# In The Supreme Court of New Jersey

Docket No.: 65,556

| | |
|---|---|
| MARINA STENGART,<br><br>Plaintiff-Respondent,<br><br>v.<br><br>LOVING CARE AGENCY, INC., STEVE VELLA, ROBERT CREAMER, LORENA LOCKEY, ROBERT FUSCO, and LCA HOLDINGS, INC.,<br><br>Defendants-Movants. | ON MOTION FOR LEAVE TO APPEAL FROM AN INTERLOCUTORY ORDER OF THE SUPERIOR COURT OF NEW JERSEY, APPELLATE DIVISION DOCKET NO.: A-3506-08T1<br><br>***Civil Action***<br><br>**Sat Below:**<br>**Hon. Clarkson S. Fisher, J.A.D.**<br>**Hon. Linda G. Baxter, J.A.D.**<br>**Hon. Christine L. Miniman, J.A.D.** |

## *AMICUS CURIAE* BRIEF OF EMPLOYERS ASSOCIATION OF NEW JERSEY


**PROSKAUER ROSE LLP**
One Newark Center - 18th Floor
Newark, New Jersey 07102
973.274.3200
Attorneys for Employers
Association of New Jersey

**Of Counsel and On the Brief:**

Marvin M. Goldstein, Esq.
Mark A. Saloman, Esq.

and

John J. Sarno, Esq. (Employers Association of New Jersey)

## PRELIMINARY STATEMENT

One of the issues currently before the Court is the enforceability of a company policy that places an employee on notice that the employer has the right to monitor, read, and possess electronic messages sent by an employee through the employer's computer and electronic communications network. This is an issue of first impression in New Jersey and, as the trial and appellate courts noted, an issue where there is a paucity of judicial guidance.[1]

Although the courts below were presented with a narrow and straightforward discovery issue, the Appellate Court's unduly expansive holding effectively destroys New Jersey employers' well-established right to review and inspect all emails prepared by employees at the workplace, during company time, using company computers, and transmitted over company networks. This holding contradicts those of jurisdictions which have considered this issue, negatively impacts both employers and employees, and fails to consider the realities of the modern workplace. The consequence is an impracticable and unpredictable legal burden

[1] As a non-profit organization comprised of more than 1,000 employers within New Jersey and dedicated exclusively to helping employers make responsible employment decisions through education, informed discussion, and training, the Employers Association of New Jersey ("EANJ") is uniquely situated to submit this *amicus curiae* brief in support of the rights of New Jersey employers to implement and apply electronic communications policies in the workplace.

with which employers must now comply, resulting in considerable uncertainty as to whether an employer's commonplace electronic communications policy is lawful.

For these and the foregoing reasons, EANJ respectfully requests that the Appellate Division's decision be reversed.

## Legal Argument[2]

### Point I

**The Appellate Division Erred By Holding That Workplace Policies Which Diminish Employees' Expectations Of Privacy Are Invalid.**

Email has dramatically changed, and is continuing to change, how people communicate while at work. According to a 2004 survey of 840 U.S. businesses, more than 81 percent of employees spent at least one hour reviewing, preparing, and responding to email on a typical workday; about 10 percent spent more than four hours per day. See "2004 Workplace E-Mail and Instant Messaging Survey," American Management Association (2004).[3] More than 85 percent of employees send and receive at least some non-business-related email at work, id., and those

[2] EANJ relies upon the Procedural History and Statement of Facts set forth in Defendants' original brief in opposition to the order to show cause; its motion for leave to appeal to the Appellate Division; and its motion for leave to appeal to the Supreme Court, incorporated herein by reference.

[3] For the Court's convenience, a copy of this survey (which can be found at http://www.epolicyinstitute.com/survey/survey04.pdfhttp://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/) is annexed to EANJ's Appendix of Unpublished Opinions.

percentages, no doubt, are higher today. Even employees who report to fixed work locations have seen their work environments evolve to the point where their interactions are electronic, rather than face-to-face. Id.

Employers monitor employee emails primarily to protect business assets and to measure productivity and compliance with other policies. According to the AMA, approximately one out of three U.S. companies experienced a negative impact on their business due to the exposure of sensitive or embarrassing information caused by employee misuse of email systems. Id.

Taking into account the unique nature of electronic communications generally, and emails specifically, courts routinely uphold the validity of electronic communications policies[4] and confirm that employees have no reasonable expectation of privacy when they use company computers or send emails through the employer's electronic communications systems. Indeed, both the appellate and trial courts here recognize "the considerable scope of an employer's right to govern conduct and

[4] The Electronic Communications Privacy Act, as amended, defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photo electronic or photo optical system." 18 U.S.C. § 2510 (12). Under this definition, an email is clearly an "electronic communication." The electronic communications policy in the instant matter refers to "media systems" presumably because it seeks to communicate with employees, not lawyers or law enforcement officials.

communications in the workplace." Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54, 72 (App. Div. 2009); accord Stengart v. Loving Care Agency, Inc., Docket No. BER-L-858-08, Slip Op. at 6 (Feb. 5, 2009) (De La Cruz, J.S.C.):

> The law recognizes the need for an employer to monitor the computer and internet usage of its employees for the purpose of protecting its business rights and to control its equipment. Indeed, nothing prohibits an employer from setting policy that notices employees that its technology resources are considered company assets or that E-mail messages and internet use and communication and computer files are considered a part of the company's business and client records or that E-mail communications using the company's technology resources are not to be considered private or personal to an individual.

See also Smyth v. The Pillsbury Co. 914 F. Supp. 97, 101 (E.D. Pa. 1996); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (employee has no legitimate expectation of privacy in contents of his workplace computer where employer had notified employees that their computer activities could be monitored), cert. denied, 534 U.S. 930 (2001); United States v. Bailey, 272 F. Supp.2d 822 (D. Neb. 2003)(employee has no expectation of privacy in email communications over employer's electronic communications policy even if employer misled employee about the confidentiality of emails). See, e.g., Employee Privacy: Computer-Use Monitoring Practices and Policies of Selected Companies, United States General Accounting Office (2002). Recent decisions have applied this view to communications

between an employee and her attorney. See, e.g., Kaufman v. SunGard Investigations Systems, Civ. No. 05-1236, 2006 WL 1307882, at *3 (D.N.J. May 10, 2006) (Linares, J.) (applying New Jersey law); Scott v. Beth Israel Medical Center Inc., 847 N.Y.S.2d 436, 441-44 (Sup. 2007) (Ramos, J.).

The electronic communications policy now before the Supreme Court is written in plain language common to procedures implemented by employers across a variety of industries.[5] Indeed, the policy is strikingly similar to the current "Network and Internet Usage Policy" promulgated by the New Jersey Department of Law and Public Safety in 2007.[6] Part VI.A.2. of this policy

[5] The policy states that the employer can "review, audit, intercept, access, and disclose all matters" on the company's systems "at any time, with or without notice." 408 N.J. Super. at 60. The policy also states, in relevant part:

> 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. . . .

Id. (Emphasis added).

[6] For the Court's convenience, a copy of New Jersey Department of Law and Public Safety Operating Procedure No. 1-07, "Network and Internet Usage Policy" (eff. March 1, 2007), which supplements the "Guidelines for Acceptable Internet Access and Use for New Jersey Government," Circular Letter No. 97-03-OTS (eff. Aug. 30, 1996) (found at http://www.state.nj.us/infobank/circular/cir9703s.htm), is annexed to EANJ's Appendix of Unpublished Opinions.

expressly provides that the Department "has the right to intercept, inspect, monitor and log any and all aspects of its computer system including . . . all electronic communications sent and received by employees." Government workers in the Department, like those of Loving Care Agency, "have no rights to privacy." Id. at Part VI.A.1.

Like the policy in this case, the Department's policy permits "incidental personal use." Id. at Part VI.H. The Department's policy, also like the policy here, does not exempt incidental and personal emails from the employer's right to "intercept, inspect, monitor and log" any and all electronic communications. In other words, both policies expressly disclaim a right to privacy in *any* email sent or received by any employee through their employer's electronic communications system, whether business related or personal.

This uniform application of the policy makes common sense because an employee's occasional personal use of an employer's electronic communications system is a courtesy extended to employees, similar to the courtesy of allowing for occasional personal use of the office telephone. Without extending this common courtesy, an employer could clearly ban *all* personal use of *all* company property, including telephones and electronic communications systems. See The Guard Publishing Company d/b/a The Register-Guard, 351 NLRB No. 70, 2007 WL 4540458, *8

(N.L.R.B. Dec. 16, 2007) (holding that an employer can restrict the use of its electronic communications systems to business use only), reversed in part, Guard Publishing Company v. NLRB, 571 F.3d 53 (D.C. Cir. 2009). Knowing that employees may need to make or receive telephone calls at work or send or receive an email from time to time, most employers accommodate occasional or incidental personal use of their communication systems, without creating an exception to their electronic communications policies.

The conclusion reached by the Appellate Division--that every time an employer permits "occasional personal use" of its electronic communications system, it simultaneously creates an expectation of privacy in such use--is without basis in law or fact. This judicial creation out of thin air defies the clear language of the written policy, which expressly provides the employer with the absolute and unconditional right to intercept, inspect, monitor, or read emails sent or received under its electronic communications system. Indeed, the policy in the instant case permits "occasional personal use" but expressly notifies an employee that the employer can "review, audit, intercept, access, and disclose all matters" on the company's systems at any time. Thus, any employee who uses the electronic communications system for personal use does so with the knowledge and understanding that all information can be

reviewed, monitored, and accessed by the employer.

This understanding also serves an important self-policing function which benefits employees by relieving the employer of the Hobson's Choice of either banning occasional personal use altogether or acting as Big Brother. A total ban of personal use of telephones and electronic communications systems will result in the discipline and discharge of employees for relatively minor, even trivial, infractions. Administering intrusive "spying" software is costly, time consuming, and creates a work environment filled with suspicion, fear, and intimidation. Either approach fundamentally undermines the employer's desire to create a positive and productive workplace.

The harsh burdens forced upon employers will create a lose-lose situation because employees will also suffer the loss of convenience and courtesy which they have grown to expect. In today's workplace, employees' occasional personal use of the Internet is a given. If the Appellate Court's decision stands, the employer's loss of the right to monitor, review, and possess its own email traffic prepared on its own computers and transmitted over its own network would adversely impact employers and employees alike.

The occasional-personal-use provision also permits the employer to specify what uses will tangibly harm the company's interests. Both the policy in the instant case, as well as the

Department of Law and Public Safety's policy, enumerate a non-exclusive list of infractions which clearly fall outside the scope of "occasional personal use," such as emails containing inappropriate messages or conduct of a sexual or discriminatory nature. Of course, knowing that all emails are subject to review at any time will not prevent an employee from having a private conversation over a cell phone during lunch or break time or, as it may be, face-to-face after work. There is little doubt, therefore, of the validity of a company policy which places an employee on notice that she has no reasonable expectation of privacy in the content of an email she prepared on a company computer, on company time, and sent over a company computer system *and* that the employer can monitor, read, or possess employee-generated emails.[7]

## POINT II

### The "Legitimate Business Interest" Test Created By The Appellate Court Is Excessively Burdensome For Employers.

The Appellate Court likewise recognizes that "the electronic age––and the speed and ease with which many communications may now be made––has created numerous difficulties in segregating personal business from company

[7] The fact that the employee in this case accessed her Yahoo account is of no moment. It is undisputed that she used the employer's electronic communications system and there is no allegation that the employer improperly obtained the employee's password to access her personal email account.

business." 408 N.J. Super. at 71. Yet, its decision geometrically complicates the employer's ability to perform this task and, consequently, operate efficiently.

Specifically, the appellate decision holds that an electronic communications policy must "reasonably further the legitimate business interest of the employer." 408 N.J. Super. at 68. As a result, emails sent to an employee's personal, password-protected, Internet-based email account––although prepared on the employer's computer and sent through the employer's electronic communications system during working hours––cannot be subject to the employer's routine monitoring and review.

Yet, the first line of defense against a departing employee's misappropriation or outright theft of confidential and proprietary business information and trade secrets is the employer's unimpeded right to continuously intercept, inspect, monitor, and log all electronic communication––especially emails sent by employees to their personal email accounts. Indeed, the overwhelming majority of employers engage in email monitoring as a matter of course. In a survey of more than 440 employers by the Society for Human Resource Management (SHRM) in 2006 (the latest available data), almost three-quarters of the companies reported ongoing monitoring of employees' email. A 2007 survey conducted by the American Management Association and the ePolicy

Institute concurred that 83 percent of responding employers engage in email monitoring. These figures are surely higher today.

The Appellate Court's blanket ruling fatally undermines an employer's right to shield itself from misappropriation or misuse of its most valuable confidential and proprietary assets by employees who leave to join competitors. Employers must be able to exercise this right unimpeded because email is perhaps the most common tool used by employees to impermissibly remove and exploit their former employer's customer lists and other valuable, protectable business data and information. See e.g., Samsung America Inc. v. Park, 2006 WL 3627072 (Ch. Div. Dec. 11, 2006) (Doyne, P.J.S.C.); Fluoramics, Inc. v. Trueba, No. BER-C-408-05, 2005 WL 3455185 (Ch. Div. Dec. 16, 2005); (Doyne, P.J.S.C.); National Risk Services, Inc. v. RK Risk Management, LLC, No. BER-C-362-05, 2005 WL 3058162 (Ch. Div. Nov. 10, 2005) (Doyne, P.J.S.C.). In today's knowledge-based economy, the impact of this ruling cannot be understated.

Aside from the unique nature of the attorney-client relationship, the Appellate Court's arbitrarily-created legal standard is unwarranted and unworkable. Indeed, an employer no longer can implement its electronic communications policy until after analyzing the *content* of all of its emails. The employer must now somehow discern that the employee's email is job-

related before the employer can properly monitor, read, or possess the email. If, on the other hand, the employer judges an email to be "personal," it must have some as yet undefined system in place to protect the "privacy" of the email's content. Considering that thousands, if not tens of thousands, of employee-generated emails traverse a midsize employer's electronic communications system on any given day, the Appellate Court's standard is truly untenable. Indeed, it is doubtful that technology even exists that could be used by an employer to meet its extraordinary new burden.

As an additional practical matter, this court-imposed test will surely spawn more litigation. The Appellate Court's holding will force employers to develop and implement draconian "no personal use" policies covering all communications at work through all company-owned media. The legality of this total prohibition is sure to be challenged when employees inevitably begin violating the policy. Allegations of selective enforcement will also be litigated. In such cases, the Superior Court will be placed in the awkward (and improper) position of second-guessing the employer's judgment as to whether such a company policy serves its business interest or questioning the employer's motivation in granting an employee a reprieve from such a rigid rule. This is a role ill suited for the trial courts. See Delgado v. LA Weight Loss Centers, Inc., No. Civ.

A. 03-6199 (JCL), 2006 WL 840395, *12 (D.N.J. March 28, 2006) (courts do not "sit as a super-personnel department that reexamines an entity's business decisions.")(citing Brewer v. Quaker State Oil Ref. Co., 72 F.3d 326, 332 (3d Cir. 1995); Sarmiento v. Montclair State University, 513 F.Supp.2d 72, 90 (D.N.J. 2007) (same).

In short, the Appellate Court has misapplied the law and misunderstood the nature of electronic communications. Email has had a substantial impact on how people communicate at work. As the trial court observed, and the Appellate Court acknowledged,

> Computers play an important role in the function of companies in today's world. Access to the internet and the ability to communicate by E-mail facilitates efficient business practices and provides instant access to information that may otherwise have been time consuming to obtain. However, the benefits of computers and internet use pose complex and novel questions for both employers and employees with respect to the legal ramifications of such use.

Docket No. BER-L-858-08, Slip Op. at 5. Employers should be free to implement and apply facially valid electronic communications policies without the impossible burden of screening each electronic transmission to determine whether the content is "personal" or business related. Thus, the Appellate Court's well-intentioned admonishment that "the moral force of a company regulation loses impetus when based on no good reason other than the employer's desire to rummage among information

having no bearing upon its legitimate business interests" is misplaced. 408 N.J. Super. at 72.

## Point III

### The Appellate Division Erred By Applying Traditional Concepts Of Property Law To Email Transmissions.

Aside from the obvious futility of implementing the "legitimate business interest" standard articulated by the Appellate Court, its opinion misapplies "property" concepts to employee-generated emails in the workplace. As an initial matter, an email is an intangible electronic transmission, having no physical property whatsoever. An email is not the equivalent of a letter stored in a folder and kept in a filing cabinet and an employer does not selectively engage in a physical invasion when it implements its electronic communications policy. Instead, an employer's policy is designed to place an employee on notice that she has no entitlement to privacy when using the company electronic communications systems. Because an employee never "owns" any email that she prepares during working time and sends through her employer's electronic communications system, the property law analysis fails. There is, in fact, no "property" for the employer to confiscate.

If, for sake of argument, an email transmission can be "property," there is no debate that an employer has the right to

monitor and inspect that "property" if it is created by an employee on company time with a company computer and transmitted over the company's network. Traditional concepts of property law, i.e., who "owns" the email in question, are inapposite and do not alter the long-settled right of employers to monitor and inspect every document or thing prepared, stored, or transmitted by employees. It makes no difference whether an employee keeps personal items in a company-owned locker, filing cabinet, desk drawer, or computer because the employee continues to "own" that "property" and the employer retains every right to inspect and examine the contents of its lockers, filing cabinets, desks, and computers at any time so long as the employee has reasonable notice. The Appellate Court's analogy--that it is improper to permit an employer to monitor its employees' email because it is somehow improper for an employer to examine its own company files because they might contain "an employee's private papers"[8]—is, therefore, misplaced.

## CONCLUSION

A less novel approach is the use of common sense to interpret employer policies that have been widely upheld by state and federal courts. However well intentioned, the Appellate Court has turned common sense on its head. Its opinion will likely force employers to adopt rigid rules that

[8] 408 N.J. Super. at 69.

harm employee morale, foster inefficiencies, and increase the costs of doing business. It imposes an unfounded legal standard based on inapplicable principles of property law that creates ambiguity and uncertainty and is sure to increase litigation. It also interferes with the good faith judgment of both employers and employees and undermines the self-regulating character of the workplace.

Accordingly, EANJ urges this Court to reverse the appellate court's June 26, 2009 decision.

Respectfully submitted,

PROSKAUER ROSE LLP

_____

Marvin M. Goldstein
Mark A. Saloman
One Newark Center
18th Floor
Newark, New Jersey 07102
Attorneys for Employers
Association of New Jersey
*Amicus Curiae* for the Appellant

and

John J. Sarno, Esq.
Employers Association of New Jersey
30 West Mount Pleasant Avenue
Suite 201
Livingston, New Jersey 07039