

Accessing Employee Emails

How much of the day-to-day operations of your payroll department depend on email? If you're like the majority of us, the answer varies from most to almost all. So what happens when a question arises and you know the answer is in an email sitting in the inbox of someone who is no longer with the organization? What are the privacy rights of that former employee and how do you balance those rights with your legitimate business needs?

I am sure many of you are thinking, "No problem. We have a policy that states our company email system is company property, and employees have no expectation of privacy." However, accessing employee emails is not a simple matter of writing a policy and diving in.

The federal *Personal Information Protection and Electronic Documents Act* Case Summary #2009-019 (found at http://www.priv.gc.ca/cf-dc/2009/2009_019_0529_e.cfm) states:

Even where emails sent or received by employees on an organization's system are considered to be corporate records, such emails are also the employees' personal information protected by the Act. [The Office of the Privacy Commissioner of Canada] considers it unacceptable for organizations to monitor employee email without good reason justifiable under the Act.

In this case, the employee alleged that the company had accessed his personal email account during a labour dispute and inappropriately used information from it to support disciplinary actions against him. The company denied it

had accessed his personal account and provided evidence that the complainant had forwarded emails from his personal account to his corporate account, where they were accessed in accordance with its email policy.

The Assistant Commissioner concluded the employee's complaints were not well-founded. In making her decision, she considered the company's email policy and that the corporate email account was accessed in the course of an investigation. Specifically, the company accessed the employee's corporate account only after an external investigation into a leak of confidential corporate information provided reasonable grounds for the investigator to suspect this employee.

However, although the Assistant Commissioner ruled against the former employee in this particular case, the case summary explicitly states that accessing and using employee emails would normally require the knowledge and consent of the individual employee. In other words, if your company's policy does not set out reasonable thresholds that must be met to monitor an employee's email, the policy may not provide a defence in the event of a complaint. This is the case even if you are in a jurisdiction where the requirement for employee consent is limited.

In British Columbia's *Personal Information Protection Act* Order P06-05, the Information and Privacy Commissioner found similarly to the federal Assistant Commissioner. In this case, in the course of an investigation, the organization accessed emails that contained personal information intertwined with work product and contact information. Once again, the fact that the emails

were accessed as part of an investigation provided reasonable cause to retrieve and examine emails—which suggests that such access outside the context of an investigation may be problematic.

So where does this leave in the case of departed employees' email accounts? Let the 6 P's be your guide: **Prior Planning Prevents Poor Privacy Protection.**

Employee emails may be work product but they are also entangled with personal information, so we must take precautions to minimize the risk of a privacy breach or complaint. Here are some steps you can take right now:

- 1. Determine what will be done with the email accounts of departed employees.** A good option is to keep a secure copy of former employees' email accounts for a reasonable time (depending on your business needs and other regulatory requirements), and allow case-by-case access to particular correspondences on request and with reasonable cause. Document any access.
- 2. Revisit (or write) your organization's email access policy.** It should state that while the organization reserves the right to examine email, it will only do so where a legitimate business reason exists. The exact wording and intent may vary depending on the type of organization and the technology it possesses. For example, certain kinds of data loss prevention or security monitoring tools inspect email content on a regular basis—usually for spam detection and virus protection—and employees should be informed.

3. Update your hiring process to ensure new employees are aware of your post-departure email access policy. Ideally, they should sign a form consenting to the use of their email files after departure.

4. Update your employee and manager refresher training to ensure everyone is aware of what will happen to their email accounts upon departure.


5. Update your termination process. Where employees are aware of the termination (resignations with notice, retirements, etc.), send a reminder to delete personal information from their email accounts. For all employees, prepare a consent form allowing access to their email account that departing employee must sign. As a contingency, in case departing employees

are not willing to give consent, also prepare a notice form reiterating your policy, which allows access where a legitimate business reason exists.

Most employees recognize that their email files are business records. However, in the case of disputes or conflict, making sure you have your policies and procedures aligned shows your due diligence. ■

John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at www.wunderlich.ca.

Notice: This column reflects solely the opinions of the author. Individuals are encouraged to seek qualified legal advice on points of law or matters of interpretation.



Created by the CPA, the authoritative source of Canadian payroll knowledge, and privacy expert Murray Long, this second edition is a must-have resource for those individuals who are responsible for payroll and related functions in their organizations.

Payroll, by its very nature, has always operated with the realities of confidentiality and privacy protection. This updated publication looks at how privacy laws apply to payroll management and discusses what should be done and what would be beneficial to do. The book contains over 140 pages of answers to real questions submitted by CPA members.

To order your copy (\$44.95 plus tax & shipping), visit www.payroll.ca.

THE CANADIAN PAYROLL ASSOCIATION CPA ACP L'ASSOCIATION CANADIENNE DE LA PAIE