A lawyer's perspective on records retention and destruction

Dan Michaluk, Hicks Morley[1]

This paper features a basic discussion of the legal requirements related to records retention and destruction. I write from the perspective of an information management and privacy lawyer. I also believe it important to state my perspective because I understand that successful records management relies on input from qualified legal counsel, but also from records management specialists, information technology professionals and persons with working knowledge of the various classes of records at issue.

I have divided this paper into two parts: the first focusing on retention and the second on secure destruction. I have further subdivided the part on retention into four subparts: (1) minimum retention periods; (2) maximum retention periods; (3) discretion and reasonableness and (4) litigation holds.[2]

RETENTION PERIODS

Minimum Retention Periods

Identifying all applicable minimum retention requirements established by statute[3] is an important step in developing and maintaining a records retention schedule.

Minimum retention periods are featured in some privacy statutes. This is based on policy intended to permit access to personal information and transparency about the use of personal information. The Ontario *Freedom of Information and Protection of Privacy Act* and its municipal-sector equivalent,[4] for example, require regulated bodies and

---

[1] I am a lawyer at Hicks Morley and provide our management clients with information and privacy advocacy and advice and employment and human rights advocacy and advice. I'd like to thank my colleagues Bushra Rehman and Robert Church for their helpful input. The views reflected in this paper are my own and not the views of Hicks Morley or its clients.

[2] Please note that I prepared this paper for the Canadian Institute's *Meeting Your Privacy Obligations* conference in May 2009, so it has a special focus on privacy regulation.

[3] Beware that record retention requirements may also be imposed by contract.

[4] The *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

institutions to retain records of personal information for one year after their use.[5] Canada's commercial sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*, has a more flexible minimum retention rule. Principle 4.5.2 of PIPEDA states, "Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made."[6]

Statutory minima are also found throughout the federal and provincial statute books. Here are some that regularly arise in my own practice:

- Employee name and address records – three years from end of employment[7]
- Date of birth records for employees under age 18 – three years from earlier of end of employment or 18th birthday[8]
- Employment start date records – three years from end of employment[9]
- Records of hours worked – three years from current[10]
- Wages paid records – three years from current[11]
- Records related to protected leaves – three years from date leave expires[12]

---

[5] R.R.O. 1990, Reg. 460, s. 5(1) (provincial) and R.R.O. 1990, Reg. 823, s. 5 (municipal, which allows municipal bodies to implement shorter retention periods by by-law). The British Columbia *Personal Information Protection Act* contains a similar rule, S.B.C. 2003, c. 63, s. 35(1).

[6] S.C. 2000, c. 5, Principle 4.5.2 (PIPEDA).

[7] *Employment Standards Act*, 2000, S.O., c. 41, s. 15(5).1.

[8] *Ibid.*, s. 15(5).2.

[9] *Ibid.*, s. 15(5).3.

[10] *Ibid.*, s. 15(5).4.

[11] *Ibid.*, s.15(5).5.

[12] *Ibid.*, s. 15(7).

- Excess hours and overtime averaging agreements – three years from last day of work subject to the agreement[13]

- Vacation time and pay records – three years from date of creation[14]

- *Occupational Health and Safety Act* medical surveillance records – longer of 20 years from time records first made or 40 years from time last of such records made[15]

- Patient records (by members of the College of Physicians and Surgeons of Ontario) – longer of 10 years from last date of entry or date patient reached or would have reached 18 years of age[16]

- Income tax records – records and books of account (subject to exceptions) to be kept for six years from the end of the last taxation year to which they relate[17]

Minimum retention periods like the ones listed above are assigned by statute either because their associated records have value to regulators as an aid to enforcement or because they are of direct value to the public itself (as with medical records). Given the current push for greater organizational accountability in the public and private sectors, organizations should be alert to new recordkeeping requirements. The Canadian Securities Administrators, for example, has proposed a new National Instrument that will soon implement a broad recordkeeping requirement on registered securities firms.[18] National Instrument 31-103 will include a far-reaching requirement to keep records of

---

[13] *Ibid.*, ss.15(8) and (9).

[14] *Ibid.*, s. 15.1(9).

[15] See e.g. R.R.O. 1990, Reg. 837, s. 15(1).

[16] O. Reg. 114/94, s. 19(1). This regulation also includes a provision that allows physicians who cease to practice to destroy records after giving notice to patients.

[17] *Income Tax Act*, R.S.C. 1985 c. 1 (5th supp) s.230 and *Income Tax Act*, R.S.O. 1990, c. I.2, s. 39.

[18] Canadian Securities Administrators, *National Instrument 31-103*, Registration Requirements (proposed 24 April 2008).

non-transaction related client communications for seven years from the date a client ceases to be a client of a firm.[19] This new regime could come into force as early as September 2009.[20]

Maximum retention periods

Maximum retention periods must also be considered in the process of establishing a retention schedule. They are a newer feature of our law than minimum retention periods[21] and unlike minimum retention periods, are generally set in broad terms. In this part of the paper, I will examine the minimum retention periods in PIPEDA and in the British Columbia *Personal Information Protection Act*,[22] neither of which have been the subject of significant comment by their respective commissioners.

PIPEDA Principle 4.5.3 states, "Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous."[23] The OPC has issued only a handful of decision summaries on this principle. They illustrate willingness to defer to retention periods established by organizations thoughtfully and in good faith.

Case Summary #157[24] and Case Summary #326[25] both addressed the retention period for credit history records retained by credit reporting agencies. In Case Summary #157 the OPC dismissed a complaint that a six-year retention period was too short.[26] In Case

---

[19] *Ibid*., s. 5.16(4)(b).

[20] Canadian Securities Administrators, *CSA Staff Notice 31-310* (3 April 2009).

[21] For a historical perspective on maximum retention rules, see B. Keele, "Privacy by Deletion: The Need for a Global Data Deletion Principle" (2009) Indiana Journal of Legal Studies16:1.

[22] S.B.C. 2003, c. 63 (British Columbia PIPA).

[23] PIPEDA, Principle 4.5.3.

[24] 2003 CanLII 36769 (P.C.C.).

[25] 2006 CanLII 18530 (P.C.C.).

[26] Though the complaint was framed as a retention complaint, the complainant in #157 was essentially challenging the accuracy of her credit history given the agency's records only dated back six years. In #326 the respondent claimed a long record was necessary to accurately and fairly assess an individual's credit.

Summary #326, the OPC deemed a maximum retention complaint to be resolved after the respondent implemented a 20-year retention period. That the OPC blessed this lengthy period as "required" after earlier considering a much shorter period for the same record suggests that it appreciates that reasonable businesses may differ in their designation of retention periods.

Although the OPC upheld a retention complaint in Case Summary #255, the analysis undertaken does not demonstrate rigorous scrutiny. The OPC held that an airport authority breached the retention principle by retaining personal information collected in issuing pass cards to employees after the end of employment. The authority had made a rather weak claim that it needed to retain this information in case employees returned. The OPC's summary indicates that the authority had no retention policy in place at all and was simply "saving steps" by retaining the information. Case Summary #255 is hardly indicative of an interventionist approach.

The maximum retention provision in the British Columbia PIPA is more qualified than the PIPEDA provision. It requires secure destruction when it is "reasonable to assume" that the stated purpose for collection is spent *and* when "retention is no longer necessary for legal or business purposes."[27]

The British Columbia OIPC has only issued one retention decision, *K.E. Gostlin Enterprises Limited*.[28] In this decision, the OIPC held that an operator of a Canadian Tire store could not indefinitely retain the name address and telephone number of individuals who make merchandise returns. The company argued that retention was necessary to detect patterns of fraudulent activity. The OIPC accepted this purpose as valid, but also held that it did not justify permanent retention, stating:

> In considering this issue, it is appropriate to take into account the nature and extent of the personal information involved, any applicable legal

[27] British Columbia PIPA, s. 35(2).

[28] 2005 CanLII 18156 (BC I.P.C.).

> requirements (such as statutory limitation periods for civil lawsuits) and the business purposes relating to retention of the personal information.
>
> The personal information involved here is not, as I have already noted, generally of a sensitive nature. Its permanent retention is not, however, justified on that basis alone. While I acknowledge the personal information is useful to detect possible patterns of fraudulent activity, I am not persuaded it is reasonable to assume that this purpose will always continue to be served, such that permanent retention is permitted under s. 35(2)(a).[29]

The OIPC ordered the organization to create a compliant retention schedule, deliver it to the OIPC for review and to destroy or annonymize records falling outside the maximum retention period established by the company. It did not recommend any specific retention period.

The British Columbia OPIC's comments on the significance of context are helpful, though they do not resolve one particularly vexing uncertainty that is associated with maximum retention rules – Can an individuals withdraw consent to retain personal information and, in effect, demand that organizations destroy records containing personal information?

Only the Alberta *Personal Information Protection Act* addresses this question expressly. Section 35 states, "Notwithstanding that a consent has been withdrawn or varied under section 9, an organization may for legal or business purposes retain personal information as long as is reasonable."[30]

In statutes like PIPEDA and British Columbia PIPA, in which such a direction has not been made, the "demand destruction dilemma" raises an important interpretation issue

---

[29] *Ibid.*, at paras. 100 and 101.

[30] S.A. 2003, c. P-6.5, s. 35 (Alberta PIPA). This seems to establish a very general "reasonableness" standard that only applies if an individual withdraws consent.

about whether retention of personal information is a "use" of personal information and about the scope of the right to withdraw consent. Although the dilemma raises significant interpretation issues, it should be resolved with reference to the strong public policy that favors the promotion of business recordkeeping systems with integrity.[31] I am not, however, aware of any Canadian cases on point.

Discretion, records as evidence and reasonableness

Developing and enforcing retention rules is a legitimate means of managing records that may contain either potentially "helpful" or "hurtful" evidence.[32] Of course, a record's value as evidence is only one aspect of its overall business value. [33] The evidentiary value of records, however, is the link between records management and litigation readiness.[34]

Regarding records that could become helpful evidence, the benefits of a defined retention rule are obvious. An organization will aim to keep such files as long as the full costs associated with retention are outweighed by the potential benefit of retention. Limitation periods for potential claims are relevant to this analysis, but there is no firm rule that a record loses all evidentiary value after its *most related* limitation period expires. A record's potential value as evidence can only be judged in light of its relevance to *all potential claims*. Accordingly, defining a record's evidentiary value is not an exact science. One might argue that a good and realistic retention rule should satisfy the "80/20

---

[31] The integrity of recordkeeping systems from which electronic records are produced goes to their admissibility and weight, as recognized in the Uniform Law Conference of Canada's *Uniform Electronic Evidence Act* (September 1998). See also George L. Paul, *Foundations of Digital Evidence* (Chicago: ABA Publishing, 2008). Mr. Paul argues that evidence about how information is governed in an information system is a key foundation for digital evidence.

[32] *Arthur Anderson, LLP v. United States*, 544 U.S. 696, 125 S. CT. 2129, 2135 (2005): "'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including Government, are common in business." Despite this quote, organizations should be cautious in setting retention periods with a view to getting rid of harmful evidence. I've used "helpful" and "hurtful" as terms of convenience and for illustration purposes. "Helpful" (business records) and "not helpful" (*e.g.*, e-mails) are more appropriate terms with less illustrative force.

[33] The American Records Management Association identifies four kinds of value: operational value, legal value, fiscal value and historical value. "Developing a Records Retention Program," online: ARMA International <http://www.arma.org/pdf/articles/DevelopingRecordsProgram.pdf> at 6.

[34] *McDougall*, *supra* note 45, at para. 29.

rule" – that is the evidence will be there when the company needs it eight times out of ten because meeting a higher standard would lead to very lengthy retention periods.[35] One can also see why it is important to incorporate a feedback loop as part of an annual records retention program review.[36]

Regarding records that could become harmful evidence, a defined retention rule protects against an adverse inference.[37] But how closely will a court scrutinize a retention rule if relevant records have been destroyed prior to anticipated litigation to the non-custodian party's prejudice? Will a court examine whether a rule was set in good faith? Will it go further and examine whether a rule is reasonable?

These questions have not yet been canvassed by Canadian courts, but American courts have demonstrated a willingness to assess the reasonableness of an organization's retention rules. The leading case is *Lewy v. Remington Arms*,[38] a case in which a firearm manufacturer's policy of destroying complaints and gun examination reports after three years from the date of their creation was challenged in a suit brought by a woman who was shot after the manufacturer's firearm accidentally discharged. The court suggested that some classes of records ought to be retained if, by their very nature, they are likely to be relevant to future litigation:

> We are unable to decide, based on the record we have before us, whether it was error for the trial court to give this instruction. On remand, if the trial court is called upon to again instruct the jury regarding failure to produce evidence, the court should consider the following factors before deciding

---

[35] Lengthy retention periods are certainly not *de rigueur*, particularly given the costs associated with reviewing large volumes of electronic records in order to meet a legal production requirement. On this topic, see The Sedona Conference Working Group 1, "The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, Second Edition." (November 2007) at 23 and 24.

[36] See Developing a Records Retention Program, *supra* note 33 at 8.

[37] See e.g. *Galenzoski v. Awad*, 2007 SKQB 436 (CanLII).

[38] 836 F.2d 1104 (8th Cir. 1988).

> whether to give the instruction to the jury. First, the court should determine whether Remington's record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents. For example, the court should determine whether a three year retention policy is reasonable given the particular document. A three year retention policy may be sufficient for documents such as appointment books or telephone messages, but inadequate for documents such as customer complaints. Second, in making this determination the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints.[39]

Does this invite a form of common law duty to preserve some types of "litigation-relevant" records in advance of anticipated litigation? Some might argue that it does, but for most records courts will likely defer to an organization's chosen retention period absent a showing of bad faith.

The willingness of courts to take a "hands on" approach to retention periods is a particularly significant issue given the trend towards shorter retention periods for transitory e-mails,[40] an issue highlighted by an American case called *Broccoli v. Echostar Communications Corp*.[41]

Broccoli involved a harassment claim made against a company that had a policy of automatically purging employee e-mails within 21-days.[42] The plaintiff moved for

---

[39] *Ibid*., at 1112.

[40] For a good article on the implementation of a new e-mail retention policy, see B.K. Winstead, "Establishing an Email Retention Policy: The Legal Perspective" (5 March 2009) online: Windows IT Pro < http://windowsitpro.com/article/articleid/101646/establishing-an-email-retention-policy-the-legal-perspective.html>.

[41] 229 F.R.D. 506 (D. Md. 2005).

[42] E-mails were automatically sent from the "sent items" folder to the "deleted items" folder after seven days and then automatically purged from the "deleted items" folder after another 14 days. Presumably e-

sanctions, in part because the company had destroyed relevant e-mails pursuant to this policy. The Court stated, "under normal circumstances, such a policy may be a risky but arguably defensible business practice undeserving of sanctions."[43] In the circumstances, the Court did sanction the company for failing to preserve evidence because it did not suspend the routine destruction of e-mails fast enough. The Court held that the company should have taken preservation steps as soon as the plaintiff complained to his supervisors about harassment, approximately eight months before he left the company. *Broccoli* demonstrates that even a "reasonable" short retention period has its risks, and that companies who adopt short retention periods also need to develop very responsive mechanisms for implementing litigation holds, the subject of the next subpart to this paper.

Record destruction holds and spoliation of evidence

Record retention programs must have "hold procedures" to ensure that routine destruction of records pursuant to retention schedules is suspended in response to reasonably anticipated litigation or government inspections and investigations.[44] This can be a difficult task, and litigants now often clash about spoliation of evidence.

Thankfully, the Alberta Court of Appeal issued some very clear and principled statements about the doctrine of spoliation in October 2008. In *McDougall v. Black & Decker Canada Inc.*,[45] the Court described the three different bases for seeking a remedy for spoliation of evidence and stressed that intentional (as opposed to negligent) destruction of evidence is most likely to lead to the imposition of sanctions absent prejudice.

---

mails could remain stored in an employee's inbox or could be organized and preserved in sub-folders. However, the company also purged all data stored by former employees within 30 days of termination.

[43] *Broccoli, supra* note 41, at para. 4.

[44] The duty is derived from the common law doctrine of "spoliation," described below, but also from enforcement provisions in regulatory statutes and the prohibition against obstruction of justice in the *Criminal Code*: R.S., 1985, c. C-46, s. 139. For the scope of the duty see, *Doust v. Schatz*, 2002 SKCA 129 at para. 29 (CanLII): "A party is under a duty to preserve what he knows, or reasonably should know, is relevant in an action."

[45] 2008 ABCA 353.

The first basis for a spoliation remedy is rooted in the law of evidence and was first recognized by the Supreme Court of Canada in the 1896 *St. Louis*[46] case. The Alberta Court of Appeal confirmed that the *St. Louis* remedy is simply a rebuttable presumption of fact – that the destroyed evidence would have been hurtful to the spoliator's case – that requires a finding of intentional destruction:

> Moreover, in my view, it is not appropriate to apply the presumption that the evidence would tell against the spoliator when evidence has been lost or destroyed carelessly or negligently, or something else short of the intention required by *St. Louis*. The presumption is no more than an adverse inference, drawn from circumstances surrounding the destruction or loss of the evidence. When the destruction is not intentional, it is not possible to draw the inference that the evidence would tell against the person who has destroyed it.[47]

The Court of Appeal also said that intentional destruction of evidence was a requirement for striking out an action based on an exercise of a court's rules-based or inherent jurisdiction to control its process. It suggested the maintenance of trial fairness should be the primary guide to the exercise of discretion and warned that the striking out of an action for spoliation is extraordinary:

> While the court always has the inherent jurisdiction to strike an action to prevent an abuse of process, it should not do so where a plaintiff has lost or destroyed evidence, unless it is beyond doubt that this was a deliberate act done with the clear intention of gaining an advantage in litigation, and the prejudice is so obviously profound that it prevents the innocent party from mounting a defence.[48]

---

[46] *St. Louis v. Canada* (1896), 25 S.C.R. 649.

[47] *McDougall*, *supra* note 45, at para. 24. For a conflicting approach, see *Dickson v. Broan-NuTone Canada Inc*., [2007] O.J. No. 5114 (Q.L.) (S.C.J.).

[48] *Ibid*., *McDougall*, at para. 33.

This does not rule out remedies against a party who cannot produce records due to negligent preservation, but such remedies are only likely to be awarded at trial based on a consideration of the actual prejudice caused by the loss.[49]

Finally, the Court of Appeal noted that there is no recognized civil duty to preserve evidence in Canadian law: "The courts have not yet found that the intentional destruction of evidence gives rise to an intentional tort, nor that there is a duty to preserve evidence for purposes of the law of negligence, although these issues, in most jurisdictions, remain open."[50] While the duty to refrain from intentionally destroying evidence has been addressed in the well-known *Spasic Estate*[51] and *Endean*[52] cases, whether there is a positive duty to preserve evidence subject to the negligence standard of care is more significant, but also less discussed.[53]

Does *McDougall* mean that Canadian organizations can throw caution to the wind when it comes to records preservation? Hardly! It does show that we may wait awhile for a good articulation of standard of care for preservation of records in Canada. Until then, organizations must look to non-jurisprudential authority for guidance. The *Sedona Canada Principles*,[54] for example, specify the following:

---

[49] *Ibid*., *McDougall*, at para. 22. See also *Commonwealth Marketing Group Ltd. v. The Manitoba Securities Commission*, [2009] M.J. No. 77 (C.A.) (QL). *Jay v. DHL*, 2009 PEICA 2 (CanLII) and *Carleton v. Beaverton Hotel*, 2009 CanLII 4245 (CanLII).

[50] *Ibid*., *McDougall*, at para. 38

[51] *Spasic (Estate) v. Imperial Tobacco Ltd.* (2000), 49 O.R. (3d) 699 (C.A.).

[52] *Endean v. Canadian Red Cross Society* (1998), 157 D.L.R. (4th) 465 (B.C.C.A.).

[53] As noted by the Alberta Court of Appeal in *McDougall*, in *Rivet v. British Columbia*, 2007 BCSC 731 (CanLII) the British Columbia Supreme Court refused to strike a claim for the negligent destruction of evidence. In *Dawes v. Jajcaj*, 1999 BCCA 237 (CanLII), the British Columbia Court of Appeal rejected an argument that the Insurance Corporation of British Columbia owed a duty of care to preserve evidence, but qualified this finding based on the record before it.

[54] The Sedona Conference Working Group 7, "The Sedona Canada Principles: Addressing Electronic Discovery." (January 2008) online: The Sedona Conference <http://www.thesedonaconference.org>. These twelve non-binding statements of principle are intended to facilitate electronic discovery in Canada and provide authoritative guidance in the resolution of electronic discovery disputes in Canada. See also The Sedona Conference Working Group 1, "The Sedona Conference Commentary on: Preservation,

- A party should not be required to search for or preserve information that is deleted, fragmented or overwritten unless the party is aware of relevant information that can only be obtained from such sources or there is a specific agreement or court order.[55]

- Generally, parties should not be required to preserve *short term* disaster recovery backup media created in the ordinary course of business.[56]

- If a party maintains data on tape or other offline media not accessible to end users of computer systems, steps should be taken promptly to preserve those *archival* media that are reasonably likely to contain relevant information not present as active data on the party's systems.[57]

RECORDS DESTRUCTION

There is a relatively uniform requirement in Canadian privacy legislation to employ reasonable or appropriate measures to protect personal information from theft, loss and misuse.[58] This rule is often reinforced with specific duties that relate to the destruction of records. PIPEDA, for example, contains the following data destruction rules:

> 4.5.3
>
> Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations

---

Management and Identification of Sources of Information that are Not Reasonably Accessible" (July 2008) online: The Sedona Conference <http://www.thesedonaconference.org>.

[55] *Ibid.*, at 15.

[56] *Ibid.*, at 16 (my emphasis).

[57] *Ibid.*, at 17 (my emphasis).

[58] I've addressed privacy legislation only in this paper, but there are other sources of secure destruction duties. The Law Society of Upper Canada, for example, requires members to, "Take care to appropriately delete or destroy information in electronic form, particularly documents on CDs or diskettes." See Law Society of Upper Canada, "File Retention" online: LSUC <http://rc.lsuc.on.ca/pdf/pmg/fileRetention.pdf>.

> shall develop guidelines and implement procedures to govern the destruction of personal information.
>
> 4.7.5
>
> Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

Though this "technology neutral" rule seems simple enough, there is more than one way to "destroy" and "erase" physical and electronic records, making something anonymous can also be a matter of degree[59] and the general safeguarding duty leaves room for the imposition of specific duties related to records destruction. In short, there is ample room for interpreting organizations' destruction-related duties.

The broadest statements on the standard for reasonable data destruction have come out of Ontario.[60] Following a high profile data breach in which medical records that were mistakenly recycled ended up being discarded on a downtown Toronto street for use in a film shoot about the 9/11 terrorist attack, the Ontario IPC issued its first order[61] under the Ontario *Personal Health Information Protection Act*. The IPC then incorporated the substance of this order into *Fact Sheet #10: Secure Destruction of Personal Information.*[62]

---

[59] There is ample case law on whether information can be used to identify individuals. For two recent examples, see *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 112 (CanLII) and *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII).

[60] Though the British Columbia OIPC made similar and broad pronouncements in *Investigation Report F06-02 (Re)*, [2006] B.C.I.P.C.D. No. 17 (QL).

[61] Order HO-001 (31 October 2005) online: Information Privacy Commissioner/Ontario http://www.ipc.on.ca/images/Findings/up-ho_001.pdf>.

[62] Information and Privacy Commissioner/Ontario, "Fact Sheet #10: Secure Destruction of Personal Information" (December 2005) online: Ontario IPC < http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf>. Endorsed by the British Columbia OIPC in *F06-2*, *supra* note 60.

Fact Sheet #10 establishes a form of standard for destruction of physical records and electronic storage media. Regarding physical records, it says, "destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed."[63] Regarding electronic storage media, it says, "destruction means either physically damaging the item (rendering it unusable) and discarding it, or, if re-use within the organization is preferred, it means employing wiping utilities provided by various software companies."[64]

Fact Sheet #10 also prescribes a number of destruction best practices. They are:

- Duplicates of official records that contain personal information should be stamped with "shred after" and "do not copy" warnings
- Hire a records destruction agent that is accredited by an industrial trade association such as the National Association of Information Destruction or one willing to uphold its principles
- Be selective and check agents' references
- Enter a signed agent's contract that sets out how destruction will be accomplished, that specifies how quickly after pickup records will be destroyed and that restricts subcontracting without consent
- Reserve a right to audit an agent's processes
- Require agents to deliver a certificate of destruction that includes the date, time , location and method of destruction and the signature of the operator[65]

---

[63] *Ibid.*, at 1.

[64] *Ibid.*, at 2. In *Report H2003-IR-002; Associate Medical Clinic (Re)*, [2003] A.I.P.C. No. 24 (QL) the Alberta OIPC recommended physical destruction or permanent deletion "though use of a commercial disk wiping utility." In *Investigation Report F06-02 (Re)*, supra note 60, the British Columbia OIPC simply recommended "wiping."

[65] *Ibid.*, at 2 and 3.

The clarity that flows from *Fact Sheet #10* is welcome, but note that there is significant debate about how to effectively wipe storage media and how the effectiveness of any wiping methodology might vary based on the properties of the subject media.[66] The IPC seems to demand less than perfect irretrievability for personal information stored on electronic storage media. It notes that data may reside on a wiped hard drive, but does not prescribe responsive measures to address this concern.[67] Though this may indicate a pragmatic rather than absolute standard, a cautious organization (particularly if dealing with sensitive personal information) may not treat "wiping" so generically. Rather, a cautious organization will take steps to understand the degree of irretrievability associated with its specific wiping methodology and the marginal cost and benefit associated with more secure methodologies.

The Ontario IPC recently had an opportunity to revisit the subject data destruction in dealing with a complaint about physical disposal of records at the Old City Hall courthouse in Toronto.[68] The investigation was undertaken after a media organization brought attention to the disposal of un-shredded court documents in clear plastic bags. The IPC assessed the records destruction practices of the Ministry of the Attorney General, the City of Toronto, the Ministry of Community Safety and Correctional Services and the Toronto Police Services Board. In the end, it only made recommendations to the City based on a finding that (1) its shredding bin program did not extend to Old City Hall, (2) there was a City office at Old City Hall without either a paper shredder or a secure bin for paper to be shredded and (3) the City had not

---

[66] For useful commentary on this issue see C. Ball, "Ball in Your Court: The Multipass Erasure Myth" (March 2009) online: Law Technology News <http://www.lawtechnews.com/r5/showkiosk.asp?listing_id=3107662> and J. Gregory, "Destroying Data" (5 January 2009) online: Slaw < http://www.slaw.ca/2009/01/05/5599/> (including comments).

[67] *Ibid.*, *Fact Sheet #10*, at 1 and 3.

[68] Privacy Complaint Report PC07-41, PC07-45, MC07-29 and MC-7-33 (12 December 2008).

incorporated a segment on secure records destruction into its new staff orientation program.[69]

Conclusion

Record retention rules are simple logical statements that establish the end point of records' lives, but the amount of law that informs their establishment and enforcement is significant. Minimum and maximum retention requirements and considerations about evidentiary value can point you to a defined end point, but destruction at that end point must be suspended if a preservation duty applies. The law also requires secure destruction of many types of records. I hope you find this paper a useful overview of the relevant considerations.

[69] *Ibid.* at 14.