Electronically Speaking

The admissibility of digital surveillance images may be affected by recent amendments to the *Canada Evidence Act* **By Elliott Goldstein**

The *Canada Evidence Act* (CEA) applies to all criminal proceedings and all civil proceedings and other matters over which the federal Parliament has jurisdiction (for example, federal courts, administrative tribunals and hearings). Recently amended by Part III of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the CEA now includes the addition of new sections that may apply to surveillance images stored in computer systems, DVRs or digital storage media.

Specifically, the PIPEDA amendments define an "electronic document" to mean "data (that is, representations of information or of concepts, in any form) that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout, or other output of that data."[1]

This definition of "electronic document" is broad enough to include a group of surveillance images recorded on the hard drive of a DVR. But, before the electronic document (for example, the surveillance images) can be admitted as evidence, it must be authenticated by any person seeking its admission. Authenticity can be proven by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

The PIPEDA amendments also affect the way in which the best evidence rule is satisfied in respect of electronic documents. The rule is satisfied "on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored ... The integrity of an electronic documents system (for example, a computer system) by or in which an electronic document is recorded or stored is proven:

- by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;
- if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
- if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it."

What this means is the integrity of surveillance images can be corroborated by proving that the system used to record them was operating properly and the images were recorded by an opposing party; or the images were recorded by a disinterested third party "in the usual and ordinary course of business."

For the purposes of determining admissibility, the court may consider "any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavor that used, recorded or stored the electronic document and the nature and purpose of the electronic document."

This points out the importance of having written procedures and guidelines, and following them, when recording and storing surveillance images.

If the surveillance image is in the form of a printout (for example, a video print made from a computerized surveillance image), then the printout will satisfy "the best evidence rule if the printout has been manifestly and consistently acted on, relief or used as a record of the information recorded or stored in the printout."

Proving the above can be done by way of affidavit evidence. However, the deponent of the affidavit (that is, the person making it) may be cross-examined by an adverse party.

The aforementioned legislative amendments do not affect any rule of law relating to the admissibility of evidence, except the rules relating to authentication and best evidence. Therefore, the party offering the surveillance images must still prove that their contents are relevant, true and accurate, and fair (that is, not misleading). Also, it must be shown that the probative value of the surveillance images outweighs their prejudicial effect.

Note that these amendments to the CEA do not apply to surveillance images recorded by conventional analog video recorders. It is only those images that are recorded and stored by a computer system or other similar device that are affected.

However, given the recent proliferation of DVR systems containing a computer hard drive as the recording mechanism, the sections of the CEA will become increasingly important. Unfortunately, because these amendments are so new, there are no reported cases decided under these sections. As time passes, there will be – and rest assured that those cases will be analyzed and presented here.

Elliott Goldstein, BA, LL.B., is a barrister and solicitor and visual evidence consultant based in Toronto, Ontario.

Author's Note

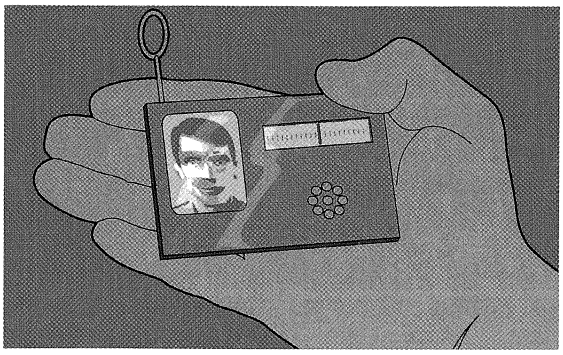
1 See CEA, s. 31.8 – Definitions. All quotations taken from ss. 31.1 - 31.8.

CANADIAN SECURITY
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT

December 2003 I Volume 25 Number 9

COVER STORY I

FEATURES I



DEPARTMENTS I