Record Retention and Destruction Policies 2015

Deeth Williams Wall LLP

Richard Austin

February 26, 2015

Table of Contents

I. The Information Age

- 4.1 billion email accounts in 2014
- 2.5 billion email users worldwide in 2014
- 353,860,000 Internet users in North America, up from 252,908,000 in 2009
- 108.7 billion emails per day in 2014
- IDC states 2.8 zettabytes (2.8 trillion GBs) of information created 2012, forecasts 40 zettabytes by 2020

Sources:

Email Statistics Report, 2014-2018 , http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf

Internet Worldwide Stats, http://www.internetworldstats.com/stats.htm

How much data is out there, http://www.webopedia.com/quick_ref/just-how-much-data-is-out-there.html

Electronic documents differ from paper documents:

➢ **Volume and Duplicability**	➢ **Environment Dependence**
➢ **Persistence**	➢ **Obsolescence**
➢ **Metadata**	➢ **Dispersion**
➢ **Dynamic, changeable content**	➢ **Searchability**

Record Retention and Destruction Policies (RRDP):

- preserve useful documents
- for the period of time for which retention is useful or required by law
- while managing the expense and
- implementing appropriate document destruction

Exclusions:

This presentation does not address:

- Litigation, e-discovery and litigation holds

- Legal file management responsibilities:
  - Practice Management Guidelines, Section 3 (http://www.lsuc.on.ca/with.aspx?id=2147490535)
  - Guide to Retention and Destruction of Closed Client Files for Lawyers (http://lsuc.on.ca/with.aspx?id=2147499150)

II. Why have an RRDP?

A. Compliance with Statutory Obligations

1. General corporate obligations:

- *Canada Business Corporations Act,* R.S.C. 1985, c. C-44, s. 20
- *Business Corporations Act*, R.S.O. 1990, c. B.16, s. 140

2. Taxing statutes, e.g.:

- *Income Tax Act*, R.S.C. 1985,c.1 (5TH Supp.), s. 230
- *Excise Tax Act*, R.S.C. 1985, C. E-15, s. 286
- *Retail Sales Tax Act*, R.S.O. 1990, c. R.31, s. 16

Compliance with Statutory Obligations:

3. Employment Related Statutes, e.g.:
   - *Canada Labour Code*, R.S.C. 1985, c. L-2, s. 252(2)
   - *Canada Pension Plan*, R.S. 1985, c. C-8, s. 24
   - *Employment Insurance Act*, S.C. 1996, c.23, s. 87
   - *Employment Standards Act*, 2000, S.O. 2000, c. 41, Part VI
   - *Occupational Health and Safety Act*, R.S.O. 1990, c. O-1, s. 26

4. Industry specific obligations, e.g.:
   - *Bank Act*, S.C.1991, c. 46, ss. 238-239
   - *Insurance Companies Act*, S.C. 1991, c. 47, ss. 261-262
   - *Trust and Loan Companies Act*, S.C. 1991, c. 45, ss. 243-244
   - *Law Society Act*, R.S.O. 1990, c. L-8, By-law 9, Part V
   - *Securities Act*, R.S.O. 1990, c. S-5, s. 19

Compliance with Statutory Obligations:

5. Privacy Obligations, e.g.:

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5

> "5.(1) ... every organization shall comply with the obligations set out in Schedule 1."

Schedule 1:

1. Accountability
2. Identifying Purpose
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

Privacy Obligations cont'd

PIPEDA Case Summary # 2007 - 380 - Bank's record keeping practices considered inadequate safeguard:

> "... On balance, the Assistant Commissioner believed that this account was the complainant's only, and therefore the bank disclosed his personal information without the complainant's knowledge or consent. She noted that ***it was not enough for the bank to argue that it was a joint account because both of the names appeared on the statements. It needed to produce evidence and it could not***.
>
> This last point led the Assistant Commissioner to comment that ***the bank's record keeping with respect to this account was so careless as to amount to an inadequate safeguard***. It could not provide documentary evidence to support its position vis-à-vis the account holder(s). It could not provide documentary evidence that it had or had not disclosed material. She commented that while there might be retention periods in place for certain documentation, these were not consistently applied, as shown by the fact that the bank could provide signature cards for an account that was older than the one under investigation." (emphasis added)

II.B Compliance with Contractual Obligations

Obligations relating to records retention and destruction

Where found:	What Obligations:
Non-disclosure agreements	Retention Period
Letters of Intent	Accuracy and completeness
Memoranda of Understanding	Format and storage media
Software license, maintenance and support agreements	Locations / obligation not to relocate
Teaming Agreements	Remote access
Master Service Agreements and Statements of Work	Delivery obligation
Subcontracts, supply agreements and purchase orders	Destruction obligation
Shipping documents	Costs

Compliance with contractual obligations:

- Touches all aspects of the business
- Requires education and training of company personnel
- Dynamic and changing
- Raises business, confidentiality and security issues
- Not susceptible to standardized approaches
- Costly
- Sometimes isn’t possible

III. Issues:

A. Minimum Retention Periods

- By contract
- By statute:
  - Defined retention periods, e.g. *Employment Standards Act, 2000*, s.15
  - General obligations, e.g. *PIPEDA*, Principle 4.5.2:

    "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."

Minimum Retention Periods:

- *Limitations Act, 2002*, S.O. 2002, c.24, Sched. B
- *Securities Act*, R.S.O. 1990, c. S-5, 129.1

Ontario v. Johnson Controls Ltd., [2002] O.J. No. 4725

> "50. … A policy with a short retention period might offer some justification to dispose of "smoking guns" and other prejudicial evidence. Any such policy that permits destruction within much less than ten years after an event probably fails to take reasonable account of the standard six year limitation period under the Limitations Act for actions in tort or contract, plus some period to allow for a discoverability period, which allows for discovery of the damage and those responsible prior to the commencement of the limitation period. A short retention period would also ignore the extended period under s. 8 of the Act."

See also:

Alvi v. YM Inc. (Sales)(cob Stitches), [2003] O.J. No. 3467(Ont. Sup. Ct.) at para. 48

336332 B.C. Ltd. v. Imperial Oil Ltd., 2002 BCSC 587 at para. 46

III.B Maximum Retention Periods

- *PIPEDA*, Principle 4.5.3:

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

  PIPEDA Case Summary #2013-001 - concerns relating to the retention of non-user numbers found to be well founded:

  > "44 Although personal information collected by WhatsApp during the contact discovery process is appropriately limited to that necessary for legitimate purposes, as specified by WhatsApp in its Terms of Service, the company's retention of out-of-network numbers remains, in our view, unnecessary and may create the potential for inappropriate or unintended uses of non-user mobile numbers."

- See also:

  Personal Information Protection Act, S.B.C 2003, c.63, s. 35

III.C Appropriate Document Destruction: Context

- The "Smoking Gun":

  "ATHM is a piece of crap!"

  Email from Merrill Lynch analyst who published high ratings of ATHM, disclosed during an SEC investigation of Merrill Lynch, resulting in $100 million fine

- Spoliation:

  "The intentional destruction, mutilation, alteration or concealment of evidence."

  Black's Law Dictionary, 9th ed.

Appropriate Document Destruction cont'd

"Justice Brooke stated his understanding of the law of spoliation based on four case authorities to which he was referred by counsel for the respondents. The following is a summary of what was stated: 1. A rebuttable evidentiary presumption arises where evidence of spoliation exists; the doctrine of spoliation is an evidentiary rule raising a presumption and not an independent tort giving rise to a cause of action. 2. In an appropriate case, destruction of documents carries a procedural but not substantive remedy, an action for damages cannot be sustained solely on the ground that documents have been destroyed. 3. Spoliation requires four elements in evidence: a) the evidence has been destroyed; b) the evidence destroyed was relevant to an issue in the lawsuit; c) legal proceedings were pending; and d) the destruction of documents was an intentional act indicative of fraud, or an intention to suppress the truth. 4. ***There is no common law duty of care to preserve property which may possibly be required for evidentiary purposes; such an obligation can only be imposed by court order granted pursuant to the Rules of Court …*** ." (emphasis added)

Holland v. Marshall, 2008 BCCA 468 (CanLII) (citations omitted)

Records Retention and Destruction Policies:

A properly adopted and implemented RRDP may help defend against charges of improper document destruction or failure to preserve:

> "Compliance with a reasonable records management policy ... should not, in the ordinary course, constitute sanctionable conduct.
>
> There are a number of factors to be considered in determining if destruction was intentional or reckless. Adherence to a document management policy in the face of reasonably contemplated or actual litigation is not appropriate."

Comment 11.e (Reasonable records management policies), Sedona Conference Working Group 7, *The Sedona Canada Principles, Public Comment Draft*, February 2007

The Ontario Public Sector:

Ontario Bill 179, *Public Sector and MPP Accountability and Transparency Act, 2014*, Schedule B:

- Adds section 10.1 to the *Freedom of Information and Protection of Privacy Act:*

  "Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution."

- Adds to the list of offences in Section 61(1) of the Act:

  "(c.1) alter, conceal or destroy a record or cause any other person to do so, with the intention of denying a right under this Act to access the record or the information contained in the record."

- Corresponding amendments to the *Municipal Freedom of Information and Protection of Privacy Act*

III.D Document Destruction

Implement appropriate document destruction policies:

- Office of the Information and Privacy commission of Canada, *Personal Information Retention and Disposal: Principles and Best Practices* at https://www.priv.gc.ca/information/pub/gd_rd_201406_e.asp
- Office of the Information and Privacy Commissioner of Ontario, *Secure Destruction of Personal Information* at https://www.ipc.on.ca/images/resources/up-fact_10_e.pdf
- Office of the Information and Privacy Commissioner of Ontario, *Best Practices for the Secure Destruction of Personal Health Information* at https://www.ipc.on.ca/images/Resources/naid.pdf

IV. Developing and Managing an RRDP

A. Internal Approvals:

- Identify RRDP issues to the board/senior management:
  - The necessity for a comprehensive and dynamic RRDP

- Establish RRDP Committee:
  - Cross-functional representation
  - With sufficient budget and authority
  - Reporting regularly to the board/senior management

IV.B Getting Started: Assessing the Situation:

- Examine any current Records Retention and Destruction Policies

- Evaluate current records retention and destruction practices:
  - What information does the company keep, how and where?
  - What information does the company destroy, where and how?
  - Are these practices in compliance with law and existing policies?

IV.C Defining the Scope of the RRDP

Records Management:

"The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including creation, maintenance (use, storage, retrieval), and disposal, regardless of media. Record management procedures are used to achieve adequate and proper documentation of corporate policies and transactions and effective and economical management of business and organizational operations"

Records:

"anything that is recorded within an organization, including email, drawings, documents/reports created by users, and information received from the outside"

All devices and locations:

servers, personal computers, laptops, Blackberries, PDAs, cell phones, iPods, hard drives, disks, sticks, social media sites, etc.

IV.D Regulatory and Contractual Requirements

For each of:

- Statutory requirements (*)
- Industry specific standards
- Contractual requirements

Understand and document:

- What records must be kept?
- For how long?
- In what form?
- What records must/can be destroyed?
- When?
- How?

(*) If the company operates outside Canada, it will be necessary to ensure compliance with international obligations

IV.E Establishing the Standards:

- Format of Records
- Destruction Periods
- Classification of Information
  - Preserving Privilege
- Integration with other policies and practices, e.g. Policies relating to:
  - Confidential information
  - Intellectual Property Protection
  - Use of corporate assets
  - Internet Usage
  - Security
- Suspension for Litigation Holds:
  - When: as soon as litigation is reasonably anticipated
  - Who can suspend

IV.F Implementation

- Communication
- Monitoring Compliance:
  - Test effectiveness of:
    - Retention practices
    - Destruction practices
    - Litigation Holds
  - Audit compliance with the policy
  - Part of individual performance evaluations
- Update as required

Questions?

Richard Austin

Deeth Williams Wall LLP

raustin@dww.com

416 941 8210