of company funds. *Id.* at 361-62, 954 *A.*2d 503. The court reviewed the search in the context of the Fourth Amendment and found no basis for the defendant's privacy claim in the contents of a company computer that he used to commit a crime. *Id.* at 365-69, 954 *A.*2d 503.

Doe v. XYC Corp., 382 *N.J.Super.* 122, 887 *A.*2d 1156 (App.Div.2005), likewise did not involve attorney-client e-mails. In *XYC Corp.,* the Appellate Division found no legitimate expectation of privacy in an employee's use of a company computer to access websites containing adult and child pornography. *Id.* at 139, 887 *A.*2d 1156. In its analysis, the court referenced a policy authorizing the company to monitor employee website activity and e-mails, which were deemed company property. *Id.* at 131, 138-39, 887 *A.*2d 1156.

Certain decisions from outside New Jersey, which the parties also rely on, are more instructive. Among them, *National Economic Research Associates v. Evans,* 21 *Mass. L. Rptr.* No. 15, at 337, 2006 WL 2440008 (Mass.Super.Ct. Sept. 25, 2006), is most analogous to the facts here. In *Evans,* an employee used a company laptop to send and receive attorney-client communications by e-mail. In doing so, he used his personal, password-protected Yahoo account and not the company's e-mail address. *Ibid.* The e-mails were automatically stored in a temporary Internet file on the computer's hard drive and were later retrieved by a computer forensic expert. *Ibid.* The expert recovered various attorney-client e-mails; at the instruction of the company's lawyer, those e-mails were not reviewed pending guidance from the court. *Ibid.*

A company manual governed the laptop's use. The manual permitted personal use of e-mail, to "be kept to a minimum," but warned that computer resources were the "property of the Company" and that e-mails were "not confidential" and could be read "during routine checks." *Id.* at 338.

The court denied the company's application to allow disclosure of the e-mails that its expert possessed. *Id.* at 337. The court reasoned,

> Based on the warnings furnished in the Manual, Evans [(the employee)] could not reasonably expect to communicate in confidence with his private attorney if Evans e-mailed his attorney using his NERA [(company)] e-mail address through the NERA Intranet, because the Manual plainly warned Evans that e-mails on the network could be read by NERA network administrators. The Manual, however, did not expressly declare that it would monitor the *content* of Internet communications. . . . Most importantly, the Manual did not expressly
662 declare, or even implicitly suggest, that NERA would monitor the content *662 of e-mail

> communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. Nor did NERA warn its employees that the content of such Internet e-mail communications is stored on the hard disk of a NERA-issued computer and therefore capable of being read by NERA.
>
> [*Id.* at 338-39.]

As a result, the court found the employee's expectation of privacy in e-mails with his attorney to be reasonable. *Id.* at 339.

In *Asia Global, supra,* the Bankruptcy Court for the Southern District of New York considered whether a bankruptcy trustee could force the production of e-mails sent by company employees to their personal attorneys on the *company's* e-mail system. 322 *B.R.* at 251-52. The court developed a four-part test to "measure the employee's expectation of privacy in his computer files and e-mail":

> (1) does 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?
>
> [*Id.* at 257.]

Because the evidence was "equivocal" about the existence of a corporate policy banning personal use of e-mail and allowing monitoring, the court could not conclude that the employees' use of the company e-mail system eliminated any applicable attorney-client privilege. *Id.* at 259-61.

Both *Evans* and *Asia Global* referenced a formal ethics opinion by the American Bar Association that noted "lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an [online service provider]." *See id.* at 256 (citing ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 413 (1999)); *Evans, supra,* 21 *Mass. L. Rptr.* No. 15, at 339 (same).

Other courts have measured the factors outlined in *Asia Global* among other considerations. In reviewing those cases, we are mindful of the fact-specific nature of the inquiry involved and the multitude of different facts that can affect the outcome in a given case. No one factor alone is necessarily dispositive.

According to some courts, employees appear to have a lesser expectation of privacy when they communicate with an attorney using a company e-mail system as compared to a personal, web-based account like the one used here. *See, e.g., Smyth v. Pillsbury Co.*, 914 *F.Supp.* 97, 100-01 (E.D.Pa.1996) (finding no reasonable expectation of privacy in unprofessional e-mails sent to supervisor through internal corporate e-mail system); *Scott v. Beth Israel Med. Ctr., Inc.*, 17 *Misc.*3d 934, 847 *N.Y.S.*2d 436, 441-43 (N.Y.Sup.Ct. 2007) (finding no expectation of confidentiality when company e-mail used to send attorney-client messages). *But see Convertino v. U.S. Dep't of Justice*, 674 *F.Supp.2d* 97, 110 (D.D.C.2009) (finding reasonable expectation of privacy in attorney-client e-mails sent via employer's e-mail system). As a result, 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 company computer.

Courts have also 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 messages with his or her attorney.
663 *Compare Scott, supra,* 847 *663 *N.Y.S.*2d at 441 (finding e-mails sent to attorney not privileged and noting that company's e-mail policy prohibiting personal use was "critical to the outcome"), *with Asia Global, supra,* 322 *B.R.* at 259-61 (declining to find e-mails to attorney were not privileged in light of unclear evidence as to

existence of company policy banning personal e-mail use). We recognize that a zero-tolerance policy can be unworkable and unwelcome in today's dynamic and mobile workforce and do not seek to encourage that approach in any way.

The location of the company's computer may also be a relevant consideration. In *Curto v. Medical World Communications, Inc.*, 99 *Fed. Empl. Prac. Cas.* (BNA) 298, 2006 WL 1318387 (E.D.N.Y. May 15, 2006), for example, an employee working from a home office sent e-mails to her attorney on a company laptop via her personal AOL account. *Id.* at 301. Those messages did not go through the company's servers but were nonetheless retrievable. *Ibid.* Notwithstanding a company policy banning personal use, the trial court found that the e-mails were privileged. *Id.* at 305.

We realize that different concerns are implicated in cases that address the reasonableness of a privacy claim under the Fourth Amendment. *See, e.g., O'Connor, supra,* 480 *U.S.* at 714-19, 107 *S.Ct.* at 1496-98, 94 *L.Ed.*2d at 721-24 (discussing whether public hospital's search of employee workplace violated employee's expectation of privacy under Fourth Amendment); *United States v. Simons,* 206 *F.*3d 392, 397-98 (4th Cir.2000) (involving search warrants for work computer of CIA employee, which revealed more than fifty pornographic images of minors); *M.A., supra,* 402 *N.J.Super.* at 366-69, 954 *A.*2d 503 (involving Fourth Amendment analysis of State Police search of employee's computer, resulting in theft charges). This case, however, involves no governmental action. Stengart's relationship with her private employer does not raise the specter of any government official unreasonably invading her rights.

V.

A.

Applying the above considerations to the facts before us, we find that Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's laptop.

Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used 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. In other words, she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit.

In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property.

Moreover, the e-mails are not illegal or inappropriate material stored on Loving Care's equipment, which
664 might harm the company in some way. *See Muick v. Glenayre Elecs.,* 280 *F.*3d 741, 742-43 (7th *664 Cir.2002); *Smyth, supra,* 914 *F.Supp.* at 98, 101; *XYC Corp., supra,* 382 *N.J.Super.* at 136-40, 887 *A.*2d 1156. They are conversations between a lawyer and client about confidential legal matters, which are historically cloaked in privacy. Our system strives to keep private the very type of conversations that took place here in order to foster probing and honest exchanges.

In addition, the e-mails bear a standard hallmark of attorney-client messages. They warn the reader directly that the e-mails are personal, confidential, and may be attorney-client communications. While a pro forma

warning at the end of an e-mail might not, on its own, protect a communication, *see Scott, supra,* 847 *N.Y.S.*2d at 444, other facts present here raise additional privacy concerns.

Under all of the circumstances, we find that Stengart could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private.

It follows that the attorney-client privilege protects those e-mails. *See Asia Global, supra,* 322 *B.R.* at 258-59 (noting "close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence"). In reaching that conclusion, we necessarily reject Loving Care's claim that the attorney-client privilege either did not attach or was waived. In its reply brief and at oral argument, Loving Care argued that the manner in which the e-mails were sent prevented the privilege from attaching. Specifically, Loving Care contends that Stengart effectively brought a third person into the conversation from the start—watching over her shoulder—and thereby forfeited any claim to confidentiality in her communications. We disagree.

Stengart has the right to prevent disclosures by third persons who learn of her communications "in a manner not reasonably to be anticipated." *See N.J.R.E.* 504(1)(c)(ii). That is what occurred here. 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. *See Evans, supra,* 21 *Mass. L. Rptr.* No. 15, at 339. The language of the Policy, the method of transmittal that Stengart selected, and the warning on the e-mails themselves all support that conclusion.

Loving Care also argued in earlier submissions that Stengart waived the attorney-client privilege. For similar reasons, we again disagree.

A person waives the privilege if she, "without coercion and with knowledge of [her] right or privilege, made disclosure of any part of the privileged matter or consented to such a disclosure made by anyone." *N.J.R.E.* 530 (codifying *N.J.S.A.* 2A:84A-29). Because consent is not applicable here, we look to whether Stengart either knowingly disclosed the information contained in the e-mails or failed to "take reasonable steps to
665 insure and maintain their confidentiality."[5] *Trilogy* *665 *Commc'ns, supra,* 279 *N.J.Super.* at 445-48, 652 *A.*2d 1273.

As discussed previously, Stengart took reasonable steps to keep discussions with her attorney confidential: she elected not to use the company e-mail system and relied on a personal, password-protected, web-based account instead. She also did not save the password on her laptop or share it in some other way with Loving Care.

As to whether Stengart knowingly disclosed the e-mails, she certified that she is unsophisticated in the use of computers and did not know that Loving Care could read communications sent on her Yahoo account. Use of a company laptop alone does not establish that knowledge. Nor does the Policy fill in that gap. Under the circumstances, we do not find either a knowing or reckless waiver.

B.

Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline

employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy. *See Hennessey, supra,* 129 *N.J.* at 99-100, 609 *A.*2d 11; *Woolley v. Hoffmann-LaRoche, Inc.,* 99 *N.J.* 284, 290-92, 491 *A.*2d 1257 (1985); *Pierce v. Ortho Pharm. Corp.,* 84 *N.J.* 58, 72-73, 417 *A.*2d 505 (1980). For example, an employee who spends long stretches of the workday getting personal, confidential legal advice from a private lawyer may be disciplined for violating a policy permitting only occasional personal use of the Internet. 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 enforceable.

VI.

We next examine whether the Firm's review and use of the privileged e-mails violated *RPC* 4.4(b). The *Rule* 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." According to the ABA Model Rules on which *RPC* 4.4(b) is patterned, the term "`document' includes e-mail or other electronic modes of transmission subject to being read or put into readable form." *Model Rules of Prof'l Conduct R.* 4.4 cmt. 2 (2004).

666 Loving Care contends that the *Rule* does not apply because Stengart left *666 the e-mails behind on her laptop and did not send them inadvertently. In actuality, the Firm retained a computer forensic expert to retrieve e-mails that were automatically saved on the laptop's hard drive in a "cache" folder of temporary Internet files. Without Stengart's knowledge, browser software made copies of each webpage she viewed. Under those circumstances, it is difficult to think of the e-mails as items that were simply left behind. We find that the Firm's review of privileged e-mails between Stengart and her lawyer, and use of the contents of at least one e-mail in responding to interrogatories, fell within the ambit of *RPC* 4.4(b) and violated that rule.

To be clear, the Firm did not hack into plaintiff's personal account or maliciously seek out attorney-client documents in a clandestine way. Nor did it rummage through an employee's personal files out of idle curiosity. Instead, it legitimately attempted to preserve evidence to defend a civil lawsuit. Its 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. There is nothing in the record before us to suggest any bad faith on the Firm's part in reading the Policy as it did. Nonetheless, the Firm should have promptly notified opposing counsel when it discovered the nature of the e-mails.[6]

The Appellate Division remanded to the trial court to determine the appropriate remedy. It explained that a hearing was needed in that regard to consider

> the content of the emails, whether the information contained in the emails would have inevitably been divulged in discovery that would have occurred absent [the Firm's] knowledge of the emails' content, and the nature of the issues that have been or may in the future be pled in either this or the related Chancery action.
>
> [*Stengart, supra,* 408 *N.J.Super.* at 76-77, 973 *A.*2d 390.]

We agree. The forensically retrieved version of the e-mails submitted to the Court is not easy to read or fully understand in isolation, and no record has yet been developed about the e-mails' full use. For the same reason, we cannot determine how confidential or critical the messages are. In deciding what sanctions to impose, the trial court should evaluate the seriousness of the breach in light of the specific nature of the e-mails, the manner in which they were identified, reviewed, disseminated, and used, and other considerations noted by the Appellate Division. As to plaintiff's request for disqualification, the court should also "balance competing interests, weighing the `need to maintain the highest standards of the profession' against `a client's right freely to choose his counsel.'" *Dewey v. R.J. Reynolds Tobacco Co.,* 109 *N.J.* 201, 218, 536 *A.*2d 243 (1988) (quoting *Gov't of India v. Cook Indus., Inc.,* 569 *F.*2d 737, 739 (2d Cir.1978)).

We leave to the trial court to decide whether disqualification of the Firm, screening of attorneys, the imposition of costs, or some other remedy is appropriate. Under the circumstances, we do not believe a remand to the Chancery judge is required; the matter may proceed before the Law Division judge assigned to the case.

667 *667 **VII.**

For the reasons set forth above, we modify and affirm the judgment of the Appellate Division and remand to the trial court for further proceedings.

For affirmance as modification/remandment—Chief Justice RABNER and Justices LONG, LaVECCHIA, ALBIN, WALLACE, RIVERA-SOTO and HOENS—7.

Opposed—None.

[1] The record does not specify how many of the e-mails were sent or received during work hours. Loving Care asserts that the e-mails in question were exchanged during work hours through the company's server. However, counsel for Stengart represented at oral argument that four of the e-mails were transmitted or accessed during non-work hours— three on a weekend and one on a holiday. It is unclear, and ultimately not relevant, whether Stengart was at the office when she sent or reviewed them.

[2] In the forensically retrieved version of the e-mails submitted to this Court under seal, the legend is reprinted only up until the location of the footnote in the above text. The retrieved messages also list Stengart's lawyer's full name more than a dozen times and his e-mail address—comprised of the lawyer's first initial, full last name, and the law firm's name—more than three dozen times. Counsel for Loving Care submitted certifications in which they explain that they were aware the e-mails were between Stengart and her lawyer but believed the communications were not protected by the attorney-client privilege for reasons discussed below.

[3] In addition, a right to privacy can be found in Article I, paragraph 1 of the New Jersey Constitution. *Hennessey v. Coastal Eagle Point Oil Co.,* 129 *N.J.* 81, 95-96, 609 *A.*2d 11 (1992).

[4] Under our rules, unpublished opinions do not constitute precedent and "are not to be cited by any court." *R.* 1:36-3. As a result, we do not address any unpublished decisions raised by the parties.

[5] Because Stengart's conduct satisfies both standards, we need not choose which one governs. *See Kinsella v. NYT Television,* 370 *N.J.Super.* 311, 317-18, 851 *A.*2d 105 (App. Div.2004) (noting "different approaches to determining whether the inadvertent disclosure of privileged materials results in a waiver" without adopting global rule) (citing *Seacoast, supra,* 358 *N.J.Super.* at 550-51, 818 *A.*2d 455 and *State v. J.G.,* 261 *N.J.Super.* 409, 419-20, 619 *A.*2d 232 (App.Div.1993)); *see also Trilogy Commc'ns, Inc. v. Excom Realty, Inc.,* 279 *N.J.Super.* 442, 445-48, 652 *A.*2d 1273 (Law Div.1994) (finding attorney's "[i]nadvertent disclosure through mere negligence should not be deemed to abrogate the attorney-client privilege").

[6] The Firm argues that its position was vindicated by the trial court's ruling that the e-mails were not protected by the attorney-client privilege. That argument lacks merit. Stengart still had the right to appeal the trial court's ruling, as she did.