Preserving E-mail and Electronic Evidence

Like paper documents, computer files must be disclosed

By Michael Fitz-James, LL.B., B.C.L.

TORONTO — Even when a document has no physical existence outside a computer disk, it still may be ordered produced as evidence for a present or future lawsuit, says Toronto's Teresa Howarth, a litigation counsel with Blake Cassels & Graydon LLP.

Many businesses assume that because of its informality, e-mail and other electronic data doesn't count as something that needs to be preserved and later produced, she told an October 26 seminar entitled "Litigation Briefs: A Snapshot of Recent Developments in The Realm of Litigation."

Howarth points out that every Canadian jurisdiction has court rules which impose a specific obligation on both plaintiffs and defendants to "secure and disclose documents which are not privileged."

In Ontario for example, Civil Procedure Rule 30.02 requires disclosure of "every document" relevant to any matter in issue — and "document" is broadly defined to include "information recorded or stored by any means or device."

Ontario's courts, she says, have already determined (specifically when the Reichmann family sued Toronto Life magazine for libel) that material merely stored on a computer disk, even if it's never been printed out, must still be produced for a lawsuit.

"In our own practice, we see e-mail becoming significantly important in commercial disputes," she says, "and once litigation is started, or even contemplated, a duty arises to preserve such evidence.

"A decision to destroy such documents carries a significant risk. Courts have imposed sanctions on businesses which have destroyed documents when they knew, or ought to have known, that the information was required for litigation."

The destruction of electronic documents can leave a party vulnerable to an adverse inference that the information was detrimental to the destroyer's case.

Moreover, clients should be aware there can be significant Criminal Code penalties when there's a wilful destruction of documents required for criminal proceedings.

Howarth stresses that businesses preserving electronic data should segregate communications that are privileged from those that aren't. Electronic exchanges with legal counsel are almost always privileged, as are communications about a lawsuit itself or its settlement.

But everything else is produceable, including material which may have been already been deleted, but nevertheless remains on the hard drive. While the content of the wastepaper basket may have be recycled long ago, an electronic trashcan can be gold mine of evidence, says Howarth.

Witness Oliver North in the Iran-Contra hearings, she says, when investigators discovered deleted e-mails on an automatic back-up tape and used them to undermine North's testimony.

Plus it's not enough, she points out, to write "confidential" on a document to preserve its private or privileged character, especially if it's been given a wide distribution.

An employer's published e-mail policy can do much to head off lawsuits in the first place, and if they do happen, offer some protection against adverse evidence being captured by an opposing party.

Employees should be made aware that the computer system is the property of the company and should be used only for legitimate business purposes. Moreover, employees should be advised that anything produced on them is subject to production in a lawsuit, says Howarth.

As well, guidelines should be created to prohibit defamatory, discriminatory, sexist or harassing material, with employees clearly informed that discipline or dismissal could result from violation of this policy.

As well, a company-wide document retention and destruction policy should be created, says Howarth, to guard against inadvertent deletion of data which may be useful in litigation.

Ottawa lawyer Lewis Eisen, executive director of the Canadian Society for the Advancement of Legal Technology, says many employers aren't sure how far they can go to stop their workers using the company e-mail to ride their private hobbyhorses.

Eisen says it's easy to snoop on employee e-mail — there are many low-cost software packages which allow this. While there haven't been any Canadian court cases on e-mail privacy, U.S. cases have consistently found if the employer owns the machine, it owns the information inside the machine as well — even if it's the employee's personal correspondence.

But snooping is time-consuming and a hassle says Eisen. He doesn't believe there's a lot of snooping going on, but many companies tell employees their computer use is being monitored so they'll be careful about what they write.

In a recent financial services industry seminar, Geoffrey Horrocks, Chief Compliance Officer with the Toronto Dominion Bank says there's been a "great hue and cry" by U.S. compliance officers who are having trouble "supervising" the mind-boggling flow of e-mail coming out of financial service firms.

There are software solutions, he says, which target specific "naughty words" in outgoing e-mail — terms like "guarantee," "buy it back," and "apologize" — but "there's a huge amount of personal communication going on — and the staff don't like you looking at their personal business."

Plus "compliance resources are scarce," says Horrocks, and he doubts whether a comprehensive job could be done in supervising employee e-mail.