Coates' Canons Blog: Ethics and Employee Email

By Chris McLaughlin

Article: https://canons.sog.unc.edu/ethics-and-employee-email/

This entry was posted on August 01, 2012 and is filed under Ethics & Conflicts, Open Government, Professional Responsibility For Government Attorneys, Public Records (General), Public Records (Personnel)

Wally Whiner is in trouble once again. Wally, an employee in Blue Devil City's finance department, has been placed on administrative leave after numerous complaints from residents about his inappropriate conduct. This isn't Wally's first ride on the disciplinary carousel; two years ago he was reprimanded and put on a performance improvement plan after a subpar annual review and allegations of misconduct from his coworkers.

As city attorney, you've been asked to work with Phyllis Finance, the city's finance officer, to investigate the matter and recommend the appropriate course of action. One morning Phyllis walks into your office with a huge stack of papers with colored sticky notes attached. She explains that the papers are copies of Wally's emails for the past two years.

"I hope it's okay I went ahead and started reading these. I thought it would make your life easier if I organized them a bit," says Phyllis. "The green stickies are emails that have offensive language. The orange stickies are emails that are purely personal—messages to Wally's wife and whatnot. The red stickies are the really interesting ones—they are between Wally and his attorney talking about their plans to sue me and the city. I can't believe this guy."

"Um, thanks, Phyllis," you stammer, not sure if you should be grateful or angry.

Questions float through your head. Is the city authorized to read Wally's emails? Are the emails between Wally and his attorney privileged? Is it too late to accept that offer to join that private law firm?

You would be right to be concerned about these questions. Attorneys who willfully violate the attorney client privilege risk both ethical discipline and harm to the interests of their clients through court sanctions and evidentiary exclusions.

The N.C. State Bar's Ethics Committee has been pondering these very same questions over the past few months. (Well, not the one about career options—you'll have to make that decision on your own.)

This fall, the Bar will publish a proposed opinion that offers some guidance as to when and how an employer's attorney may read employees' emails. The committee's effort was assisted by this detailed analysis of the relevant law provided to the Bar by the N.C. Bar Association's Labor and Employment Section.

So what's the bottom line? As with so many other sticky ethical questions, the answer is, "it depends."

An employer's right to read employees' emails—including potentially privileged emails—depends on whether its employees had reasonable expectations of privacy in personal emails sent on the employer's system. (It may also depend on whether the employer is covered by state public records law, an issue I'll address in a moment.)

If an employee did not have a reasonable expectation of privacy, then the employee waived the attorney client privilege by sending personal emails over the employer's email system. When courts make determinations about the reasonableness of employees' privacy expectations, the most important factors are usually the employers' policies and practices concerning personal employee use of their computer systems.

The more explicit an employer's policy is about a complete and unqualified lack of privacy for employees who use the employer's computer systems, the more likely an employee will be found to have waived his or her privilege by using those systems to communicate with an attorney. Courts will sometimes stretch to find ambiguities in seemingly clear employer policies in order to support a reasonable expectation of privacy.

In the influential *Stengart v. Loving Care Agency, Inc*. case out of New Jersey, 990 A.2d 650 (N.J. 2010) , the court sanctioned the employer's attorney for reviewing emails between an employee and her attorney despite the fact that the employer's policy stated, "emails are not to be considered private or personal to any individual employee." The court concluded that the employer's attempt to eliminate any right to privacy in the use of its computer systems was undermined by a subsequent portion of the employer's policy that stated, "occasional personal use of [employer email systems] is permitted." This qualifying statement, according to the court, created "ambiguity about whether personal email use is company or private property."

Some employer policies state that employees have no right of privacy in "Internet usage" but do not make specific reference to personal emails. Although it's true that emails are sent via the Internet, I think most non-techies view email and surfing the web as distinct activities. Under such a policy, an employee might reasonably assume that the employer reserved the right to monitor the web pages he or she visited using the employer's computers but not the right to read personal emails sent over those computers. If so, then the employer's policy would not eliminate the attorney client privilege in employees' personal emails.

Also important to the privacy determination is the employer's promotion and practice of its computer use polices. How is that policy communicated to employees? Is it buried in a stack of papers handed to the employee on the first day of new employee orientation or is it routinely emphasized and publicized by the employer? If the policy states that the employer has the right to monitor and review employee's computer use, does the employer actually conduct such monitoring?

In *U.S. v. Long,* 64 M.J. 57 (C.A.A.F. 2006), a Marine was found to hold a reasonable expectation of privacy in her personal emails sent on the military's computer system despite a warning displayed to all employees at every computer log-on which stated, "All information, including personal information, placed or sent over this system may be monitored." Testimony from the government's network administrator revealed that the employer never read personal emails while monitoring its systems because of concerns about employee privacy. This practice, when added to the fact that all employees were provided with system passwords known only to them and not by the system administrator, led the court to conclude that the government did not have the right to read the Marine's personal emails—even those that were not privileged.

As these cases make clear, the right to privacy and privilege waiver determinations are highly fact specific. Recognizing this fact, in its proposed opinion the N.C. Bar Ethics Committee concluded that an employer's attorney may read emails between an employee and that employee's attorney only if the employer's attorney "is able to conclude, confidently and in good faith, that the privilege was waived . . . However, in deference to the bar's interest in protecting the attorney client privilege, [the employer's attorney] should err on the side of recognizing the privilege whenever an analysis of the facts and case law is inconclusive." In other words, better to be safe than sorry.

The only bright-line rule created by the N.C. Bar's proposed opinion concerns an employer's attempt to read personal emails on password-protected commercial emails systems such as Gmail that are not part of the employer's email system. In sum, don't do it! Agreeing with most courts and other bar organizations, the N.C. Bar concludes that neither the employer nor the attorney has the right to access and read personal, password-protected emails on commercial email systems even if those emails were sent using the employer's computers.

Some local governments use Gmail or other email providers as their official work email systems. If so, then the bright-line rule would not apply. The government's attorney instead would need to conduct the standard expectation-of-privacy inquiry described above.

The proposed opinion goes on to conclude that the employer has no duty to inform the employee or the employee's attorney that the employer is in possession of emails between those two parties. *[Note to my county attorney friends who attended my ethics session in New Bern last month: this is a recent change from the original version of the proposed opinion that we discussed in that session.]* This conclusion mirrors a 2011 ethics opinion from the ABA on the same

question. The employer's attorney should counsel the employer that disclosure might be in the employer's best interest so as to avoid subsequent disqualification or sanctions from a court, but at the end of the day the disclosure decision is in the hands of the client and not the attorney.

Finally, the proposed opinion touches upon the unique public records law obligations faced by government attorneys. A Catch-22 situation could arise when a public records request seeks all emails sent by a particular government employee. The government's attorney has an obligation to review the emails in question to determine if they are public records. But the attorney also has an ethical obligation *not* to read an employee's emails if they are covered by that employee's personal attorney client privilege. How can the attorney satisfy both obligations?

The proposed opinion concludes, rightfully in my view, that the public records law obligation trumps the ethical obligation in this situation. The attorney should read all emails subject to the public record request. If an email is a public record—in other words, if it was "made or received pursuant to law or ordinance or in connection with the transaction of public business" and is not subject to an exception to the public records laws—then it must be produced regardless of whether it is potentially subject to the employee's personal attorney client privilege.

Remember that the attorney-client-privilege exception to public records law covers only written communication from the local government's attorney to the local government's governing board. Emails that might be covered by an employee's personal attorney client privilege do not fall within this exception and would need to be produced if they were otherwise public records.

Thankfully, I think it highly unlikely that a particular email would be both a public record and covered by the employee's personal attorney client privilege. For the email to be covered by that privilege, it must concern the employee's effort to obtain personal legal advice.

In most situations, an employee's personal legal advice would not constitute "the transaction of public business." The email therefore would not be a public record and would not be subject to disclosure.

And then we're back to the more basic issue discussed above: the government's attorney would need to decide whether the employee waived his or her privilege by using the employer's computer system for personal email. (Sadly the opinion doesn't tell us how the attorney is expected to forget what was in those emails if they turn out to be privileged after the public records review . . .)

So what do you do with Wally Whiner's emails?

First, you need to take a detailed look at Blue Devil City's computer use policies and practices and decide whether Wally waived his privilege. Second, you should discuss with the city council the possibility of alerting Wally and his attorney that you are in possession of the emails. Third, you need to advise city employees that they should not be in the habit of reading personal employee emails without first consulting you.

Finally, you really might want to reconsider that private law firm offer.

Links

- canons.sog.unc.edu/wp-content/uploads/2012/08/Proposed-2012-FEO-5-Ewalt-July-2012.docx
- canons.sog.unc.edu/wp-content/uploads/2012/08/employee_email_law_summary.pdf