EPSTEIN BECKER GREEN | CLIENT ALERT

NJ Supreme Court Restricts Employer's Ability To Review Employee's Communications With Personal Attorney on Employer's Computers

by James P. Flynn

April 2010

While many employers worry that some court decisions will add "insult to injury," New Jersey employers must now be aware of *Stengart v. Loving Care Agency Inc.*, -- A.2d --, -- N.J. -- (2010), decided March 30, 2010, which presages adding "injury to injury." That is because it first injures employers' interests by stating that an employer cannot write an enforceable policy that "ban[s] all personal computer use and provide[s] unambiguous notice that an employer could retrieve and read" all emails that an employee wrote through a personal email account using an employer's computer. Slip op. at 28. In *Stengart,* this meant that an employee's communications with personal counsel concerning matters adverse to the company may occur during work time using the employer's resources. And if that were not injury enough to the employer's interests in having employees actually work on company business while at the office using the company's resources, the *Stengart* Court then went on to add another possible injury—on remand, the trial court should consider disqualifying the company's counsel for not immediately upon finding such communications on the employer's computer returning to the departed employee (or her counsel) all copies of such communications. The *Stengart* decision demands that employers, especially in New Jersey, not only revisit their written policies, but also that they consider how such policies are actually being applied and enforced. Decisions like *Stengart* can also directly impact on steps that have become part of best practices responses in trade secret and restrictive covenant cases involving departing employees, and which occur in all manner of employment situations.

Background

Plaintiff Marine Stengart was the Executive Director of Loving Care, Inc., a home care services agency, who resigned and then sued Loving Care for constructive discharge under the New Jersey Law Against Discrimination. Stengart was issued a company

laptop computer. The Court also assumed for its analysis that the company had a well-publicized electronic communications policy that made all aware that the employer's computer and system (including those allowing for internet access) were all company property to be used for company business. The company had contended that there was no reasonable expectation of privacy in any communications that an employee had through such equipment or system because the communications were, as announced in the policy, subject to monitoring, were considered the property of the company, and were embedded within the company's physical property. Stengart, nonetheless, used her company computer to communicate with her personal counsel through her Yahoo account. Such communications were discovered by her former employer on that computer after her termination. Loving Care's counsel did not immediately disclose the existence of such communications to Stengart or her counsel, and instead referenced and included those of relevance to a response to a later discovery request.

The Court's Analysis

The Court's analysis was driven by two basic factors, one case-specific, one more general, on the issue of whether a privilege ever existed or was waived.

Of specific concern to the Court was Loving Care's written policy, which clearly stated that email and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records, that "such communications are not to be considered private or personal to any individual employee," that the company reserved the right to review, audit, intercept, access and disclose "all matters on the company's media systems and services at any time." Slip op. at 11. But the policy also stated that "occasional personal use is permitted." Slip op. at 11. The Court, assuming the policy was in effect, and despite language in the policy that specifically applied to "internet use and communication" in addition to email, found that an objective reader might not conclude that the policy applied to using a work computer to access a personal, password-protected Yahoo account. Moreover, the Court held that the company's reasonable statement that "occasional personal use" of the company email would be tolerated somehow further frustrated the company's effort to thwart the creation of any reasonable expectation of privacy.

But, more generally, the *Stengart* Court found that the interests protected by the attorney-client privilege outweighed employers' interests in enforcing electronic communications policies. In doing so, the Court seemed to ignore the fact that privileged communications require an expectation of confidentiality, and none should have arisen on the facts of this case. The Court's analysis suggests strongly the policy's provision allowing for occasional "personal" use somehow created an expectation of privacy, ignoring the distinction between "private" and "personal." In *Stengart*, the terms were used interchangeably, even though the words do not necessarily carry the same connotation.

The holdings of the *Stengart* Court go beyond the earlier Appellate Division decision in the case, which had only implied that a policy cannot be written that would have led the Court to have found any claim of privilege inert or waived. Indeed, the Supreme Court expressly stated that an enforceable policy eliminating all personal use could not be written, and also noted that "a zero-tolerance policy [on personal use of computers]" is "unworkable and unwelcome in today's dynamic and mobile workforce…" Slip op. at 22. That reading is certainly furthered by the Court's remand to consider whether the employer's counsel should be disqualified under RPC 4.4(b) for having kept and reviewed the communications.

Takeaways and Next Steps

The decision leaves employers with several questions, and they are questions that can have particular impact in the area of trade secret and restrictive covenant litigation:

1. *Should an employer want a policy that reaches or governs personal communications?* They should. Though the *Stengart* Court says that no legitimate business interest is furthered by transforming all private communications into company property, the Court misses the important point that many legitimate business interests are furthered by stemming private communications during work, the most basic being the employer's interest in having work being done at work. Indeed, the very examples earlier used by the Appellate Division as to what is accessible instantly "with the touch of a keyboard or a click of a mouse" (*e.g.*, medical records, bank accounts, phone records, and tax returns) illustrate well that these are the very sort of personal items that an employer has a great interest in keeping from being disclosed in or to the workplace. In warning employees that what is personal and private will be neither if brought into the workplace, employers are protecting themselves and their employees, and also assuring that they are not paying employees to come to the workplace to work on personal medical, financial or other matters between lunch breaks and coffee breaks. Moreover, the Court fails to recognize that many of the monitoring duties that New Jersey courts have already imposed on employers actually require one to review the content of communications to determine, for example, whether the contents include pornographic material or harassing communications. *Compare Stengart,* Slip. Op. at 28 (employer "has no need or basis to read the specific contents" of communications") (emphasis in original)*, with e.g.*, *Doe v. XYC Corp*., 382 N.J. Super. 122 (App. Div. 2005) (an employer has a duty to take "prompt and effective action" to prevent an employee that it had notice was viewing child pornography in the workplace from continuing such criminal activity) *and with Blakey v. Continental Airlines*, 164 N.J. 38 (2000) ("employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace. Besides, ***it may well be in an employer's economic best interests to adopt a proactive stance*** when it comes to dealing with co-employee harassment. The best defense may be a good offense against sexual harassment.") (emphasis added); *Lehmann v. Toys-R-Us*, 132 NJ 587 (1993) (effective anti-

harassment policies including monitoring mechanisms). How, after *Stengart*, an employer can monitor employees' personal communications in fulfillment of these obligations without viewing the contents of such communications is unclear.

2. *Does* Stengart *allow for the creation of such a policy?* It may. But drafting and then upholding that policy against legal challenge will take great care. We know this because a close reading of *Stengart* leaves the careful room to operate—as the Supreme Court says, "Our conclusion…does not mean that employers cannot monitor or regulate the use of workplace computers." For instance, *Stengart* says that a policy requiring that one work at work and not spend valuable time on personal communications is appropriate, "[b]ut employers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy." Of course, overlooked by the Court is that one cannot define the communicative activity as one outside the employer's business interests without knowing the content that would show that. Thus, the *Stengart* Court's distinction between communicative conduct and communicative content probably fails analytically, which is implicitly acknowledged by the Court's noting that an employer may have an interest in certain types of personal content as reflected in previously decided cases. (The United States Supreme Court will be addressing in the near future the subject of personal communications using an employer's electronic or computer equipment in the case of *City of Ontario v. Quon*, where arguments will be heard April 19, 2010, and a decision is expected by mid- to late-June). Nevertheless, one can enforce such a policy by blocking access to Internet-based email accounts from employee computers, or through other mechanisms and policies that focus on the time devoted to such communications as opposed to their content. Because the New Jersey court has spoken so strongly against any "no personal use" policy, one can foresee the arguments here applied to personal Yahoo accounts being raised in a future case concerning an employer's email system, though an employer there will have much stronger position on the expectation of privacy issue and employers have to hope that *Quon* will provide some pro-employer analysis to support the employer position in such a future New Jersey case.

3. *With or without a new policy, what should employers do if they find attorney-client communications on a departed employee's computer?* The first thing that one must do is collect, segregate and preserve such communications. Once that has been done, whether by one's internal IT staff or outside IT consultants, the existence of such documents should be made known to outside counsel. Then things get a little more complicated. If the employer is already in litigation, it would appear that *Stengart* compels one to either then turn over all copies to the plaintiff and his/her counsel or present them to the court for *in camera* review as to whether or not they are privileged or if privilege has been waived. Because fully reviewing the documents at issue after becoming aware that they are arguably privileged raises the possibility of later disqualification under RPC 4.4(b), an employer may even consider retaining special counsel separate from regular employment counsel to handle the application to the

court, and to advise the client concerning the issues that have arisen without running the risk of having primary defense counsel disqualified from the matter. An even more sensitive, nuanced analysis will be required if that matter is not yet in litigation, and there is no already designated third-party decision-maker available. At that point, the employer, along with employment counsel and possibly special counsel, must carefully weigh a number of practical, legal, ethical and business factors before determining how to approach the relevant issues.

Having both employment counsel and possibly special counsel familiar with those issues and the new landscape defined by *Stengart* will be essential to avoiding damaging one's position concerning claims that the departed employees are expected to file. This is especially true as it relates to departing employees in the trade secret or restrictive covenant context, where one often seeks to document through forensic computer analysis what communications occurred in preparation for a departure and what confidential information may have been transmitted. The last thing one wants when operating with a need for speed is some ancillary disqualification issue to arise for one's outside counsel. That is why segmenting roles and responsibilities is important, and it may be that special counsel can turn the tables on a departing employee and his/her counsel by demonstrating that the pre-departure communications were actually advice as to how and under what circumstances information could be taken. This would have the potential to render the communications unprivileged ones in furtherance of a "crime or fraud," which exception has been construed in New Jersey and elsewhere to apply to civil wrongs of a wide variety, and could possibly lead to the ex-employee's counsel becoming a witness in the matter, which could have its own potentially disqualifying or limiting implications.

For more information about this Client Alert, please contact:

James P. Flynn
Newark
973-639-8285
JFlynn@ebglaw.com

* * *