dentons.com

DENTONS

Insights and Commentary from Dentons

On March 31, 2013, three pre-eminent law firms—Salans, Fraser Milner Casgrain, and SNR Denton—combined to form Dentons, a Top 10 global law firm with more than 2,500 lawyers and professionals worldwide.

This document was authored by representatives of one of the founding firms prior to our combination launch, and it continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

Child-Specific Privacy Standards in Context

This decision provides further direction for those who are conscious of the protection of the privacy of children and who wonder about the specific content of those obligations. Unlike the United States, Canada has no *Children's Online Privacy Protection Act* [*COPPA*]. While there are set age and child-specific standards in Canadian criminal laws, we have no set age and child-specific standards in our federal privacy legislation, the *Personal Information Protection and Electronic Documents Act*.[4]

The Supreme Court noted that:

> Recognition of the *inherent* vulnerability of children has consistent and deep roots in Canadian law. This results in protection for young people's privacy under the *Criminal Code*, R.S.C. [...] the *Youth Criminal Justice Act* [...], and child welfare legislation, not to mention international protections such as the *Convention on the Rights of the Child* [...], all based on age, not the sensitivity of the particular child.

The court has sent a message that in contexts where children may be particularly vulnerable—even when the child is 15 years old, and the context is Facebook—the law will protect their privacy on an objective basis based on age, not individual maturity or temperament.

[*Editor's note*: **Margot Patterson** is Counsel with Fraser Milner Casgrain LLP. Margot is recommended by Best Lawyers in Canada 2013 as one of Canada's leading lawyers in the area of Communications Law. She blogs at <www.datagovernancelaw.com>.]

---

1 [2012] S.C.J. No. 46 (S.C.C.).

2 *Ibid.* at para. 27.

3 [1988] S.C.J. No. 67 (S.C.C.).

4 S.C. 2000, c. 5 [*PIPEDA*]. While the Office of the Privacy Commissioner of Canada ("OPC") has published useful presentations such as *Understanding Your Online Footprint: How to Protect Your Personal Information on the Internet*, available at <http://www.youthprivacy.ca/en/Presentation/Speaking_Notes_4-6_Youth_Presentation_Package_EN.pdf>, the OPC's standard statement referencing informed consent for the collection, use, retention, and disclosure of personal information from children is simply that "it is difficult to obtain meaningful consent from children."

• OWNERSHIP & POLICIES NOT DETERMINATIVE OF PRIVACY IN ELECTRONIC DEVICES •

Timothy M. Banks
Fraser Milner Casgrain LLP

Employee Privacy at Work

Are device ownership and acceptable use policies determinative of an employee's expectation of privacy?

Many employers attempt to diminish the expectations of privacy of employees in work-supplied electronic devices through "computer use" policies. These policies typically state that work-supplied devices are to be used solely for work purposes and that the employer may monitor the employee's use of these devices. These policies are perhaps honoured more in their breach with employees frequently accessing online banking, social networks, and other websites and online applications from workplace-supplied computers and smartphones.

Leaving aside the practical ineffectiveness of prohibiting personal use, there is a new complication on the horizon in the form of the "bring-your-own-device" ("BYOD") movement. BYOD means that the employer can no longer claim a proprietary interest in the device, which is usually stated as the basis for justifying the employer's right to control and monitor the use

of the device. With BYOD, the employee will own the laptop or smartphone. This limits the employer's legal and practical ability to control the employee's use of the device. Nevertheless, the employer has an interest in ensuring that the device is secure and may install software or applications onto the device. Indeed, the employer's IT department may provide support for software and applications loaded onto the device, justifying some control of the device.

Supreme Court of Canada Examines Constitutional Rights

On October 19, 2012, the Supreme Court of Canada released its much-anticipated decision in *R. v. Cole*.[1] The court considered whether an employee had a reasonable expectation of privacy in material on a work-issued laptop. The question was whether the computer could be searched by the police without a warrant if the employer handed the computer over to the police. The court concluded that the employee had a reasonable expectation of privacy and that a warrant would ordinarily be required. However, in the circumstances of the case, the majority of the court declined to exclude the evidence as a remedy for the breach of the employee's constitutional right to be free from unreasonable search and seizure.[2]

The court's reasons establish the following important privacy principles:

- In assessing the privacy interest, the focus is on the informational content of the device and not on the device itself.[3]
- Ownership of the device is a relevant factor but not determinative in determining whether an expectation of privacy is reasonable.[4]
- Computers used by employees may "contain information that is meaningful, intimate, and [touching on the user's] biographical core."[5] The information may expose biographical information regarding "the likes, interests, thoughts, activities, ideas, and searches for information of the individual user."[6]
- Everyone in Canada has the constitutional right to privacy from the state (law enforcement) with respect to this type of personal, biographical information[7] on workplace computers, provided that it would be reasonable to expect the computer to be used for personal purposes.[8]
- Workplace-acceptable use policies may diminish an employee's reasonable expectation of privacy but will not, on their own, remove the expectation entirely.[9] The operational context that must be examined to determine whether an employee's expectation of privacy is reasonable will also include the practices and customs of the employer, which may include the reality that workplace-issued devices are permitted to be used by employees for incidental personal use.[10]

Possible Implications for Employers

R. v. Cole was decided in the criminal law context in a situation in which the employer was a public body that was conceded to be subject to Canada's *Charter of Rights and Freedoms*.[11] Caution should be exercised, therefore, in extrapolating the principles in *R. v. Cole* to the private sector and non-criminal contexts. Indeed, the majority of the court expressly stated that it would "leave for another day the finer points of an employer's right to monitor computers issued to employees."[12]

However, a few points are clear. The court concluded that even if the employer has lawful possession of a device for the employer's own administrative purposes, this does not mean that the employer can waive the reasonable expectation of privacy of the employee by turning the

device over to the police;[13] nor does an employer's rights to monitor vest the police with lawful authority to search the device for the purposes of a criminal investigation.[14] This does not mean that the employer cannot tell the police what it has found, which could be used by the police to obtain a warrant.[15]

In addition, *R. v. Cole* demonstrates that ownership and acceptable use policies will not be determinative in assessing whether employees have a reasonable privacy interest in information stored on devices used for employment. Ownership and acceptable use polices may still be relevant, but the court will consider the totality of circumstances of the use of the device.

In a BYOD environment, the privacy interest of the employee may be even greater than it was in the circumstances of *R. v. Cole*. If an individual may have a reasonable expectation of privacy in the information stored on a workplace-issued device, it is likely a shorter step to concluding that an individual has a reasonable expectation of privacy in the context of a BYOD program. Employers should consider whether their administrative policies and practices are appropriately tailored to the operational reality that employees are using workplace-issued devices and BYODs for personal use and how that may affect their ability to monitor employees, particularly where that monitoring is surreptitious. Moreover, an overreaching policy will not provide comfort to an employer if it is out of step with the practical reality of the workplace.

[*Editor's note*: **Timothy M. Banks** is a partner in the Business Law Department of Fraser Milner Casgrain LLP and national lead for the firm's privacy practice. He blogs at <www.datagovernancelaw.com>.]

---

1 [2012] S.C.J. No. 53.

2 Justice Abella dissented, finding that the Charter-infringing conduct was serious and that there were no exigent circumstances or other legitimate reasons preventing obtaining a warrant for what was an entirely unrestricted search of the computer.

3 Majority Reasons (Fish J.) at para. 41.

4 *Ibid.* at para. 51.

5 *Ibid.* at para. 58.

6 *Ibid.* at paras. 3 and 47.

7 *Ibid.* at paras. 34–37, 42–43, and 45–48.

8 *Ibid.* at para. 1.

9 *Ibid.* at para. 52.

10 *Ibid.* at paras. 53–58.

11 *The Constitution Act, 1982*, being Schedule B to the *Canada Act 1982 (UK),* 1982, c. 11.

12 Majority Reasons, supra note 3 at para. 60.

13 *Ibid*. at paras. 74–79.

14 *Ibid*. at para. 67.

15 *Ibid*. at para. 73.