BLG PUBLICATION

Borden Ladner Gervais

Workplace computers and electronic devices: protecting confidential information and preserving evidence

Part Two: We've secured the evidence but can we look at it?

If you have not read part one of this four part series, see the June issue of BLG's L&E News.

Having taken appropriate measures to protect your confidential information and secure the evidence showing that an employee may have unlawfully copied, transferred or destroyed your company information and now that you have this evidence in hand (in the form of a laptop, a hard drive, a smartphone, a USB key or any other type of storage device), you ask yourself a very important question: am I allowed to look at and use whatever information or data I have found on my employee's workplace device?

You might be tempted to answer "yes, it's the company's device, we can do what we want with it!" After all, the company paid for the device, it paid for the internet connection data service, it paid the employee while he or she was using the device, so why can't the company look at and use any information it finds on an employee's workplace device?

The answer is not so simple because employees have a "reasonable expectation of privacy" in the workplace.

In its October 2012 decision in *R.* v. *Cole*,[1] the Supreme Court of Canada clearly stated that "Canadians may reasonably expect privacy in the information contained on [...] *work* computers, at least where personal use is permitted or reasonably expected". Given that "computers that are reasonably used for personal purposes — whether found in the workplace or the home — contain information that is meaningful, intimate, and touching on the user' s biographical core", the SCC took the position that everyone can expect privacy in personal information of this kind. That being said, with respect to a workplace computer, there will be a "diminished expectation of privacy" when compared to a personal computer used at home.

It is important to note that the decision in *R.* v. *Cole* concerns a criminal matter which brought into play the *Charter of Rights and Freedoms*, which does not apply to private sector employers. However, the principles articulated in this decision have been imported into the labour and employment law context, both before civil courts and in grievance arbitrations, in many provinces across the country.

What does this mean from a practical perspective? First, before engaging in a process of searching for or analyzing information on an employee's workplace device (computer, smartphone, etc.), the employer should have reasonable grounds to do so. A process whereby the employer randomly or regularly searches employees' workplace devices could be a violation of their privacy. Rather, employers should perform searches only when they have some evidence or information that leads them to reasonably believe that an act of misconduct has occurred, such as, for example, that an employee may have illegally copied, transferred or destroyed company information.

Second, workplace policies governing the use of devices and the confidentiality of their content can be useful in that they can set out what type and frequency of personal use of workplace devices is permitted, if any. Policies can also mention what information belongs to whom and who can have access to it. However, in *R.* v. *Cole*, the SCC mentioned that "while workplace policies and practices may diminish an individual's expectation of privacy in a work computer, these sorts of operational realities do not in themselves remove the

expectation entirely". Arbitrator Allen Ponack has written "given the ubiquitousness of email, smart phones, tablets, and the like it is almost impossible to conceive, short of erecting an absolutely impenetrable firewall, how some personal use will not occur".[2] Therefore, employers cannot rely on workplace policies to fully circumvent employees' reasonable expectation of privacy.

Third, once the employer (or the computer forensics expert), is engaged in the process of searching for or analyzing information found on an employee's workplace device, this should be done in the least intrusive way possible, and reasonable steps should be taken in order to protect the employee's privacy. Such steps could include limiting the scope of the search to that which is necessary in order to find proof of the employee's wrongdoing and avoiding emails or text messages that are of a purely personal nature (exchanges between family members or with legal or financial advisors, for example). Also, if the search must include emails or text messages that are of a purely personal nature, then the person conducting the search should exclude from their report any information of a personal nature that is not directly relevant to the alleged wrongdoing.

Stay tuned for part three in the August edition of L&E News when we will provide practical tips when using the services of a computer forensics expert.

[1] *R.* v. *Cole*, [2012] 3 SCR 34, 2012 SCC 53 (CanLII)

[2] *Saskatchewan Government and General Employees Union* v. *Unifor Local 481*, 2015 CanLII 28482 (SK LA)

AUTHOR

Patrick Trent
T 514.954.3154
PTrent@blg.com

Borden Ladner Gervais

BLG OFFICES

Calgary

Centennial Place, East Tower
1900, 520 - 3rd Avenue S.W.
Calgary, Alberta, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, Québec, Canada
H3B 5H4

T 514-954-2555
F 514-879-9015

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, Ontario, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Toronto

Scotia Plaza
40 King Street West
Toronto, Ontario, Canada
M5H 3Y4

T 416.367.6000
F 416.367.6749

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, British Columbia, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415