BLG PUBLICATION

Borden Ladner Gervais

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

Sooner or later, most employers who provide their employees with computers or electronic devices to access and use company information[1] will be faced with situations in which they suspect current or former employees of having copied, transferred or destroyed company information without the right to do so.

This is part one of a four part series in which we will discuss this matter from a legal and practical perspective. Where an employer believes that an employee may have engaged in such behaviour, the employer's actions should be focused on two key objectives: protecting the confidentiality of the information in question and securing the evidence of the wrongdoing.

In this first part, we will provide tips regarding what an employer should do when they are concerned that a current or former employee has unlawfully copied, transferred or destroyed company information. These are the do's and don'ts with respect to the crucial initial minutes and hours following the time at which such a situation arises.

In the second part, we will explore the legal tests governing an employer's right to access and analyse information (emails, documents, recordings, videos, metadata etc.) on their employees' workplace computers or electronic devices. In the third part, we will provide practical tips when using the services of a computer forensics expert. In the fourth and final part, we will review some of the measures employers can take to protect their confidential information which is accessible via computers or electronic devices.

Part One: We think he's copied everything, what do we do?

There are a number of circumstances in which an employer can have grounds to believe that an employee has unlawfully copied, transferred or destroyed company information. Common examples are:

- An employee is regularly accessing information which isn't related to his duties;
- An employee uses external storage devices (USB keys, external hard drives, etc.) with his workplace computer;
- An employee regularly sends emails from his work email address to a personal email address or uses his personal email address for most of his work related emailing; or
- A former employee fails to return, or takes a long time to return, a workplace computer or electronic device after the termination of their employment.

When a situation such as this arises, the employer must use the utmost caution in its efforts to protect its confidential information and secure the evidence of the wrongdoing.

In order to protect its confidential information, the employer should consider taking one or some of the following measures:

- Restricting, in whole or in part, the employee's access to the employer's confidential information via its computer systems;
- Asking the employee to hand over all external storage devices which have been connected to their workplace computer or electronic device;

- Asking the employee to hand over their workplace computer or electronic device and providing them with a replacement.

Obviously, by asking the employee to hand over certain devices, the employer will reveal to the employee the fact that he has concerns regarding the employee's conduct. Therefore, such measures should only be taken as a last resort in order to avoid the imminent disclosure of confidential company information.

In circumstances where the risk of imminent disclosure is low or where the employer is uncertain as to whether or not the employee is engaged in any wrongdoing, the employer can take certain measures to monitor the employee's use of their workplace computer or electronic device. These will be discussed in greater detail in Part Two of this series.

However, where the employer has actually taken possession of the employee's workplace computer or electronic device, we recommend the following:

- The computer or electronic device should be turned off and kept in a secure and locked location;
- Be aware that the simple action of turning on a computer or electronic device can modify data stored on the device which, in turn, can compromise the evidence on the computer or device. Therefore, the data stored on the computer or electronic device should not be accessed by company employees, including IT, no matter how knowledgeable they are with respect to computers, software and electronic devices. The only exception to this recommendation is where the company employee accessing the computer or device is trained in computer forensics analysis and has the appropriate hardware and software to access data without compromising it;
- The employer should keep a written chain of possession report of the workplace computer or device which details when and where the employee handed over the computer or device, who it was handed over to and where it was kept. This report should be updated every time the computer or device changes hands until such time as it is in the hands of a computer forensics expert.
- If the employer decides that it wants to access the data on the workplace computer or device, then it should be sent to a computer forensics expert for data recovery and processing in such a way that the evidence will be secured and preserved.

Stay tuned! Part Two will be in the July edition of L&E news.

[1] I.e. “workplace computers and electronic devices”.

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