



Employee computer use and privacy

You are in-house counsel for a new dot-com retailer, XYZ.ca Inc., which has not yet established a computer/Internet/e-mail policy for employees. One day Amy, the director of XYZ.ca Inc.'s information technology department, reveals in confidence that while performing maintenance on XYZ.ca Inc.'s network, she discovered that Bob, a web designer, has been accessing and storing adult images from the web on the internal hard drive of the company's workstation computer, which he uses.

- 1** Amy found Bob's offending material in a folder on his computer that was password locked, hidden from other network users, and labelled "personal." Can Bob successfully assert that he has a reasonable expectation of privacy over these files so as to undermine the propriety of Amy's discovery of the images?

 - (a) No. XYZ.ca Inc. has unlimited rights to monitor Bob's workstation computer for any reason as it is the company's property.
 - (b) Yes. Bob's efforts to indicate that personal material was stored on the hard drive were sufficient to prohibit Amy from opening the folder.
 - (c) Maybe. It depends on all of the circumstances, including the manner in which the material was found.

- 2** The next day, Carlotta, the director of human resources at XYZ.ca Inc., contacts you to determine if there are grounds to discipline Bob, in light of the fact that Bob has not breached a written policy and there was no circulation of the offending material. Should Bob be disciplined?

 - (a) No. Discipline of an employee should occur only if the employee has breached a written workplace policy.
 - (b) No. Bob's conduct has not caused any harm (e.g. no one has complained).
 - (c) Yes. Termination for cause is objectively reasonable in the circumstances.
 - (d) Yes. Bob's conduct impacts XYZ.ca Inc.'s interests in the employment relationship and this is grounds for discipline.

- 3** Carlotta later reports to you that another employee, Dan, made disparaging remarks about XYZ.ca Inc. on his Facebook page, including criticizing his supervisor, accusing the company of being "run by crooks," and encouraging his friends to boycott XYZ.ca Inc.'s products. What can you do?

 - (a) Nothing. What Dan says or does outside of work and on his own time is beyond the scope of the employer's interests.
 - (b) Investigate the allegations, including monitoring Dan's Facebook account and determine whether Dan is the author of these statements and, if so, discipline him.
 - (c) Terminate Dan for cause.

- 4** Emily comes to you complaining that Frank, a fellow employee, has posted threatening and derogatory remarks about her on Twitter. There is a personality conflict between these two employees. You should not get involved in this dispute, which is outside of the workplace.

 - (a) True
 - (b) False



1 (C) While the law recognizes an employer's right to monitor the workplace, this right may be subject to an employee's reasonable expectation of privacy in some circumstances. *R. v. Cole*, 2011 ONCA 218 (a criminal case), sets out the scope of an employee's reasonable expectation of privacy when using computer equipment supplied by the employer.

In the case, Richard Cole, a teacher, had stored nude photographs of a student in a hidden folder on the hard drive of his laptop supplied by the employer, the school board. The folder was discovered when the school's computer technician observed a large amount of activity between the teacher's laptop and the school's server. The technician accessed the hard drive to conduct a virus scan and found the hidden folder. The school board had given teachers permission to use the laptops for personal use. There was no written policy permitting the school board to monitor the computer equipment or to supervise the employee's use of the laptop.

In determining whether Cole had a reasonable expectation of privacy over these files, the court examined all of the circumstances, including efforts made by the teacher to assert privacy over some of the files on the hard drive. The court held that, in the circumstances, the teacher's reasonable expectation of privacy was subject to an implied right of the school board to search computers as part of routine network maintenance. To the extent that the teacher's private documents were gathered by the school board during routine network maintenance, there was no breach of the teacher's reasonable expectation of privacy.

Without a written policy providing XYZ.ca Inc. with an unlimited right to monitor Bob's computer, Bob may have a reasonable expectation of privacy over the file he has marked private; however, based on the Cole decision, Amy's routine network maintenance, which led her to access Bob's computer and the relevant files, might not constitute a breach of his reasonable expectation of privacy.

2 (D) In the absence of a written policy that clearly sets out the permitted uses of company computers, XYZ.ca Inc. may still have grounds to discipline Bob if his conduct constitutes a breach of loyalty to his employer, is indicative of a failure to provide his full time and attention to his work, or if his conduct is of such a nature that it cannot be condoned by the employer.

All employers should develop a clear computer/Internet/e-mail policy that sets out the permitted uses of this technology; provides for the employer's right to monitor an employee's computer, Internet and e-mail use; explicitly provides that the employee has no reasonable expectation of privacy over e-mails and other information stored on the employer's computer; and sets out the consequences for improper use. The policy should also apply to hand-held personal digital assistants (PDAs).

3 (B) and, in some circumstances, (C). This issue raises the need to balance the employer's right to protect its economic interests with the employee's reasonable expectation of privacy. A recent British Columbia labour arbitration decision found that an employee did not have a reasonable expectation of privacy when he published offensive and derogatory comments about his employer on his Facebook website, which was accessible to a very large number of people, including other employees.

An employer should investigate the allegations in order to determine whether the offending comments are in fact attributable to the employee. The employer must be careful about monitoring the employee's social networking site and possibly acquiring information not otherwise known about the employee and, if the employee is disciplined or terminated, risk being accused of relying on that information (which reliance may in some circumstances be improper). Depending on the nature of the employee's comments and the employee's past work record, discipline may be warranted. Termination for cause has been upheld in circumstances where the comments published on social networking sites were egregious and damaging to the employer's business and reputation.

4 (B) An employer has a duty to ensure a workplace free of harassment. While the complaint is about conduct outside of the workplace, the fact that Emily has raised these concerns with her employer warrants a further investigation on the part of the employer in order to determine whether the conduct is indicative of workplace harassment, or signals a risk for workplace violence. Recent amendments to the Ontario Occupational Health and Safety Act require an employer to be proactive in addressing workplace harassment and violence by implementing workplace harassment and violence policies, training employees on these policies, and performing risk assessments for workplace violence.

YOUR RANKING?

- **One or less correct:** *might be time to brush up*
- **Two correct:** *not bad, but some further work needed*
- **Three correct:** *very well done, but not perfect*
- **Four correct:** *impressive*



A daily blog of Canadian Legal News
 Powered by *Canadian Lawyer & Law Times*
canadianlawyermag.com/legalfeeds