



Martin Aquilina, Partner
Business Law
Ottawa
(613) 786-0170
martin.aquilina@gowlings.com

Martin practises in the area of business law, with a focus on corporate and securities matters. He has experience in financial services regulatory matters and private placements of both equity and debt securities, as well as mergers and acquisitions.

E-Mail Archiving by Securities Registrants

Martin Aquilina

E-mail has become an integral tool in the modern business world. However, its widespread use in the workplace and our personal lives has also given rise to new risks and obligations. As e-discovery specialists Susan Wortzman and Susan Nickle note, the “constant transmission and informal nature of electronic documents such as e-mails induce individuals to express thoughts or information they would be unlikely to ... state in more formal correspondence.”¹ And in litigation, Wortzman and Nickle add that because e-mails may contain information that is unavailable anywhere else, they may be the “key to ultimate success or failure of the case.”

Accordingly, securities regulators may seek to strictly curtail the deletion of old e-mails. Some commentators believe the Canadian Securities Administrators (CSA) may have done just that in its proposed record keeping rules. National Instrument 31-103 – Registration Requirements (NI 31-103), which may come into effect by year-end, requires that registered firms (registered dealers, advisers, and those in the new category of investment fund managers) keep their records “safe and in a durable form.”² In the first two years dating from their creation, the form in which such records are stored must permit their “prompt” provision to the regulator. Thereafter, it must be possible to provide the records within a “reasonable period of time.” Activity and

relationship records must be retained for a minimum of seven years from the date of the activity or the date the client relationship ends, as the case may be. (Investment fund managers, as well as market dealers who do not handle, hold or have access to client assets, are exempt from these requirements.)

Yet retaining e-mails extensively and indiscriminately poses certain risks. Alan M. Gahtan, an expert in information technology law, believes that it may generally be “desirable, from a preventive risk perspective, to make greater use of selective backup strategies.”³ In Ontario, a firm’s electronic documents are discoverable, and courts have been willing to give the opposing side extensive access to them. Because people tend to share their personal opinions and otherwise speak freely in e-mails, considerable risk is associated with such access: exchanges might be misinterpreted or taken as the firm’s position at trial. Employee privacy issues provide another reason for adopting a selective e-mail retention policy. A firm must be mindful of these issues when creating its archives and must be careful to segregate privileged e-mails from its general records.

Other important considerations include the costs at trial. Gahtan points out that extensive retention of e-mail can lead to high production costs during litigation: “If a business routinely backs up its entire

network, including its e-mail system, and retains backup tapes for a period of years, it potentially exposes itself to horrendous burdens in discovery and may find itself needing to unnecessarily review millions of e-mail messages.⁴ Litigants are generally responsible for their own costs of production. Though the courts are sometimes willing to consider other allocations in the case of e-discovery, they have yet to provide definitive guidance on this point.



In light of these potential consequences, firms may want to take advantage of cost-effective tools that are capable of archiving all inbound and outbound e-mail. Once litigation is reasonably anticipated, a firm that overzealously deletes its e-mails may risk allegations of spoliation, that is, the destruction of or the failure to preserve evidence. In the United States, where e-discovery jurisprudence is more advanced, Kirby Behre and Mark Koehn of Paul, Hastings, Janofsky & Walker LLP write, "Just a few years ago, litigants were infrequently sanctioned for e-discovery failures, in part, because many judges ... chalked up discovery mishaps to 'the learning curve.' Those days are over."⁵ Today, a firm that is unable to adequately produce the electronic documents required of it in court risks an order for costs and/or an adverse evidentiary inference against it.

Not to mention that there are numerous legally mandated retention periods for information held by registrants. A firm that prematurely destroys its e-mail

risks subjects itself to sanction, depending on which regulations apply. In a securities context, such regulations include Rule 10.12 of the Universal Market Integrity Rules, which requires that traders and certain dealers retain the record of each order they place for seven years, as well as sufficient information to identify the beneficial owner. That record must be readily accessible for the first two years of the retention period. Similarly, Rule 29.5(7) of the Investment Industry Regulatory Organization of Canada's Dealer Member Rules requires that dealer members retain all business-related electronic communications sent to a single current or prospective client for five years.⁶

A registrant's legal position on e-mail retention is subject to an underlying tension. On the one hand, a firm must preserve its records to the extent legally required of it, and it must do so efficiently to facilitate production should a lawsuit arise. On the other hand, it may be prudent from a risk-management perspective to destroy e-mails that are not strictly required to be maintained.

To balance these competing goals, registrants should adopt a detailed document retention policy that provides for when litigation is and is not reasonably anticipated. When unneeded records are destroyed, they should be destroyed as a class, rather than individually, to avoid any negative inferences being drawn later on. Even when litigation is not anticipated, the policy must be commercially reasonable and implemented in good faith. Once litigation is anticipated, the policy must suspend the destruction of documents and provide for their preservation.

1 Susan Wortzman and Susan Nickle, "The Preservation and Destruction of Electronically Stored Information in Ontario" in *E-Discovery in Canada* (Markham ON: LexisNexis Canada) 45 at 46

2 *Registration Requirements*, C.S.A. NI 31-103 (24 April 2008) at ss. 1.1(1), 5.16(1)

3 Alan M. Gahtan, *Electronic Evidence* (Scarborough ON: Carswell, 1999) at 83

4 *Ibid* at 90

5 Kirby Behre and Mark Koehn, "Minimizing the Risk That E-Discovery Failure Will Create Corporate Liability" *Law.com* (11 July 2008), online: <<http://www.law.com/jsp/ihcl/PubArticleIHC.jsp?id=1202422898147>>

6 *Dealer Member Rules*, Investment Industry Regulatory Organization of Canada, r. 29.7