**CANADIAN BAR ASSOCIATION**

# Information to Supplement the CODE OF PROFESSIONAL CONDUCT

# Guidelines for Practicing Ethically with New Information Technologies

**September 2008**

# *Ethics and Professional Issues Committee*
# *Canadian Bar Association*

**Co-Chairs**

**David C. Day, Q.C.**
*St. John's*

**Alan J. Stern, Q.C.**
*Halifax*

**Members**

**Inez Cardinal, Q.C.**
*Saskatoon*

**Felicia S. Folk**
*Vancouver*

**Shannon Farrell**
*Charlottetown*

**Paul D. Paton**
*Kingston*

**Project Consultant**

**Elizabeth F. Judge, Ph.D.**
*Faculty of Law, University of Ottawa, Ottawa*

**Editorial Consultant**

**Vicki Schmolka**
*Kingston*

**Staff Liaison**

**Kerri Froc**
*CBA, Ottawa*

**Guidelines for Practising Ethically with New Information Technologies**

**Table of Contents**

1. Introduction
2. Practice Competence
3. Confidentiality
4. Encryption
5. Privilege
6. Electronic Storage, Retention, and Deletion
    - Storage
    - Archiving
    - Deletion
7. Metadata
8. Security
9. Marketing
10. Accessibility
11. Service Delivery
12. Intellectual Property and Software
13. Electronic Legal Research and Information Retrieval
14. Participation in Online Discussions

**Appendices**

**Appendix 1: Resources**

1. General Information
2. Resources for Conducting Canadian Legal Research Online
3. Legal Ethics and New Information Technologies
   i. "Guidelines on Ethics and the New Technology"
   ii. Other
4. Information Technologies Resources
5. Specific Resources
    a. Introduction
    b. Electronic Storage, Retention, and Archiving
    c. Marketing
    d. Accessibility
    e. Intellectual Property and Software
    f. Electronic Research and Information Retrieval

**Appendix 2: Metadata Information and Resources**

1. Resources
2. Drafting Practices that Create or Carry Over Metadata
3. Avoidance and Removal
    a. Minimizing the Creation of Metadata
    b. Managing and Removing Metadata
        i. Using Features Built-in to the Program

ii. Installing Add-ons from the Program Vendor
iii. Using Programs from Third-Party Vendors
4. References and Resources for Metadata

**Appendix 3: Steps to Improve Information Technology Security**

1. Backups of Data
2. Access Restrictions and Authentication Protocols
3. Encryption
4. Firewalls and Intrusion Detection Software (IDS)
5. Anti-Virus Software and Computer Security Software Suites
6. Policies on Computer Security for Employees and Staff
7. Securing Personal Information
8. Wireless Networking
9. Security Resources

**Glossary**

## Introduction

New information technologies, once mastered, can save time, contribute to efficiencies, and improve service. They are a benefit to lawyers and their clients.

These Guidelines recommend best practices in the use of information technologies. This is not a set of mandatory rules. For those, please refer to your governing body's code of professional conduct.

These Guidelines supplement the CBA Code of Professional Conduct and, in doing so, to assist lawyers when they use new technologies.

The Guidelines highlight best practices when using an information technology, with emphasis on the need to preserve the security of information and to maintain client confidentiality and privacy.

One striking element of information technologies is the rapid speed at which they are being integrated into our work and world, and the haste with which some of them become obsolete and are discarded.

Inevitably, courts are being called on to make decisions about a lawyer's ethical and legal responsibilities in response to the technology revolution. Some recent decisions have held that lawyers, in some circumstances, have an ethical obligation to use new technologies or, at least, have access to someone who can.

The Ethics and Professional Issues Committee will update these Guidelines regularly so that they remain relevant and useful to practitioners. We would appreciate your help. Please tell us if we have overlooked anything and make suggestions for resources or other information that need to be added to the Guidelines.

**The CBA does not endorse any product mentioned in these Guidelines.**

The Guidelines include information about specific resources. Some resources are for sale, others are free. In either case, listing a resource in these Guidelines does not mean that the CBA endorses the product. The intent is only to offer lawyers practical, accessible information so they can make their own choices.

- Information technologies include:
- office productivity software programs, including applications such as word-processing, spreadsheets, and presentations;
- computer-assisted legal research;
- e-mail;
- e-filing;
- voicemail;

- wireless devices, such as cordless computer peripherals (computer mouse, keyboard printer);
- pagers, cellular phones, and two-way radios;
- Global Positioning Satellite devices;
- personal data assistants;
- smart phones;
- facsimile machines;
- voice over Internet protocol (voice calls over a broadband Internet connection);
- video conferencing (interactive audio and video telecommunications);
- intranet (private computer networks – "private versions of the Internet" – that use Internet protocols to share information and resources but are usually restricted to an organization's employees);
- extranets (parts of the intranet that are made available to people from outside the organization, such as clients or suppliers); and
- external networks, including the Internet.

## 1. Practice Competence

### CBA Code of Professional Conduct: Practice Competence

The Rule in Chapter II of the Code (Rule II) provides:

> 1. The lawyer owes the client a duty to be competent to perform any legal services undertaken on the client's behalf.
> 2. The lawyer should serve the client in a conscientious, diligent and efficient manner so as to provide a quality of service at least equal to that which lawyers generally would expect of a competent lawyer in a like situation.

Commentary 4 to Rule II, added to the Code in 2004, specifically mentions competence with respect to technologies:

> Competence involves more than an understanding of legal principles; it involves an adequate knowledge of the practice and procedures by which those principles can be effectively applied. To accomplish this, the lawyer should keep abreast of developments in all areas in which the lawyer practices. The lawyer should also develop and maintain a facility with advances in technology in areas in which the lawyer practices to maintain a level of competence that meets the standard reasonably expected of lawyers in similar practice circumstances. [emphasis added]

Commentary 6 to Rule II states in part, on the subject of "Seeking Assistance," that

> The lawyer must be alert to recognize any lack of competence for a particular task and the disservice that would be done the client by undertaking that task.

**Practice Competence Best Practices**

To meet the ethical obligation for competence in Rule II, lawyers must be able to recognize when the use of a technology may be necessary to perform a legal service on the client's behalf, and must use the technology responsibly and ethically.

Lawyers may satisfy this duty by personally having a reasonable understanding of the technology and using it, or by seeking assistance from others who have the necessary proficiency. Lawyers also need to have a reasonable understanding of the technologies that their clients are using, when such knowledge is relevant to providing legal advice.

## 2. Confidentiality

**CBA Code of Professional Conduct: Confidentiality**

The Rule in Chapter IV of the Code (Rule IV) provides that:

> Maintaining Information in Confidence
>
> 1. The lawyer has a duty to hold in strict confidence all information concerning the business and affairs of the client acquired in the course of the professional relationship, and shall not divulge any such information except as expressly or impliedly authorized by the client, required by law or otherwise required by this Code.

Guiding Principle 1 of Rule IV reads:

> The lawyer cannot render effective professional service to the client unless there is full and unreserved communication between them. At the same time the client must feel completely secure and entitled to proceed on the basis that, without an express request or stipulation on the client's part, matters disclosed to or discussed with the lawyer will be held secret and confidential.

**Confidentiality Best Practices**

The Code principles apply to all forms of communication, including electronic communication using new information technologies. Lawyers must display the same care and concern for confidential matters regardless of the information technology being used.

Lawyers must ensure that electronic communications with or about a client are secure and not accessible to unauthorized individuals. When communicating confidential information to or about a client, lawyers should employ reasonably appropriate means to minimize the risk

of disclosure or interception of the information. In assessing whether to use a particular information technology to communicate confidential information to or about a client, lawyers should assess the situation from different perspectives. What are the risks that a particular information technology poses for inadvertent disclosure or interception? What impact will the choice of technology have on the client with respect to costs, accessibility, and ease of use?

Lawyers should inform a client of the risks of unauthorized disclosure and interception before using information technologies. Lawyers need to ensure that their clients, too, understand that they need to protect the confidentiality of communications to them. Seeking client consent before using a particular technology for communications may be appropriate.

Lawyers should also be aware that changes to information technologies mean changing risks over time. For example, in the shift from telephone answering machines to digital voicemail, telephone messages now attract confidentiality risks similar to those for e-mail communications, namely that messages can be easily saved, copied and forwarded.

## 3. Encryption

### Law Society Guidelines: Encryption

The Federation of Law Societies of Canada's "Guidelines on Ethics and New Technology", which have been adopted as published or in a revised form by many of the law societies (see Appendix 1: Resources, 3(i)), advise that lawyers should use encryption when the information is "extraordinarily sensitive." However, developments in both technology and the law support the use of encryption to protect all confidential information. This is an evolving issue.

Recent provincial privacy commissioner decisions have ruled that personal information must be encrypted when stored on vulnerable devices, such as laptop computers or USB drives. See the March 2007 decision of the Information and Privacy Commission of Ontario, and the September 2006 decision of the Alberta Information and Privacy Commission (cited in Appendix 1: Resources, 5(b)).

### Encryption Best Practices

It is therefore recommended that lawyers:

- use encryption to protect confidential information that is transmitted electronically (e.g. e-mails);
- implement computer access restrictions (e.g. strong passwords and encryption) to protect confidential information that is stored electronically, including confidential information stored on portable storage devices (e.g. USB drives), on mobile computing devices (e.g. laptops and personal data assistants (PDAs)), and on desktop and networked computers; and
- use full-disk encryption for any mobile computing device.

More information about passwords and encryption is in Appendix 3: Steps to Improve Information Technology Security.

## 4. Privilege

### CBA Code of Professional Conduct: Privilege

Confidential information includes privileged information. Guiding Principle 3 to Rule IV of the Code states:

> The importance of the even broader ethical rule regarding confidential information is illustrated by the Supreme Court of Canada's approach to solicitor-client privilege. The Court has held that solicitor-client privilege must remain as close to absolute as possible if it is to retain its relevance. Solicitor-client privilege is a rule of evidence, an important civil and legal right and a principle of fundamental justice in Canadian law. The public has a compelling interest in maintaining the integrity of the solicitor-client relationship. Confidential communications to a lawyer represent an important exercise of the right to privacy, and they are central to the administration of justice in an adversarial system.

### Privilege Best Practices

Lawyers should exercise the same care to protect the confidentiality and privilege of electronic communications as is normally expected of them using any traditional form of communication.

## 5. Electronic Storage, Retention and Deletion

### Court Rules on Electronic Retention and Production

In many Canadian jurisdictions, civil procedure rules and court rules with respect to document retention and discovery define "document" and "record" to include information in both paper and electronic formats.

### Electronic Storage, Archiving and Deletion Best Practices

#### *Storage*

To protect electronic information, measures should be undertaken to store electronic information and to have onsite and offsite backups.

Lawyers should:

- back up information that is stored electronically, ideally on a daily basis; and

- store one copy of removable storage media (such as CD-R, CD-RW, DVD-R, DVD-RW, magnetic tapes, removable hard drives, and other magnetic or optical media) in a secure, offsite, location that provides protection from fire, water damage, heat and other integrity risks.

Offsite physical storage of computer information protects data from being corrupted or lost, and facilitates data recovery in the event of a disaster, such as a flood, earthquake, fire, power failure, power surge or destruction of the physical site of the law office.

Technology applications sometimes become obsolete (*e.g.* 5 ¼ inch floppy disks), and the media on which information is stored may degrade over time, rendering the information unreadable or irretrievable. Lawyers should, therefore, on a routine basis:

- revisit policies on storing and backing up electronic information to ensure that the chosen methods remain compatible with current technology; and
- check stored electronic information to ensure that the information is retrievable and that the media and applications are operable.

Storing data only in an electronic format may be appropriate for some clients, but for other clients, retaining both electronic and paper versions may be prudent. A "paperless office" means an office with a policy of not keeping paper copies, except where original hard copies are required for evidentiary or other legal purposes. Factors to consider before choosing a "paperless" relationship with a client include the client's preferences, the client's resources, the client's knowledge of and familiarity with technology, and legal obligations governing document retention and electronic discovery rules.

***Archiving***

Lawyers should implement document management practices that comply with the legal requirements for records retention for electronically-stored information. Where retention obligations require the preservation of a record, the electronic information should be preserved without alteration and should be protected from corruption, spoliation and deletion. Appropriate archival methods should be used to preserve electronically-stored information that is not on the law practice's active computer system.

Electronically-stored client information presents distinctive challenges regarding disclosure and production for electronic discovery, due to the potentially wide scope and high costs, uncertainties about the form of production, challenges regarding preservation of the integrity of the information, and difficulties of evaluating the proportionality of the costs and time for producing potentially relevant electronic information to the nature, purpose and complexity of the dispute.

Guidelines and recommended best practices for electronic discovery include Ontario's guidelines for the discovery of electronic documents and the Sedona Canada principles for electronic document production. They recommend meeting regularly with clients to discuss electronic discovery issues and best methods to use to preserve electronic data. (See Appendix 1: Resources, 5(b).)

***Deletion***

Deleting a document should be done in compliance with any applicable document retention obligations.

There are several ways to delete documents on a computer. The deletion method should be appropriate to the level of sensitivity of information in the document.

The standard "delete" function is to delete the file, and then empty the computer's recycle or trash bin. Deleting a file removes the name of the file from the directory of a computer and marks the space on the computer's hard drive which the file had occupied as available space that can be written over to store other files.

After a standard delete, however, a document, or other file, continues to be recoverable from the computer's hard drive. It may take considerable computer usage before a computer overwrites the particular freed space in the memory of a computer's hard drive. A standard delete does not prevent the contents of the document or other file from being recovered. Moreover, the contents of deleted documents and other files can be recovered even after they have been overwritten.

To purge sensitive data on a computer so the contents cannot be recovered by anyone, including a subsequent owner of the computer or someone who acquires a stolen or lost computer, other deletion measures must be taken. "Wiping," "scrubbing" or "shredding" securely deletes anything on a computer's hard drive so it cannot be restored. Shredding is more time consuming than a standard deletion, but the time required to perform even a strong "military wipe," has been substantially reduced by programs introduced in 2007.

File wiping software programs work by overwriting the contents of a file with new random ("garbage") data multiple times and by removing information about that file in the computer's directory. Examples of these programs can be found through Internet searches, using terms such as "file wiping" or "data wiping."

Some computer manufacturers and recycling organizations offer programs where computers can be returned for recycling. Several jurisdictions in Canada have enacted, or are considering, measures to reduce e-waste through mandatory or voluntary e-waste initiatives. If a computer containing confidential information is to be relinquished, as part of these recycling initiatives or otherwise, the most prudent way to protect the data on the hard drive against unauthorized access is to scrub the hard drive by means of a file wiping program.

Another option is to destroy the medium that stores the confidential data. This is generally considered to be the most secure method for ensuring that data cannot be recovered. For confidential information that has been copied onto portable storage media such as DVDs or CDs, CD shredders can be used to permanently destroy the DVD or CD.

(See Appendix 1: Resources, 5(b).)

# 6. Metadata

**Overview**

Metadata, in simplest terms, is information about other data. Many computer programs embed information into the program output when it is created, opened and saved.

Some metadata is stored internally as part of the program's output. The output could be files, images, presentation slides, documents, spreadsheets or other output. For this section, the word "document" is used to represent all these kinds of program outputs.

Metadata, although hidden on normal viewing, can be revealed and accessed by others when the document is circulated electronically. The information in metadata may include:

- the document author's name, initials, firm name, computer name, or the name of the network server or hard disk where the document was saved;
- the date the document was created;
- the identities of other authors;
- the identities of reviewers;
- document revisions, including insertions and deletions, tracked changes and comments added by reviewers;
- revision counts;
- the date of the last save, last edit and last print;
- the number of times the document has been printed;
- the distribution of the document;
- information about the printer on which the document was printed;
- information about the template used to create the document;
- document versions;
- total editing time;
- location of the stored file (e.g. C://desktop/clientname/filenumber); and
- bookmarks and customized styles.

Metadata in electronic documents can be useful during the drafting stages of a document, enabling collaboration through adding comments, tracking revisions, or recording information about each version of the document. However, metadata may be harmful when the document is distributed electronically to others, for instance, when submitting an electronic file to a court, circulating a draft of a document to opposing counsel in the course of negotiations, or distributing documents to adverse parties. The document's metadata may contain hidden information that the sender would not want to share with the recipients, such as comments on revisions or the time and by whom the comments were made.

Without taking steps to eliminate metadata, it will be part of a document no matter what means are used to distribute the document – by attaching it to an e-mail; copying it to a memory stick, a DVD or CD format or to a disk; or uploading it to a network or extranet. The embedded information, although not visible when normally viewing the document, can easily be accessed in a human-readable form through simple steps such as right-clicking and viewing the properties of a document or using a text-editor.

Rule IV, Commentary 4, provides as a general rule that a lawyer should not disclose having been consulted or retained by a person except to the extent that the nature of the matter requires such disclosure. The metadata could reveal, for instance, confidential information about a client or the fact that the client has consulted with the lawyer, and violate the duty of confidentiality.

**Metadata Best Practices**

Lawyers have an ethical obligation, when transmitting documents electronically, to exercise reasonable care to ensure that clients' confidential information is not disclosed in the metadata.

There are practices that minimize the creation of metadata, as well as ways to remove the hidden data before distribution or publication so it is not accessible to people for whom it is not intended. Before removing metadata, lawyers should ensure that there are no legal requirements to retain the metadata (*e.g.* discovery obligations).

"Mining" refers to actions taken to find and uncover hidden metadata that the document creator or document sender did not intend to reveal. Lawyers may wish to guard against metadata mining by negotiating confidentiality agreements or seeking protective orders to protect metadata information from being used by the recipient against the sending party or from being introduced as evidence in litigation.

Specific suggestions for limiting the creation of metadata and for removing metadata are in Appendix 2: Metadata Information and Resources.

## 7. Security

**Overview**

When lawyers use information technologies, such as faxes, cell phones, e-mail, web mail and wireless devices, to communicate about or with a client, they should take appropriate steps to reduce the risk of inadvertent disclosure or interception of the communications and unauthorized access to the information.

Computer security vulnerabilities include:

- "malware" – a term for malicious and unwanted software designed to enter a computer system without consent and damage the hardware, software or electronic

information stored on the computer, and includes computer viruses, worms, adware, spyware and Trojan horses;

- use of wireless communication technologies that can be intercepted if improperly set up without security measures, such as encryption;
- unauthorized interception and copying of data; and
- loss of data through theft, accidental loss, breakage, obsolescence, corruption or degradation of the storage media, disasters, power failures and power surges.

**Security Best Practices**

The security of confidential electronic communications and information can be improved, and the risk of data loss and unauthorized communications and data access minimized, by measures such as:

- requiring authentication (e.g. strong passwords);
- using encryption;
- installing firewalls and intrusion detection software;
- employing anti-virus software;
- establishing clear policies for everyone to follow on computer use to ensure the security and integrity of firm data on Internet, laptops, and desktop computers; and
- securing wireless networks.

(See Appendix 3: Steps to Improve Information Technology Security.)

## 8. Marketing

**CBA Code of Professional Conduct: Marketing**

The Rule in Chapter XIV (Rule XIV) on "Advertising, Solicitation and Making Legal Services Available" states:

> Lawyers should make legal services available to the public in an efficient and convenient manner that will command respect and confidence, and by means that are compatible with the integrity, independence and effectiveness of the profession.

Guiding Principle 3 to Rule XIV provides:

> Despite the lawyer's economic interest in earning a living, advertising must comply with any rules prescribed by the governing body, must be consistent with the public interest, and must not detract from the integrity, independence or effectiveness of the legal profession. Advertising must not mislead the uninformed or arouse unattainable hopes and expectations, and must not adversely affect the quality of legal services, or be so undignified or otherwise offensive as to be prejudicial to the interests of the public or the legal profession.

Guiding Principle 7 to Rule XIV states in part that

> lawyers may offer professional services to prospective clients by any means except means (a) that are false or misleading… or (e) that otherwise bring the profession or the administration of justice into disrepute.

**Marketing Best Practices**

Advertising that uses information technologies such as websites, list services, blogs and wikis needs to meet the Code's marketing principles.

Lawyers should have the same concern for the integrity of the communication when using information technologies as they do when advertising through traditional means, such as printed brochures, television commercials or telephone books. Lawyers should abide by the rules of their governing body with respect to advertising online and through other information technologies.

Lawyers should also follow applicable legislation and governing body rules and regulations on unsolicited commercial e-mails.

Online resources are available to ensure that a website is functioning properly. These resources check that the links on websites are not broken and validate that the HTML and XHTML markups of webpages are compliant with the standards of the World Wide Web Consortium. These online resources can be found by entering keywords such as "browser compatibility," "broken links," "standards compliance," "link validation," "HTML validation" or "XHTML validation" into a search engine.

(See Appendix 1: Resources, 5(c).)

## 9. Accessibility

**CBA Code of Professional Conduct: Accessibility**

The Rule in Chapter XX (Rule XX) on "Non-Discrimination" provides that:

> Except where differential treatment is permitted by law the lawyer shall not discriminate… on grounds including, but not limited to, an individual's ancestry, colour, perceived race, nationality, national origin, ethnic background or origin, language, religion, creed or religious belief, religious association or activities, age, sex, gender, physical characteristics, pregnancy, sexual orientation, marital or family status, source of income, political belief, association or activity, or physical or mental disability.

Commentary 1 to Rule XX, "Duty of Non-Discrimination," states:

1. The lawyer has a duty to respect the dignity and worth of all persons and to treat persons equally, without discrimination. Discrimination is defined as any distinction that disproportionately and negatively impacts on an individual or group identifiable by the grounds listed in the Rule, in a way that it does not impact on others. This duty includes, but is not limited to: (a) the requirement that the lawyer does not deny services or provide inferior services on the basis of the grounds noted in the Rule…

**Accessibility Best Practices**

Information technologies enhance access to the law and legal resources because information is available more quickly and less expensively, resulting in increased access to justice. Hardware and software systems and assistive technologies such as screen readers, touch screens, voice recognition technologies, one-button controls or hands-free systems, can greatly improve access to the law for people with disabilities. However, it is important that the choice of a technology does not outpace the capacity of a client to use it. Not all clients have computer systems with large storage capacities or can afford the latest versions of software.

As well, while website design and information technology formats make it possible for people, regardless of their individual physical or sensory abilities, to access the material, website designs must be compatible with assistive technologies to be useful.

The Web Content Accessibility Guidelines (WCAG) issued by the World Wide Web Consortium (W3C) provides authoritative guidelines on website accessibility. (See Appendix 1: Resources, 5(d).)

## 10. Service Delivery

**CBA Code of Professional Conduct: Service Delivery**

Providing legal services over the Internet may violate governing bodies' rules on the unauthorized practice of law. See the Rule in Chapter XVII of the Code and governing bodies' provisions on practice by unauthorized persons.

**Service Delivery Best Practices**

The speed and global nature of the Internet raise particular ethical issues. Lawyers should ensure that electronic delivery of legal services is consistent with the Code principles on conflicts of interest and confidentiality. They should not appear to be offering advice in a jurisdiction where they are not authorized to practice.

In delivering services through information technologies, such as e-mail or text messaging, lawyers should take care that information is not inadvertently disclosed to unintended recipients. Lawyers should review electronic addresses to ensure that only the intended recipients receive the communications.

Lawyers should think twice and be certain of their intention before:

- using “reply all” on e-mail;
- using the automatic fill-in functions of e-mail applications; or
- using “reply” with a group list service, which would result in the reply being sent to all e-mail addresses registered with the group e-mail distribution list.

## 11. Intellectual Property and Software

### Licence Requirements

Software typically comes with end-user licence agreements that specify the terms of use and the permission to use the associated intellectual property in the software.

Typical arrangements for licences are:

- a user-based licence that restricts the software to a single user;
- a site licence that permits the software to be used at a particular location; or
- a network licence that permits a maximum specified number of users to use the software at the same time.

The licence may also specify a date after which the purchaser is no longer licenced to use the software.

Vendors may provide the terms of the licence by enclosing them in the box with the software (shrink-wrap) or by presenting them online during the software installation process (click-wrap or browse wrap).

Open source software is also available under a variety of open source licences.

### Intellectual Property and Software Best Practices

Lawyers should carefully review and comply with the terms of applicable software licences. Compliance steps include conducting periodic software audits, establishing software policies, maintaining logs, and educating all lawyers and staff on compliance with software licencing requirements.

(See Appendix 1: Resources, 5(e).)

## 12. Electronic Legal Research and Information Retrieval

Increasing numbers of authoritative and accurate electronic sources for primary and secondary law materials are available through Internet-based search services and through online and CD-ROM databases. Many of these sources are freely available to the public, including the material on the legal portals CanLII and LexUM, and statute and case databases. See Appendix 1: Resources, 5(f).

The Internet facilitates dynamic and up-to-date information. However, the Internet's dynamism can also be a drawback. "Link rot" or "broken link" refers to common occurrences such as URL changes, website relocations, content changes, website redesigns, the disappearance of a website or webpage, and inactive URLs that no longer direct the user to a working version of a webpage. Additionally, information on websites, especially topically-oriented sites that continually update their content, may no longer be available in the same location.

**Electronic Legal Research and Information Retrieval Best Practices**

If an official copy is required for law practice (*e.g.* for a filing to a court or tribunal), the status of online legal information (as official or unofficial) should first be verified on the issuing site.

Prudent practice dictates saving websites as PDFs, including the URL and the date of access, to preserve a record of the information and to enable online information to be attributed and properly cited. Online resources, like other resources are cited in legal materials, should provide adequate information to attribute sources to their authors and enable readers to find the cited sources.

(See Appendix 1: Resources, 5(f).)

## 13. Participation in Online Discussions

**CBA Code of Professional Conduct: Online Discussions**

The Rule in Chapter XVIII (Rule XVIII) provides:

> The lawyer who engages in public appearances and public statements should do so in conformity with the principles of the Code.

Participation in online discussions is a type of public appearance, which can have important benefits for public education about the law. (Rule in Chapter XV, and Commentaries 7–9, 11–13 to Rule XVIII.)

At the same time, participation in online forums can pose concerns for:

- client confidentiality (Rule in Chapter IV);
- unintended formation of client relationships (see definition of "client" in Interpretation; Rule in Chapter III, "Advising Clients"); and
- conflicts of interest (Rules in Chapters V–VI; Commentary 6, to the Rule in Chapter VI).

The Rule in Chapter VII of the Code on "Outside Interests and the Practice of Law" (Rule VII) provides that,

> The lawyer who engages in another profession, business or occupation concurrently with the practice of law must not allow such outside interest to jeopardize the lawyer's professional integrity, independence or competence.

**Online Discussion Best Practices**

The Internet offers many opportunities for lawyers to communicate to and interact with other lawyers and non-lawyers in Canada and globally. Participation in online discussions can take the form of postings and comments to blogs, law blogs ("blawgs"), wikis, chat rooms, Internet forums, list serves, social media, and other electronic forums and media. A lawyer's communications in online public forums are public statements that should be in conformity with the Code.

Lawyers who communicate in online forums should ensure that they make clear when they are writing as a lawyer and offering legal services. In those instances, they should provide contact information, and be certain they are able to identify the person with whom they are communicating. Conflict traps lurk in cyberspace. Further, any statement concerning the client's affairs should be in the best interests of the client and within the scope of the retainer (Commentary 2 to Rule XVIII).

Lawyers who participate in online discussions should be vigilant to avoid jeopardizing their professional integrity, independence or competence (See Rule VII, "Outside Interests and the Practice of Law").

Lawyers should be courteous, civil, and act in good faith with respect to everyone with whom they have dealings in the course of an action or proceeding. This includes their communications in online discussions (Commentary 16, "Courtesy," to the Rule in Chapter IX).

In communicating online, lawyers should encourage public respect for, and try to improve, the administration of justice (Rule in Chapter XIII). Any criticism of, and proposals for improvements in, the legal system should be *bona fide* and reasoned (Guiding Principle 2 to Rule XIII).

Commentary 3 to Rule XIII states that the "lawyer in public life must be particularly careful in this regard because the mere fact of being a lawyer will lend weight and credibility to any public statements."

Lawyers should be circumspect in their participation in online public discussions. Online public discussions should be conducted with the same respect for the administration of justice required of public statements that lawyers may make in other forums and media.

Public statements in online forums must comply with the Rule in Chapter XIV on advertising, solicitation, and making legal services available.

## Appendix 1: Resources

### 1. General Information

M. Drew Jackson and Timothy L. Taylor, *The Internet Handbook for Canadian Lawyers*, 3d. ed. (Carswell, 2000).

Carole A. Levitt and Mark E. Rosch, *The Lawyer's Guide To Fact Finding On The Internet*, 2d ed. (American Bar Association, 2004)

Barry Sookman, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions* (Toronto: Carswell, 2006)

Index of File Extension Information (*e.g.* defining PDF, DOC, WPD): <http://www.fileinfo.net/common.php>.

TechnoLawyer: http://www.technolawyer.com

### 2. Resources for Conducting Canadian Legal Research Online

Canadian Legal Information Institute (CanLII): <www.canlii.ca>.

LexUM: http://www.lexum.umontreal.ca/index.epl?lang=en

### 3. Legal Ethics and New Information Technologies

#### (i) Law Society Guidelines on Ethics and the New Technology

Federation of Law Societies of Canada, "Guidelines on Ethics and the New Technology," National Ethics Group of the National Technology Committee, Federation of Law Societies of Canada (1999)

Law Society of Alberta, "Ethics and New Technology Guidelines" (modified), <http://www.lawsocietyalberta.com/lawyerservices/FromTheAdvisor/FromPracticeadvisor2/ethicsandtechnology.cfm#1>.

Law Society of British Columbia, "Guidelines on Ethics and the New Technology," (modified),<http://www.lawsociety.bc.ca/practice_support/articles/FedGuidelines.html>

Law Society of Newfoundland and Labrador, "Guidelines on Ethics and the New Technology" (modified and appended as Schedule A to Newfoundland and Labrador's Code), <http://www.lawsociety.nf.ca/code/code_schedulea.asp>.

Law Society of New Brunswick, "Guidelines on Ethics and the New Technology" (appended to New Brunswick's Code), <http://lawsociety-barreau.nb.ca/assets/documents/Code_of_professional_conduct_March_2006.pdf>.

Law Society of Upper Canada, "Guidelines on Ethics and the New Technology," (modified), <http://www.lsuc.on.ca/media/tech_guidelines.pdf>.

Nova Scotia Barristers' Society, "Guidelines on Ethics and the New Technology," <http://www.nsbs.ns.ca/publications/techno_ethics_guidelines.pdf>.

Manitoba, "Guidelines on Ethics and the New Technology" (modified), <http://www.lawsociety.mb.ca/pubdocs/ethics_newtech.pdf>.

Saskatchewan, "Guidelines on Ethics and New Technology" (appended to Code of Professional Conduct): <www.lawsociety.sk.ca/newlook/PUblications/EthicsTech.pdf >.

**(ii) Other**

Law Society of Upper Canada, *Technology Guideline*, Member Resource Center: <http://mrc.lsuc.on.ca/jsp/pmg/technology.jsp>

ABA, "Ethics and Technology 2006: How NOT to Commit Malpractice With Your Computer," ABA, Law Practice Management Section, Center for Professional Responsibility, Standing Committee on Lawyers' Professional Liability, and the ABA Center for Continuing Legal Education

Legal Ethics, <www.legalethics.com> (website with resources on primarily US-based legal ethics subjects, including ethics and information technologies)

**4. Information Technologies Resources**

World Wide Web Consortium (W3C): <http://www.w3.org/ >.

Treasury Board, Chief Information Officer Branch, Government of Canada: <http://www.tbs-sct.gc.ca/cio-dpi/index_e.asp >.

LawPRO (Lawyers' Professional Indemnity Company (Canada)), "Resources @ Technology Associations," LawPRO's practice Pro technology resources: <http://www.practicepro.ca/information/tassocs.asp>.

LawPro Links: An A-Z Directory of Web Resources (US-based; not affiliated with Lawyers' Professional Indemnity Company (Canada)) : <http://www.llrx.com/llrxlink.htm >.

Slaw.ca, cooperative weblog about Canadian legal research and IT: <http://www.slaw.ca/ >.

## 5. Specific Resources

### (a) Introduction

Canadian Bar Association, Code of Professional Conduct:
http://www.cba.org/CBA/activities/code/

### (b) Electronic Storage, Retention and Archiving

Information and Privacy Commissioner of Alberta, Investigation Report P2006-IR-005 (September 2006), online:
<http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf >

Canadian e-Discovery Portal (LexUM): <http://www.lexum.umontreal.ca/e-discovery/>.

Guidelines for the Discovery of Electronic Documents in Ontario:
<http://www.oba.org/en/pdf_newsletter/E-DiscoveryGuidelines.pdf >.

Discovery Task Force E-Discovery Guidelines and Resource page, Ontario Bar Association: <http://www.oba.org/en/main/ediscovery_en/default.aspx >.

Information and Privacy Commission of Ontario, Order HO-004 (March 2007), online: <http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf >

Sedona Canada Principles: Addressing Electronic Document Production (February 2007 Public Comment Draft) : <http://www.lexum.umontreal.ca/e-discovery/2_07WG7pubcomment.pdf > (disclosure and discovery of electronically stored information in Canadian civil litigation)

Les Sedona Canada Principles : La Production des Documents Électroniques (May 2007 Version Publique Pour Commentaires) : <http://www.lexum.umontreal.ca/e-discovery/5_07SedonaCanadaFrancais.pdf >.

The Sedona Conference Glossary for E-Discovery and Digital Information Management (January 2008 Version):
http://www.thesedonaconference.org/content/miscFiles/canada_pincpls_FINAL_108.pdf

Practice PRO, “Electronic Discovery: A Reading List,”
<http://www.practicepro.ca/practice/eDiscovery_Rlist.asp >.
E-discovery Amendments and Committee Notes, United States Federal Rules of Civil Procedure (effective December 2006):
<http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf >.

Ann Macaulay, “How to Make Your Office (Almost) Paperless,”
<http://www.cba.org/cba/PracticeLink/TAYP/paperless.aspx >.

**(c) Marketing**

W3C (World Wide Web Consortium) HTML and XHTML Markup Validation Service: <http://validator.w3.org/>.

**(d) Accessibility**

Treasury Board of Canada, "CLF for the Internet—Accessibility" (2004): <http://www.tbs-sct.gc.ca/clf-nsi/inter/inter-01-00_e.asp >.

World Wide Web Consortium (W3C), "Web Content Accessibility Guidelines (WCAG): <http://www.w3.org/TR/WAI-WEBCONTENT/ >.

Adobe's information for improving online accessibility, its guide for making PDF formats accessible for people with visual, hearing, and learning disabilities and for people with motor or dexterity impairment, and its instructions for making PDFs accessible for screen readers: < www.adobe.com/accessibility/ >.

Adobe's conversion service (in which a URL of a PDF can be sent to Adobe and Adobe returns the contents in either HTML or in plain text for speech conversion software): < http://www.adobe.com/products/acrobat/access_onlinetools.html >.

Additional resources for information technology accessibility can be found by entering keywords such as "web page accessibility," "HTML accessibility," "browser compatibility," "WCAG" or "section 508" (U.S. accessibility standard), into a search engine.

**(e) Intellectual Property and Software**

Lists of common open source software for office applications are available at

<http://www.webi.org/ > and

<http://en.wikipedia.org/wiki/List_of_open_source_software_packages >.

**(f) Electronic Legal Research and Information Retrieval**

CanLII: < http://www.canlii.ca/ >

LexUM: < http://www.lexum.umontreal.ca/ >

Department of Justice (Canada): < http://laws.justice.gc.ca/en >

**Courts of Appeal:**

Alberta: < http://www.albertacourts.ab.ca >

British Columbia: < http://www.courts.gov.bc.ca/ca >

Manitoba: < http://www.manitobacourts.mb.ca/ >;

<http://www.canlii.org/en/mb/mbca/index.html > (judgments)

New Brunswick: < http://www.gnb.ca/cour/03COA1/index-e.asp >;

<http://www.canlii.org/en/nb/nbca/index.html > (judgments)

Newfoundland: < http://www.justice.gov.nl.ca/just/lawcourt/appeal.htm >;

< http://www.canlii.org/nl/cas/nlca > (judgments)

Nova Scotia: < www.courts.ns.ca/Appeals/index_ca.htm >

Ontario: < www.ontariocourts.on.ca/appeal.htm >

Prince Edward Island: < http://www.gov.pe.ca/courts/supreme/index.php3 >;

< http://www.canlii.org/en/pe/pescad/index.html > (judgments)

Quebec: < www.tribunaux.qc.ca/mjq_en/c-appel/index-ca.html >

Saskatchewan: < http://www.lawsociety.sk.ca/newlook/Library/database.htm >

(judgments)

Nunavut: < http://www.nucj.ca/index.htm >;

< http://www.canlii.org/en/nu/nuca/index.html > (judgments)

Northwest Territories: < www.justice.gov.nt.ca/dbtw-wpd/nwtjqbe.htm >

Yukon: < http://www.yukoncourts.ca/courts/appeal.html >

Federal Court of Appeal: < http://decisions.fca-caf.gc.ca/en/index.html >

**United States:**

US Government Portal: < http://www.usa.gov/ >

LII: Legal Information Institute (Cornell)

< www.law.cornell.edu/ >

**European Union:**

< http://eur-lex.europa.eu/en/index.htm > (English)

< http://eur-lex.europa.eu/fr/index.htm > (French)

**World Legal Information Institutes:**
< http://www.worldlii.org/ >

## Appendix 2: Metadata Information and Resources

### 1. Resources

Electronic Frontier Foundation, "List of Printers Which Do or Do Not Display Tracking Dots," < http://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots>

Electronic Frontier Foundation, "Harry Potter and the Digital Footprints," <http://www.eff.org/deeplinks/2007/07/harry-potter-and-digital-fingerprints >.

### 2. Drafting Practices that Create or Carry Over Metadata

Common drafting practices can create or contain metadata. Starting from a completed document and using the "save as" function can carry over metadata associated with the original document. Collaborative tools, such as comments and track changes, create metadata about reviewers, authors, previous versions, revisions, and deleted and redacted information. Including the file location (especially if it incorporates client information) in footers and headers can unintentionally reveal more information than desired (*e.g.* that a client relationship exists) if the document is later distributed to others.

### 3. Avoidance and Removal

Document creators can:

a) minimize the creation of metadata; or

b) remove metadata to produce a clean copy of a document.

#### a. Minimizing the Creation of Metadata

The creation of metadata can be minimized by the following practices:

i. Start to draft a document by using a template with only minimal (and non-client specific) information. If a document is "re-purposed" by starting from a completed document and "saving as" to give the document a new name, there is a risk that the metadata from the original document will be carried over to the "re-purposed" document.

ii. Accept track changes before the document is distributed. Merely switching to a viewing mode that does not reveal track changes information (*i.e.* switching from "Final" to "Final Showing Markup) does not remove the information. To remove the information, use the "accept all changes in document" button. For documents in which the collaborative features of track changes and comments are not needed, those features should be turned off at the beginning to avoid creating metadata.

iii. Do not allow fast saves. In Microsoft Word, PowerPoint, and Excel, this option can be turned off by Tools>Options>Save Tab, and unchecking the box for "allow fast saves."

**b. Managing and Removing Metadata**

Metadata in documents can be managed, minimized and removed by:

i. using features built-in to the program to reveal and to remove hidden identifying information;

ii. installing add-ons from the program vendor (*e.g.* Microsoft, Adobe, Corel); or

iii. using programs from third-party vendors.

Programs with features to manage the creation of metadata, removal of metadata and production of clean documents are often termed "metadata scrubbing programs," "metadata removal tools" or "metadata management software." These programs can be used to prevent sensitive information from being disclosed inadvertently.

**(i) Using Features Built into the Program**

The numerous applications and programs used in law practices cannot be covered comprehensively here, but the following recommendations illustrate how internal features in some of the most commonly used programs can be accessed.

Microsoft Office Word 2003 or Word XP
In Microsoft Office Word 2003 or Word XP, metadata embedded in a document can be determined by going to Open>File>Properties>. The tabs in the dialog box for General, Summary, and Statistics provide information about the document. To remove this identifying metadata from a document created in Word 2002 or Word 2003, go to Tools>Options>Security, and check the box to Remove Personal Information From This File On Save (Word 2002) or Remove Personal Information From File Properties On Save (Word 2003), and click on OK.

The same Security tab also provides options that can be checked to issue a warning before printing, saving or sending that a file contains tracked changes or comments, and to make hidden markup visible when opening or saving. The latter function provides reminders about the metadata in a document but does not remove it.

To create a clean copy of a document, copy the document into a clean file by going to Edit>Select All (Ctrl + A), then copy the document (Ctrl + C), open a new document (Ctrl + N), paste the contents (Ctrl + V) and then save this document with a new name by using the "Save As" function. To have a clean copy, the "Save As" function must be used in the new document. Renaming an existing document using "Save As" (*i.e.* opening up a document and treating it as an electronic template for a new document) will carry over metadata from the original document.

PowerPoint 2002

In PowerPoint 2002, metadata can be removed by File>Save As>Tools>Security Options>, then selecting "Remove personal information from this file on save" check box, and then click OK. For further information, see Microsoft Knowledge Base, "How to Minimize the Amount of Metadata in PowerPoint 2002 Presentations".

Microsoft Excel

For Microsoft Excel, see Microsoft Knowledge Base, "How to minimize metadata in Microsoft Excel workbooks".

Additionally, the Information Rights Management function in Office 2003 can be set to reduce metadata.

WordPerfect

To view metadata in a document created in WordPerfect, select File>Properties for summary statistics. The revision history can be viewed by going to Edit>Undo/Redo. The option for the revision history can be turned off by de-selecting the button for "Save Undo/Redo items with document" under the Edit/Undo/Redo/Options button. Corel offers a program for WordPerfect Office X3 documents, in the File>Save Without Metadata. Additional information can be found in Corel's Knowledge base, <http://support.corel.com/scripts/rightnow.cfg/php.exe/enduser/std_alp.php>, Answer ID 753605 and 759035.

Adobe's Portable Document Format

Adobe's Portable Document Format (customarily described as "PDF" format) usually includes less metadata than Microsoft Office and other office productivity applications, but metadata can still be included in a PDF document. In a PDF, metadata may be embedded either through the Acrobat features themselves (such as Acrobat "sticky notes") or because the information was present in a document that was created in another program (*e.g.* WordPerfect or Word) before it was converted to a PDF document and the metadata from that program was carried over into the PDF document. Examples of metadata in PDF documents include keywords, annotations and comments, and field information.

To view a summary of the metadata in a PDF document, select File>Document Properties.

To set security options, click the boxes for the preferences in the dialog box that appears.

Acrobat 8 includes a metadata removal feature called Examine Document, accessed by choosing Document>Examine Document>, then click the information to remove (metadata, hidden text, annotations and comments, bookmarks) and then select the Remove All Checked Items boxes. Metadata is used in PDF documents to track Bates Numbers, so removing metadata will affect the functioning of features related to Bates Numbers.

### (ii) Installing Add-ons from the Program Vendor

Word, PowerPoint, and Excel

One example of an add-on from a program vendor is Microsoft's free "Remove Hidden Data" add-on to help permanently remove hidden data and collaboration data for Word, PowerPoint and Excel in versions 2003 and XP. This add-on can be downloaded and installed at: <http://www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&displaylang=en>.

This tool can be used to create a clean copy before the document is distributed or published, while allowing collaboration features such as comments and track changes to function as the document is being prepared. From an open document, go to File>Remove Hidden Data>, and when the dialog box appears, type a name for the new clean version, and click Next. At the completion of the process, a results log also appears.

This "Remove Hidden Data" feature is included in the Office 2007 suite.

### (iii) Using Programs from Third-Party Vendors

Examples of metadata removal programs by third-party vendors that scrub output from applications in Microsoft and Adobe include:

- Payne Metadata Assistant http://www.payneconsulting.com/products/;
- Workshare Protect http://www.workshare.com/products/;
- Doc Scrubber < www.docscrubber.com >;
- Softwise Consulting's Out-of-Sight www.softwise.net/frameSet.html; and
- iScrub http://esqinc.com//index.php?p=products&id=2.

OpenDoc

Metadata scrubbing programs are also available for the OpenDoc open source office suite, such as 3BView's 3BClean product, <www.3bview.com/3bclean.html>.

Many of these third-party programs provide more finely calibrated customization options than the manufacturers' computer software versions. For example, they may include options to permit some metadata, so the document maker can take advantage of functions requiring that information, and to set distribution parameters that work with other programs such as Outlook or Notes and will prevent the document from being distributed externally. Some programs have a feature to automatically remove metadata from e-mail attachments before they are sent.

## 4. References and Resources for Metadata

David Hricik, "Mining for Metadata: Is it Ethical to Take Intentional Advantage of Other People's Failures?"(33rd National Conference on Professional Responsibility, delivered at the Fairmont Chicago, 2 June 2007), (Aspen Publishers, 2007) 1.

Office of the Privacy Commissioner of Canada, "The Risks of Metadata," <http://www.privcom.gc.ca/fs-fi/02_05_d_30_e.asp >.

American Bar Association, Standing Committee on Ethics and Professional Responsibility, "Review and Use of Metadata," Formal Opinion 06-442, 5 August 2006.

Microsoft, Knowledge Base, "How to Minimize Metadata in Microsoft Excel workbooks," < http://support.microsoft.com/kb/223789/EN-US/ >.

Microsoft, Knowledge Base, "How to Minimize Metadata in Office Documents," Article 22396, < http://support.microsoft.com/kb/223396/en-us >.

Microsoft Knowledge Base, "How to Minimize the Amount of Metadata in PowerPoint 2002 Presentations," < http://support.microsoft.com/kb/314800 >.

Microsoft, Knowledge Base, "Remove Hidden Data Tool for Office 2003 and Office XP," Article 834427, < http://support.microsoft.com/kb/834427 >.

Microsoft, Knowledge Base, "Control metadata in your legal documents," < http://office.microsoft.com/en-us/help/HA011400341033.aspx >.

Corel, Knowledge base, "How Can I Remove Metadata From WordPerfect Documents," Answer ID 753605; and "How Do I Remove Metadata From a WordPerfect Document," Answer ID 759035; available through the search engine at: <http://support.corel.com/scripts/rightnow.cfg/php.exe/enduser/std_alp.php >.

United States National Security Agency, "Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF," <http://www.fas.org/sgp/othergov/dod/nsa-redact.pdf >.

Dan Pinnington, "Beware the Dangers of Metadata," *LawPRO Magazine* (June 2004), available at: <www.lawpro.ca/magazinearchives>.

"e-Discovery," September 2005 issue *LawPRO Magazine*: <http://www.lawpro.ca/lawpro/LawPROmagazine4_2_Sep2005.pdf>.

## Appendix 3: Steps to Improve Information Technology Security

### 1. Backups of Data

To protect against the loss of data from theft, power failures, power surges, disasters, or damage to hardware or software, it is best to regularly backup data and have secure off-site data storage. (See also section 6 in the Guidelines.)

### 2. Access Restrictions and Authentication Protocols

Access restrictions are used to limit access to a computer or network to authorized users. The most common protocols for access restrictions are passwords and, increasingly, smart cards and biometric systems.

Use a password that is easy to remember (without writing it down), hard to guess, and frequently changed. A strong password is difficult for another person to guess and for a computer to determine.

A password should contain a combination of alpha- and numeric-characters, lower- and upper-case letters, symbols, characters created from Alt or Control and another key on the keyboard, and should be at least eight characters long. The password should not be composed of a dictionary word (in any language), a dictionary word spelled backwards, or a dictionary word with digits only on the front or on the end. These passwords are especially vulnerable to "dictionary attacks" by hackers. Simple substitutions of other characters for letters in a dictionary word (such as the digit one for the letter "l"), sequences (such as chronological numbers or adjacent characters on a keyboard), repeated characters ("aaa"), usernames, and the default password that comes with the system should not be used.

Passwords should also not be composed of a personal name, a family member, a pet's name, or any biographical information such as birthdays, addresses or phone numbers.

It is good practice for a system to require password entry:

- at the time of startup of a computer;
- to return to work after the computer has been on standby ("sleep"), or the screen saver is on;
- when an application starts up; and
- when a file is opened.

### 3. Encryption

Encryption protects communications from being read by other than the intended recipients.

There are many encryption methods, but "public key encryption" is a common and effective method. OpenPGP is the most wide spread e-mail encryption standard. GnuPG and PGP programs follow that standard.

Common programs with file encryption and full hard-drive encryption features to protect information stored on laptops include:

- SafeGuard Easy http://americas.utimaco.com/;
- PGP Personal 8.0 http://www.pgp.com;
- SecureDoc http://www.winmagic.com; and
- PointSec for PC http://www.checkpoint.com/pointsec/.

Common programs to protect information stored on mobile handheld computing devices (*e.g.* PDAs, smartphones and wireless "push" e-mail) and removable media include:

- SafeGuardPDA and Safeguard PushMail http://americas.utimaco.com/;
- TealLock http://www.tealpoint.com/softlock.htm;
- PointSec Mobile http://www.checkpoint.com/products/datasecurity/mobile/index.html; and
- Smartphone Security http://www.trustdigital.com/products/smartphone_sec_client.asp.

**4. Firewalls and Intrusion Detection Software (IDS)**

Firewall technology is a software or hardware device that provides security for a computer or a computer network by managing permissions for data to exit or enter through a system of defined rules. Windows XP Service Pack 2, for example, includes Windows Firewall, a program which controls incoming (but not outgoing) traffic.

**5. Anti-Virus Software and Computer Security Software Suites**

"Anti-virus software" should be used to detect and remove malicious software (*e.g.* computer viruses, spyware, adware, worms) on a computer or computer network. A list of common anti-virus software, including commercial products, free software and open source options, can be found at http://en.wikipedia.org/wiki/List_of_antivirus_software.

Microsoft's Malicious Software Removal Tool is available for download at: <http://www.microsoft.com/security/malwareremove/default.mspx >.

"Stand-alone" anti-virus software is available, but more usually anti-virus software is packaged in a software suite that contains protection for a broad range of computer security vulnerabilities, such as malicious software, unauthorized intrusion, identity theft, phishing, unsolicited commercial e-mail, and undesired Internet pop-ups. Security suites often incorporate firewalls and other security features such as scanning e-mails for infected attachments and filtering URLs.

Commercial anti-virus and computer security protection is usually purchased as a software licence by a limited-period subscription, which can be renewed, for Internet-transmitted software updates.

Some common anti-virus software and computer security software suites include:

- PC Security Shield's Shield Deluxe: <http://www.pcsecurityshield.com/lp/shield-deluxe-4.aspx?trk=WTK&affid=650>
- Trend Micro Internet Security: <http://us.trendmicro.com/us/products/personal/index.html >
- Check Point's ZoneAlarm Internet Security Suite: <http://www.checkpoint.com/products/za_iss/index.html >
- McAfee's Total Protection, VirusScan Plus, and Internet Security Suite: <http://www.mcafee.com/ca-en/?langid=34>
- Microsoft Windows Live OneCare: <http://onecare.live.com/standard/en-us/default.htm>
- Kaspersky's Anti-Virus and Internet Security: <http://usa.kaspersky.com/>
- BitDefender's Internet Security, Antivirus, and Total Security: http://www.bitdefender.com/
- CA Anti-Virus and Anti-Spyware: <http://www.ca.com/ca/en/>
- F-Secure's Internet Security: <http://www.f-secure.com/estore/fsis2007.html>
- Symantec's Norton AntiVirus, Norton 360 and Norton Internet Security: <http://www.symantec.com/index.jsp>.

## 6. Policies on Computer Security for Employees

Computer security policies governing Internet, laptop and desktop computer use should be established for employees. Issues that can be covered under these policies include:

- appropriate intranet and Internet use;
- restrictions on the downloading, viewing and circulation of discriminatory and harassing content (see Rule XX);
- permitted use of law firm or company e-mail addresses;

- prohibitions on the use of portable storage medium (such as USB drives) or portable computers to carry non-secured unencrypted confidential information outside the office, given that these media are especially vulnerable to theft and loss;
- circumstances for using privileged-and-confidential-material warnings on e-mail; and
- limitations on the ability of employees to add or download software to networked or individual computers.

Protocols should be implemented that require the use of strong technical protection measures to protect confidential information on computers and to require that these measures be updated on an appropriate schedule to ensure an adequate level of protection for confidential information relative to current security options.

## 7. Securing Personal Information

Confidential personal information should be appropriately safeguarded. Confidential personal information is more vulnerable when it is aggregated and stored in one file location and is also more at risk for identity theft. Confidential personal information should not be accessible on the Internet.

Necessary protective measures to protect confidential personal information on computers include:

- strong technical measures, *e.g.* encryption and other access controls;
- physical measures, *e.g.* locks, cables, laptop tracking software, alarms; and
- administrative measures, *e.g.* compliance audits, employee education.

## 8. Wireless Networking

It is important to safeguard the privacy of communications and ensure against unauthorized access to the network. For example, there is a risk of interception when a computer communicates wirelessly to a printer. Unauthorized access to a network could occur from deliberate actions by crackers who, on entry to the network, could take passwords or install malicious software. Unauthorized access could also occur from accidental connections by those in proximity whose wireless devices connect to an inadequately secured wireless access point.

The security of a wireless network can be improved by the following practices:

- Use strong encryption. Wi-Fi Protected Access (WPA and WPA2) are examples of strong encryption to secure a network;

- Change the default password of the router, which links networked computers. The protocols for creating a strong password in "Access Restrictions and Authentication Protocols," Section 2 of this Appendix, should be applied;

- Change the default name of the wireless network (referred to as the "Service Set Identifier" (SSID)), and, in creating the new name, avoid usernames, the company name, the address, or other information that can be easily identified;

- Use firewalls on both the network device and the computer;

- Turn off the "auto connect" setting on your computer, in which the computer will automatically search for an open wireless network;

- Turn off the wireless network if there are certain times when persons will not be connecting or limit 24-hour access to certain users; and

- Connect only to secure wireless networks, if the activity is confidential.

### 9. Security Resources

"Password Security: A Guide for Students, Faculty, and Staff of the University of Michigan," University of Michigan, Information Technology Division, Reference R1192, Revised April 1997, < http://www.umich.edu/~policies/pw-security.html >
(Guides for choosing a strong password).

Microsoft, Security Central resource page: <http://www.microsoft.com/security/default.mspx >.

Rutgers**,** "Wireless Security Recommendations," <http://techdir.rutgers.edu/wireless.html >.

Microsoft, "Improve the Security of Your Wireless Home Network with Windows XP," <http://www.microsoft.com/windowsxp/using/networking/security/wireless.mspx >.
Alberta Information and Privacy Commissioner, Investigation Report P2006-IR-005 (September 2006), <http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf >

Information and Privacy Commissioner of Ontario, Order HO-004 (March 2007), <http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf >

PracticePRO, "Managing the Security and Privacy of Electronic Data in a Law Office," http://www.practicepro.ca/practice/ElectronicDataSecurity.asp

## Glossary

| | |
|---|---|
| blawg | a web log about the law |
| blog | a web log with entries arranged in reverse chronological order |
| broken web link | a cross-referenced hyperlink that is not working and does not bring the reader to the right working webpage |

| | |
|---|---|
| chat room | an online site where participants exchange messages through an online conversation |
| hacking | an unauthorized intrusion into a computer system, hence hacker, the person behind the intrusion |
| HTML | a coding language that defines how information is displayed on webpages |
| Internet forum | an Internet forum includes online discussion groups and message boards |
| list serve | an electronic mailing list in which messages addressed to the server are automatically redistributed to the list of subscribed e\|mail addresses |
| memory stick | a transportable device for storing data, also called a “thumb drive,” “flash drive” or “USB drive” |
| phishing | fraudulently using electronic communications to appear to be a legitimate business, for example, a bank, auction site, Internet service provider, or credit card company, by spoofing their brands and fooling users into disclosing sensitive personal information, such as passwords, usernames, and account information |
| pop-up | a website that automatically opens another small web browser window over the original website’s content. Pop-ups have practical functions but can also be used in phishing schemes and to display unwanted advertising. |
| scrubbing | an action to delete anything on a computer’s hard drive so that it cannot be restored |
| social media | examples include Facebook, YouTube, MySpace |
| spam | unsolicited commercial e-mail |
| strong password | a combination of numbers and letters that is difficult for another person to guess and for a computer to determine |
| URL | the abbreviation for Uniform Resource Locator, which is the address that is entered into the address bar of a web browser to take the user to a specific website or webpage: *e.g.* <http://www.cba.org/CBA/Gate.asp> |
| wikis | a collaborative accessible website where site visitors can edit the material |
| wiping | an action to delete anything on a computer’s hard drive so that it cannot be restored |
| XHTML | a coding language that defines how information is displayed on webpages |