8 FAQS: Is Monitoring Computer Use a Privacy Violation?

As an employer, you have a legitimate right to monitor how employees are using their work computers. At the same time, while the equipment might belong to you, employees commonly consider their use of work computers personal and confidential. So who's right? Here are 8 FAQs to help you get your arms around this tricky issue.

Q 1. Do Employees Have Privacy Rights vis-à-vis their Employers?

Answer: One way or another, yes. But where these rights come from and how far they extend varies by location and situation:

- **Personal Privacy Legislation:** Employees who work for federally regulated employers have privacy rights under the federal PIPEDA (*Personal Information Protection & Electronic Documents Act*). Employees who work for organizations subject to Alberta, BC or Québec regulation have rights under provincial versions of PIPEDA. But employees who work for organizations subject to the laws of other jurisdictions can't rely on a personal privacy statute for privacy vis-à-vis their employers.
- **Collective Agreements:** However, employees might have personal privacy rights in their employment information under the terms of a collective

agreement. And these privacy protections may be greater than those provided by PIPEDA or its AB, BC and QC equivalents.

- **Common Law:** Last but certainly not least, most employees have at least some form of privacy rights under common law, that is, case law made by courts and arbitrators in actual lawsuits.

Q 2. What Kind of Privacy Rights Do Employees Have?

Answer: Essentially, privacy protections limit the employer's right to collect, use and disclose personal information about their employees without the employees' consent. The question that arises, then, is whether an employer needs employees' consent to monitor how they use their work computers and impose discipline for improper uses. Employees and unions will claim that these are the kinds of collections and uses of personal information for which employees must give consent.

Q 3. Don't Employers Have Rights to Use that Information to Run Their Business?

Answer: Yes. More specifically, employers are allowed to collect, use and disclose personal information about employees to perform legitimate business functions. The employer's argument would be that monitoring employee computer use is a legitimate and important business function because of the risks of employee abuses like:

- Engaging in web surfing, social networking and other personal activities that reduce their productivity;
- Downloading, viewing and sending pornographic, racist and other offensive material;
- Communicating messages that demean colleagues, the company and customers;
- Misappropriating confidential or proprietary information; and
- Carrying out business activities that are illegal or a conflict of interest.

Q 4. Does the Employer's Right to Monitor Computer Use Outweigh Employees Privacy?

Answer: That is precisely the question a court, privacy tribunal or arbitrator would have to answer if an employee brought an actual case against the employer for monitoring computer use. For employers, the good news is that there have, in fact, been a number of such cases and most of them have gone the employer's way. For example, according to a leading case from Alberta, "in the information technology world today," great harm can be done to companies "with the click of a mouse." Accordingly, "an employer is entitled not only to prohibit use of its equipment and systems for [improper] purposes but also to monitor an employee's use of the equipment to ensure compliance" [*Poliquin v. Devon Canada Corp.*, [2009] A.J. No. 626, June 17, 2009].

But each case is different and monitoring has been found to cross the line where the information wasn't vital or appropriate to access and there were less intrusive ways for employers to obtain it. In other words, while monitoring computer usage is generally okay, it still must be done in a "reasonable" way.

Example: An employee filed a privacy complaint with the Alberta Privacy

Commissioner after discovering that his employer had installed keystroke logging software on his computer without his knowledge. The Commissioner ruled that the employer could and should have used less intrusive means to monitor the employee's work and informed the employee that it was monitoring him [*Order F2005-003*, Alberta Information and Privacy Commissioner, June 24, 2005].

Q 5. How Do I Know Where to Draw the Line?

Answer: As the HR director, you need to understand what is and isn't permissible. *Basic Rule:* You can access computer data as long as employees don't have a "reasonable expectation of privacy" in the material. "Reasonable expectation" is based on 2 things:

- **What the employee actually expected.** The employee must have what's called a subjective expectation of privacy, i.e., he must sincerely believe that the information in his computer will be kept from his employer. Thus, employees who know that their computer data can't be kept private have no claim. The employee's use of passwords, hidden files, encryption and other security conventions is evidence of a subjective expectation of privacy.
- **Whether the employee's privacy expectation was reasonable.** A sincere expectation of privacy isn't enough. Employees must also show that it was reasonable for them to have such an expectation. Reasonableness is an objective standard that's based on what a person of average prudence would expect. That makes it harder for employees to argue that a privacy expectation was reasonable when the computer equipment is owned by the company; an employee has a stronger case when the data the employer accesses is stored on a personal computer that the employee owns and uses for work purposes.

Q 6. How Do I Protect My Organization's Right to Monitor Employee Computer Use?

Answer: Having to argue in front of a judge or arbitrator what was on an employee's mind and what should have been on his mind is a dicey proposition. The best strategy is to find a way to put an end to any privacy expectations by your employees *before* they ever arise.

Q 7. How Do I Keep Employees from Having Reasonable Expectations of Computer Privacy?

Answer: Adopt a policy stating that data kept on company computers and systems is *not* private and is, in fact, subject to monitoring. As long as it's clearly written and consistently implemented, a computer use policy will make it extremely difficult for employees to claim they have a reasonable expectation of privacy in their computer files.

Example: During routine monitoring of the server and network, the IT director of an Ontario high school found a file containing nude photographs of a student on the hard drive of a laptop assigned to a teacher. The school gave the file to the police who charged the teacher with child pornography. The teacher argued that he had a reasonable expectation of privacy in the material. The court found that the teacher had a subjective expectation of privacy—the pictures were in a "grey file" under "My Documents" and the laptop was password-protected.

The court ruled that his expectation wasn't *reasonable*. Although password-protected, the laptop was owned by the school. The Canadian Supreme Court ultimately ruled the other way and said the computer use policy didn't eliminate the teacher's expectations of privacy in his hard drive [*R. v. Cole*, 2012 SCC 53, Oct. 2012].

Q 8. How Do I Create Computer Use Policy?

Answer: The *Cole* case doesn't mean computer use policies won't work. In fact, the Court even acknowledged that such policies can diminish employees' reasonable privacy expectations. The significance of *Cole* is that it illustrates the importance of creating the right policy.

As a starting point, you can use the Insider's Model Computer Use Policy. Although you need to tailor it to your own workplace, the Model Policy illustrates what to include in your own policy, including a clear statement that:

- All computers and information technology systems provided to employees are owned solely by the company and aren't the employee's property [Policy, para. 1];
- Computers and equipment must be used solely for work-related purposes. It's also important to list prohibited uses, like surfing the web, downloading pornographic, racist, defamatory or other offensive material and downloading or transmitting confidential company information [Policy, para. 2];
- Employees have no right to expect that their files, emails and other data will be kept private [Policy, para. 3];
- The company will monitor computer usage and emails for purposes of security, network maintenance and to verify compliance with the Policy. Our Policy goes the extra step of spelling out that the company can hang onto and review emails, including showing them to third parties [Policy, para. 4];
- The obligation to obey the Policy is an implied part of the employee's contract. Several courts have recognized that affording the Policy the status of contract is an indication to employees of its seriousness and thus easier to enforce [Policy, para. 5];
- Employees agree not only to obey but enforce the Policy if they become aware of potential violations. As a practical matter, requiring employees to report violations can make the policy more effective and easier to enforce. On a more subtle plane, it might also make a court less likely to side with the employee in a dispute. Note that in upholding the right to monitor spelled out in a computer use policy despite privacy concerns, the *Poliquin* court went to great pains to point out that the employee held a supervisory position and thus participated in enforcing the policy. Consequently, his violations were less easy to accept [Policy, para. 6].