THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
INFLUENCE. LEADERSHIP. PROTECTION.

Legal Ethics in a Digital World

CBA Ethics and Professional Responsibility Committee

(These guidelines build on the 2008 *Guidelines for Practising Ethically with New Information Technologies*, the 2009 *Guidelines for Ethical Marketing Practices using New Information Technologies* and the 2014 *Practising Ethically with Technology* guidelines.)

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8 **tel/tél. :** 613.237.2925 | **toll free/sans frais:** 1.800.267.8860 | **fax/téléc.:** 613.237.0185 | www.cba.org **Membership/Adhésion:** memberservice@cba.org | **PD/DP :** pd@cba.org | **Sections:** cba.sections@cba.org | **General/Général:** info@cba.org

Legal Ethics in a Digital World

Table of Contents

Introduction

Technology has become an important part of contemporary legal practice. Lawyers should be able to recognize when using technology is needed to provide a legal service effectively and understand how to use technology responsibly and ethically.[1] Although codes of professional conduct in Canada[2] do not explicitly require the use of technology like their American counterpart,[3] a number of ethical obligations under the codes – for example, to adapt "to changing professional requirements, standards, techniques and practices"[4] and to maintain "office staff, facilities and equipment adequate to the lawyer's practice"[5] – suggest that the appropriate use of technology in the circumstances must be considered. If you decide the use of technology is appropriate to provide a legal service or to manage your practice, other rules of professional conduct, such as those governing client confidentiality and marketing by lawyers, will guide your conduct in the use of that technology. The information provided here is intended to help you navigate the intersection between the use of technology and your ethical and professional obligations.

The CBA's Access to Justice Committee recognized in its 2013 Summary Report, *Reaching Equal Justice: An Invitation to Envision and Act*, that "[t]echnology (including information technology) can be harnessed to improve access to justice….[although] [c]areful planning is needed to prevent technological innovations from creating or reinforcing barriers to equal justice."[6] The Report recommended "The Federation of Law Societies, law societies, or the CBA Ethics Committee, [provide] guidance on ethical and professional obligations when using technology to deliver legal services."[7] Similarly, the CBA Legal Futures Initiative noted in its preliminary report that "[a]s more and more transactions are conducted online,

---

1 Elaine CRAIG, "Examining the Websites of Canada's 'Top Sex Crime Lawyers': The Ethical Parameters of Online Commercial Expression by the Criminal Defence Bar", (2014) *UBC Law Review* (forthcoming), available at SSRN.

2 Even the newly adopted Quebec *Code of Professional Conduct of Lawyers*, CQLR c B-1, bears no mention of such an obligation.

3 Notably, in 2012, the commentary to Rule 1.1 in the American Bar Association's *Model Rules of Professional Conduct* was amended to clarify that lawyer competence requires lawyers to keep abreast of benefits and risks associated with the use of relevant technologies.

4 See, for example, FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 3.1-1 (k). Note that the FLSC *Model Code* is referred to throughout. While it has no authority, most law societies have adopted it in whole or in part. Please refer to the specific comparable provisions in your own jurisdiction.

5 See, for example, FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, Commentary to r. 3.2-1.

6 CANADIAN BAR ASSOCIATION – ACCESS TO JUSTICE COMMITTEE, *Reaching Equal Justice: An Invitation to Envision and Act*, 2013, Ottawa, CBA, p. 21.

7 CANADIAN BAR ASSOCIATION – ACCESS TO JUSTICE COMMITTEE, *Reaching Equal Justice: An Invitation to Envision and Act*, 2013, Ottawa, CBA, p. 22.

there may be a need to revisit legal and regulatory systems to ensure that there is a sufficient degree of oversight."[8]

Given the range of ethical questions raised by using technology in a law practice, and the diversity among law practices, we do not claim to offer a comprehensive resource, or to be prescriptive. Our goal is to help you spot potential ethical issues related to the use of technology and to direct you to resources to determine best practices and solutions that are appropriate for your situation. The three main areas covered – security, marketing, and providing services electronically – were identified as areas where lawyers most often face ethical risks in using technology. There are other areas of concern (some of which are addressed in section 4, "Other uses of technology") and new issues will emerge as both the law practice environment and available technologies evolve. Learning how to practice ethically with technology should be approached as an ongoing and dynamic task.

When reviewing the listed resources, remember that your ethical and legal obligations are governed by the code of professional conduct in your jurisdiction. The resources should also be evaluated for their currency – we intend to update this document every few years, but changes in technology will likely outpace us (as may changes to your professional code of conduct, but probably not as fast). If you are uncertain regarding the legal or regulatory applicability of a particular practice or resource, please consult with your law society.

---

8 CANADIAN BAR ASSOCIATION – CBA LEGAL FUTURES INITIATIVE, *The Future of Legal Services in Canada: Trends and Issues*, 2013, Ottawa, CBA, p. 29.

1. Security

- ✓ Are your physical, organizational and technological security measures adequate?
- ✓ Is your computer equipment physically secured using cables or other measures?
- ✓ Are you using firewalls and intrusion detection software appropriately?
- ✓ Are you using anti-malware software appropriately?
- ✓ Are there firm policies in place regarding technology use?
- ✓ Are firm lawyers and staff given adequate technology training?
- ✓ Do you have measures in place to ensure data integrity?
- ✓ Are you meeting your legal and professional obligations when using electronic signatures?
- ✓ Is your data backed-up?
- ✓ Have you assessed your current practices and policies for potential barriers to access and taken steps to remove existing barriers?
- ✓ Are your passwords, other access restrictions and authentication protocols sufficient?
- ✓ Do you use encryption where appropriate?
- ✓ Have you taken adequate steps to safeguard client data when travelling internationally?
- ✓ When discarding equipment, do you take appropriate measures to guard against unauthorized disclosure of client information?
- ✓ Have you taken adequate steps to guard against the inadvertent disclosure of metadata?
- ✓ Is your use of foreign cloud computing resources interfering with client confidentiality?
- ✓ Is there an incident response plan in place in your firm?

Are your physical, organizational and technological security measures adequate?

Like all professionals, lawyers have a legal duty to protect the security of the personal[9] or otherwise confidential[10] data that clients have entrusted to them or that they come to possess through other means. This implies an underlying obligation to adopt physical (locks, cables, laptop tracking software, alarms, etc.[11]), organizational (security policies[12], training[13], etc.) and technological (firewalls[14], intrusion detection

---

9 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1, section 4.7.

10 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 3.3-1. It should also be noted that certain forms of confidential data such as trade secrets can, under certain circumstances, be qualified as property (*Cadbury Schweppes Inc. v. FBI Foods Ltd.*, [1999] 1 SCR 142, par. 47), and that a lawyer must "care for a client's property as a careful and prudent owner would when dealing with like property". See FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 3.5-2.

11 For further discussion of potential physical security measures, see Dan PINNINGTON, "Cybercrimes and Law Firms: The Risks and Dangers are Real" (2013) 12(4) *LawPRO* Magazine 6.

12 A number of model policies are available online, dealing with topics such as appropriate email and internet use, restrictions on downloading and use of portable devices. See, for example: LAW SOCIETY OF BRITISH COLUMBIA, "Sample internet and email use policy"; *LawPRO*, "Model Electronic Document Handling Policy"; *LawPRO*, "Model Portable Device Security, Privacy and Usage Policy" ; *LawPRO*, "Model Technology Usage Policy" ; and John W. SIMEK and Sharon D. NELSON, "Essential Law Firm Technology Policies and Plans" (2012) 38(2) *Law Practice Magazine*.

software (IDS), anti-virus/anti-malware software,[15] among others[16]) security measures to protect that data.[17]

To better appreciate what this general obligation actually entails, it is important to understand what these security measures aim to protect against. As one author puts it: "[t]here are really only six bad things that can happen to data. It can be disclosed, destroyed or modified, either accidentally or intentionally."[18] Guarding against these "bad things" implies that security measures must protect the (a) integrity, (b) availability, and (c) confidentiality of client data and other types of confidential information.[19]

Do you have measures in place to ensure data integrity?

a. Integrity

When discussing integrity within the general framework of information security, we are not referring to a lawyer's "duty to uphold the standards and reputation of the legal profession",[20] but rather to the integrity of documents or data. In this context, integrity implies that data "is the same as that in the source documents and has not

---

13 Training is an important aspect of data security to ensure technical competency and an understanding of related ethical issues. For example, being able to recognize a problem (such as unauthorized access or an infected computer) can be essential to neutralizing or mitigating risks posed by cyber-crime. For tips on how to recognize when a computer has been infected, see, for example, Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10, 16.

14 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. Recent versions of operating systems have built-in firewalls that can be activated to protect computers. For further discussion, see Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10, 17.

15 Malware includes viruses as well as worms, adware, botnets, spyware, rootkits, scareware, ransomware and Trojan horses. Lawyers should run anti-malware software to prevent, detect and remove malware. See, for example: Dave BILINSKY, "Tech security for lawyers" (2012) 1 *Benchers' Bulletin* 9; CYBER AUTHOR, "Five Ways to Avoid a Cyber Attack at Your Law Firm" (2014) *ALPS 411*; Adam CARLSON, "3 Reasons Anti-Virus Software Alone Is No Longer Enough" (2013) *Law Technology Today*; and Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10.

16 This list is taken from Dan PINNINGTON, "Cybercrimes and Law Firms: The Risks and Dangers are Real" (2013) 12(4) *LawPRO Magazine* 6, 9, which also provides definitions of each of these terms.

17 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1, section 4.7.3.

18 Peter S. BROWNE, "Computer security: a survey" (1972) 4-3 *ACM SIGMIS Database* 1.

19 These guidelines aim to highlight the risks associated with data possessed by lawyers. As information security is a complex subject, we strongly recommend you consider consulting with an outside expert about which security measures to adopt to better manage your risk. See Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10, 10: "*LawPRO* encourages firms to seek appropriate help from knowledgeable experts when required".

20 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 2.1-2.

been exposed to accidental or malicious modification, alteration, or destruction".[21] Not only is ensuring data integrity necessary under PIPEDA,[22] it also goes to the very heart of a lawyer's competency as "the obligation to be competent and to render competent services requires that the opinion be based on sufficient information."[23] Obviously, incomplete or corrupted data cannot be construed as sufficient.

Lawyers should adopt security measures to monitor the integrity of the data they collect or hold. This can be done using digital signatures, archival policies, metadata comparison, and ensuring that documents are backed up so that a corrupted file can be replaced by an untouched copy.

Are you meeting your legal and professional obligations when using electronic signatures?

Integrity is also closely linked to authenticity, non-repudiation, and traceability, usually ensured in online communication through the use of electronic signatures. Lawyers should familiarize themselves with this technology, and applicable regulations.[24] For example, the legality of electronic signatures and documents are dealt with in PIPEDA and the *Electronic Commerce Act 2000*.[25] It should be noted that the very definition of an electronic signature varies from one jurisdiction to the next.[26]

Consider implementing standard office practices to limit and clearly indicate who may access your electronic signature, to what documents it may be added, and under what circumstances.[27]

---

21 Harold F. TIPTON and Micki KRAUSE, *Information Security Management Handbook*, 6th ed., Boca Raton, Auerbach, 2007, p. 3043.

22 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1, section 4.7.1.

23 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, Commentary to r. 7.2-7.

24 For further discussion on the use of electronic signatures, see, for example, Marg BRUINEMAN, "Signing on the dotted line easy as 1-2 in the digital world" (2013) *Canadian Lawyer*; David BILINSKY, "E-billing, e-signatures and paperless offices" (2012) 2 *Benchers' Bulletin*; and Catherine SANDERS REACH, "Sign on the Dotted Line" (2014) *Slaw.ca*.

25 LAW SOCIETY OF UPPER CANADA, "Electronic Signatures".

26 For example, in Quebec, typing one's name at the bottom of an electronic document is considered a valid electronic signature in many instances, while other jurisdictions limit electronic signatures to digital signatures, i.e. electronic signatures that use encryption algorithms to ensure a document's authenticity. See *An Act to Establish a Legal Framework for Information Technology*, CQLR c C-1.1, section 39.

27 For example, the Law Society of Upper Canada advises that: "Neither the lawyers' Rules of Professional Conduct (Lawyers' Rules) nor the Paralegal Rules of Conduct (Paralegal Rules) prohibit the use of electronic signatures. If you choose to use an electronic signature you should ensure that security measures have been put in place to prevent unauthorized access, use, or copying. If you provide your electronic signature to an employee you must supervise the employee to ensure its proper use." [Part I of By-Law 7.1 and rule 5.01 of the Lawyers' Rules or subrule 8.01(3) of the Paralegal Rules].

Is your data backed-up?

b. Availability

Data availability can be defined as the "property of being accessible and usable upon demand by an authorized entity"[28]. A recognized part of lawyer competence is "communicating at all relevant stages of a matter in a timely and effective manner";[29] this cannot be done if pertinent data is unavailable because of server maintenance, power failures or other events such as cyber-attacks, water damage or aged hard drives that limit access to computerised files.

For this reason, backing up files is a necessary component of any security policy.[30] The Law Society of Upper Canada's Technology Practice Management Guideline states that "[l]awyers should have back-up and disaster recovery plans for information technologies" and suggests the following policies and procedures:

- regular back-up of data;
- back-up disks or tapes in a secure off-site location;
- routine checks to ensure data can be restored; and
- insurance to cover the costs of recovering lost hardware or electronic information.[31]

This is especially important if information is stored on servers belonging to a third party – be it through a basic hosting contract or a cloud computing infrastructure – due to the increased risk that data may be temporarily unavailable due to connection problems or the service provider's decision to limit access because of a late payment or other contractual disputes.

Have you assessed your current practices and policies for potential barriers to access and taken steps to remove existing barriers?

That being said, your obligation to ensure the availability of data encompasses more than timely access to computerised files. These files must also be intelligible for the individual that requires access. This entails having access to the software necessary to read a given file (an older version of word processing software such as Word Perfect, for example), but might also involve ensuring that the electronic documents are accessible to persons with disabilities[32], whether firm members, clients or potential recruits."[33]

---

28 Harold F. TIPTON and Micki KRAUSE, *Information Security Management Handbook*, 6th ed., Boca Raton, Auerbach, 2007, p. 3020.

29 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 3.1-1.

30 See, for example: LAWPRO, "Backup Best Practices and Strategies"; and AMERICAN BAR ASSOCIATION, "FYI: Data Backup". See also BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team".

31 LAW SOCIETY OF UPPER CANADA, "Technology Practice Management Guideline".

32 For example on how to achieve this, see ACCESS ONTARIO, "Making information accessible to people with disabilities"; and GLOBAL ALLIANCE FOR ACCESSIBLE TECHNOLOGIES AND ENVIRONMENTS (GAATES), *Accessible Information and Communication: A Guide for Small Business*, Toronto, GAATES, 2013.

As noted in the Web Content Accessibility Guidelines (WCAG) 2.0 issued by the World Wide Web Consortium (W3C)[34], websites and web content can pose particular access challenges to persons with disabilities. Other accessibility issues pertain to formatting documents using styles that can impede accessibility for individuals using assistive devices like screen readers.[35]

Accessibility standards – specifically as they pertain to electronic documents – differ from one province to the next.[36] You should be aware of the applicable standards and assess your compliance.

Are your passwords, other access restrictions and authentication protocols sufficient?

c. Confidentiality

Lawyers are required to "hold in strict confidence all information concerning the business and affairs of a client acquired in the course of the professional relationship and must not divulge any such information."[37] Although Canadian rules of professional conduct do not specify measures lawyers should take to safeguard the confidentiality of client information when using technology[38], laws such as PIPEDA provide guidance regarding the types of security measures lawyers and others should

---

33 Codes of professional conduct acknowledge that lawyers have "a special responsibility to respect the requirements of human rights laws in force in Canada, its provinces and territories and, specifically, to honour the obligations enumerated in human rights laws." See FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, Commentary to r. 6.3.

34 WORLD WIDE WEB CONSORTIUM (W3C), "Getting Started with Web Accessibility".

35 The Accessible Digital Office Document (ADOD) Project offers tools that can assist in creating accessible office documents. See: Accessible Digital Office Document (ADOD) Project.

36 For example, accessibility standards applying to law firms are set under the *Accessibility for Ontarians with Disabilities Act, 2005*, SO 2005, c 11 (for further discussion of these obligations, see ONTARIO MINISTRY OF ECONOMIC DEVELOPMENT, EMPLOYMENT & INFRASTRUCTURE, "Making Ontario Accessible"; ACCESS ONTARIO, "A Guide to the Integrated Accessibility Standards Regulation" (2014); LAW SOCIETY OF UPPER CANADA, "AODA Integrated Standards - Legal Obligations for Law Firms of Fewer than 50 Employees"; and LAW SOCIETY OF UPPER CANADA, "AODA Integrated Standards - Legal Obligations for Law Firms of 50 or more Employees") and the *Accessibility for Manitobans Act*, CCSM c A1.7 (for further discussion of these obligations, see GOVERNMENT OF MANITOBA, "Manitoba Disabilities Issues Office"). Regarding the general accessibility to electronic documents, Quebec law states that: "The wishes of the person having the right of access as to the medium or technology to be used must be taken into account, unless substantial practical difficulties would be involved, owing in particular to high cost or the information transfer required". See *An Act to Establish a Legal Framework for Information Technology*, CQLR c C-1.1, section 23.

37 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 3.3-1.

38 While not authoritative, the American Bar Association's *Model Rules of Professional Conduct* rule 1.6(c) and commentary may be helpful for factors to consider in determining the reasonableness of efforts to prevent inadvertent or unauthorized disclosure of client information, including: the sensitivity of the information; the likelihood of disclosure if additional safeguards are not employed; the cost of employing additional safeguards; the difficulty of implementing the safeguards; and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use.)

consider implementing – physical measures such as locked filing cabinets and restricted access to offices, organizational measures such as security clearances and limiting access on a "need-to-know" basis, and technological measures such as the use of passwords[39] and encryption.[40] Be aware of provincial and federal laws, such as privacy legislation, that impact how you handle information.[41]

Have you taken adequate steps to safeguard client data when travelling internationally?

Security measures should be put in place to guard against third party access to confidential data during its life cycle (i.e., the timespan between the data's creation and destruction). This implies that information should be protected from its creation to its destruction, and through every intermediary phase. For example, if confidential data is carried out of the office, encryption mechanisms should be adopted to secure it during transport.[42] In fact, when possible, it is safer to access information through a

---

39 Effective measures include using strong passwords and two-factor or multi-factor authentication. The use of two-factor or multi-factor authentication is increasingly recommended. This measure "bolsters security by pairing something you know – your password – with something you have". See: Sam GLOVER, "Passwords: a User Guide for Lawyers and Law Firms (2014) *Lawyerist*. Lawyers should also take care to ensure that passwords, once created, remain secure. For more on passwords and password protection, see: David J. BILINSKY, "Secure Passwords" (2013) *thoughtfullaw.com*; David WHELAN, "Your Passwords S****" (2014) *Slaw.ca*; Dan PINNINGTON, "Keeping Your Passwords Strong and Secure" (2013) 12(4) *LawPRO Magazine* 30; LAWYERS' INSURANCE ASSOCIATION OF NOVA SCOTIA, "Data Security"; and BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team".

40 It is recommended by some that lawyers use "full disk encryption on your work computer and any device that has client confidential or private information on it." See David WHELAN, "Getting Started with Law Office Technology" (no longer available online). See also: Dave BILINSKY, "Tech security for lawyers" (2012) 1 *Benchers' Bulletin* 9; BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team" ; and Seth SCHOEN, "New Year's Resolution: Full Disk Encryption on Every Computer You Own" (2011). When using wireless networks within a legal practice, it is recommended that lawyers "use WPA or WPA2 (WPA2 is better) or 802.1x wireless encryption" and also "WEP encryption is found on older devices and it is recommended that you not use it as it can easily be cracked". Finally, lawyers should protect their wireless networks by taking the following additional steps: turn off SSID broadcasting; disable guest networks; turn on MAC filtering; change default router name and password; and disable remote administration. See Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10.

41 See, for example, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *PIPEDA and Your Practice — A Privacy Handbook for Lawyers*, Ottawa, OPCC, 2011 (discussing, among other things: application and requirements of PIPEDA; privacy issues in managing a law practice; and privacy issues in civil litigation). Special obligations may also arise under provincial legislation when dealing with medical records. See Nina BOMBIER and Paul-Erik VEEL, "When Medical Records Go Missing", (2014) *Lawyers Weekly* 15 (regarding Ontario's *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A).

42 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *PIPEDA and Your Practice — A Privacy Handbook for Lawyers*, Ottawa, OPCC, 2011, p. 11. See also: BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team".

secure VPN connection[43] than to carry files on a laptop hard drive or USB key. This is especially true when traveling internationally since, when crossing borders, the electronic devices in your possession may be subject to search by border officials.[44] When out of the office, be mindful of using wireless networks since they are often unsecured and can expose a client's personal data to third parties.[45]

When discarding equipment, do you take appropriate measures to guard against unauthorized disclosure of client information?

Once client data is no longer needed, it should be properly deleted.[46] Using the standard "delete" function available on a computer, tablet or smartphone is insufficient to prevent third parties from subsequently recovering a file. Although the most secure option is to physically destroy the medium that stores the confidential data, "wiping," "scrubbing" or "shredding" are also relatively secure forms of deletion.[47] A number of file wiping software programs can be used for this purpose. When deleting data, don't overlook hard drives in copiers and printers that store images of documents.[48]

Have you taken adequate steps to guard against the inadvertent disclosure of metadata?

When communicating with opposing counsel electronically, ensure that documents sent via email do not contain metadata with confidential information.[49] Metadata is information about other data. Many computer programs embed information into the program output when it is created, opened and saved. Although hidden on normal viewing, metadata can be revealed and accessed by others when a document is circulated electronically. The information in metadata may include: the document author's name; the date the document was created; document revisions, including insertions and deletions, tracked changes and comments added by reviewers; and the

---

43 A VPN or virtual private network can allow lawyers to connect to their firm's network through the internet in a secure manner.

44 Luigi BENETTON "How to secure your laptop before crossing the border" (2009) *CBA PracticeLink*. See, also, LAW SOCIETY OF UPPER CANADA, "Technology Practice Tips: Clean Devices (Transcript)"; and Seth SCHOEN, Marcia HOFMANN and Rowan REYNOLDS, "Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices" Electronic Frontier Foundation, 2011.

45 Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10.

46 BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team".

47 To learn more about the secure deletion of electronic files and equipment, see, for example: LAW SOCIETY OF BRITISH COLUMBIA, "Closed Files – Retention and Disposition" (2015); Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10; and Sharon D. NELSON and John W. SIMEK, "Technology and the Sale of a Law Practice" (2012) 29(4) *GP Solo*.

48 For further discussion of this risk, see, for example: Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10.

49 BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team".

location of the stored file.[50] Therefore, except in cases where a lawyer is legally required to communicate metadata (e.g. discovery obligations), steps should be taken to minimize the creation of metadata or to wipe it from sent files.[51]

Is your use of foreign cloud computing resources interfering with client confidentiality?

Confidentiality is also a concern when information is housed on servers that reside outside of Canada since certain foreign governments have adopted legislation allowing them access to such information.[52] The Law Society of British Columbia has adopted strict rules regarding the use of cloud computing or other third-party based hosting services when the servers are situated outside of the country.[53] Even servers situated in Canada will fall under foreign jurisdiction if they are the property of foreign interests. In the same vein, information sent through the internet that temporarily travels outside the country (referred to as "boomerang routing") can be subject to foreign laws. For these reasons, unless otherwise instructed by the client, confidential information sent to a server (or a third party) using the internet should be encrypted. [54]

Is there an incident response plan in place in your firm?

Notwithstanding all the security measures that are put into place, there will always be a risk that a clients' data could be disclosed, destroyed or modified. For this reason it remains important for any law firm to develop an incident response plan. A number of commentators have stressed the importance of having such a plan to deal with security breaches if and when they occur[55].

---

50 For a lengthier, more complete list of what information may be contained in metadata, see Dan PINNINGTON, "Beware the Dangers of Metadata" (2004) *LawPRO Magazine* 36.

51 See, for example: "Remove hidden data and personal information from Office documents"; "Remove hidden data and personal information by inspecting documents"; "Removing sensitive content"; Dan PINNINGTON, "Beware the Dangers of Metadata" (2004) *LawPRO Magazine* 36; David Bilinsky, "Beware of Tracked Changes in Word" (2010), *Slaw.ca*; Donna PAYNE, "Metadata: The Good, the Bad, and the Misunderstood", (2013) 30(2) *GPSOLO*; District of New Jersey, "Guidelines for Editing Metadata".

52 The risk is significant: "[s]ince you are placing yours – and your client's data – in the hands of third parties, it also raises issues of security and privacy, regulatory compliance and risk management, amongst others." LAW SOCIETY OF BRITISH COLUMBIA, "Cloud Computing Checklist" (2013). This risk may be greater if the provider is located outside Canada, in a jurisdiction with different rules with respect to privilege and confidentiality of records. CANADIAN BAR ASSOCIATION, "FAQs about Privilege and Confidentiality for In-House Counsel" (2012).

53 See Dave BILINSKY, "Frequently Asked Questions (And Answers) on BC Lawyers' Use of Cloud Computing" (2014) *Slaw.ca*.

54 For more information on this issue, see David FRASER, "Cloud computing: A Privacy FAQ" (2014) *National Magazine*; LAW SOCIETY OF BRITISH COLUMBIA, "Cloud Computing Checklist" (2013); LAW SOCIETY OF BRITISH COLUMBIA, "Cloud Computing Due Diligence Guidelines" (2012); Dan PINNINGTON "Protecting Yourself from Cybercrime Dangers: The Steps You Need to Take" (2013) 12(4) *LawPRO Magazine* 10 ; and David WHELAN, "Step by Step Cloud Computing For Lawyers" (2013).

55 See, for example: CYBER AUTHOR, "Five Ways to Avoid a Cyber Attack at Your Law Firm" (2014) *ALPS 411*; Nora ROCK, "Be Ready with an Incident Response Plan" (2013) 12(4) *LawPRO Magazine* 28; and Pablo FUCHS, "On Guard" (2013) *National*.

2. Marketing

- ✓ Does your online presence comply with ethical rules regarding marketing?
- ✓ Does your use of electronic communications for marketing purposes comply with anti-spam legislation?
- ✓ Are you aware of the diverse ethical risks related to marketing through social media?
- ✓ Does your use of social media put you at risk of inadvertent disclosure of confidential information?
- ✓ Do you have a social media policy?

Does your online presence comply with ethical rules regarding marketing?

Lawyers are governed by ethical rules when engaged in marketing activities. For example, Rule 4.2-1 to the Federation's *Model Code* provides that "A lawyer may market professional services, provided that the marketing is: (a) demonstrably true, accurate and verifiable; (b) neither misleading, confusing or deceptive, nor likely to mislead, confuse or deceive; (c) in the best interests of the public and consistent with a high standard of professionalism."[56] It goes without saying that these ethical standards apply to marketing whether you use a print format or electronic formats such as websites, email, or social media (like Facebook, LinkedIn and Twitter).

Law firm websites, because they serve as the primary online window for most firms, have noticeably come under scrutiny for not respecting ethical rules. One study points out that "[c]ontent on […] lawyer websites that is arguably inconsistent with these rules includes material that could be perceived to promote the acquittal of clients that appear to be factually guilty, marketing that includes characterizations of one's representation as aggressive, material that appears to trivialize sexual violence, advertisements that promote the use of particular types of defence strategies at trial, and webpage content with misstatements of the law or misleading and confusing legal information."[57]

Aside from being a very valuable marketing tool, law firm websites can also serve as a public service to help promote access to justice. After all, "[a]ccess to justice requires that the public have available understandable information about the justice system, its resources, and means of access."[58] Law firm websites have the potential to help individuals "access justice by developing and disseminating information and materials as broadly as possible in forms and by means that can reach the largest possible number and variety of people."[59] In this sense, "the website law blog is the

---

56 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of professional Conduct*, r. 4.2-1.

57 Elaine CRAIG, "Examining the Websites of Canada's 'Top Sex Crime Lawyers': The Ethical Parameters of Online Commercial Expression by the Criminal Defence Bar", (2014) *UBC Law Review* (forthcoming), available at SSRN.

58 WASHINGTON STATE SUPREME COURT, "Washington State Access to Justice Technology Principles", (2004).

59 WASHINGTON STATE SUPREME COURT, "Washington State Access to Justice Technology Principles", (2004).

modern incarnation of a lawyer's public service."[60] For your website to truly be useful both as a marketing tool and as a tool to facilitate access to justice, make sure that its content is easy to understand for potential clients. As one expert suggests:

- use plain English and simple sentences
- be concise with points, titles, sentences and paragraphs
- use hyperlinks to help readers navigate quickly to useful information
- make sure people and contact details are instantly accessible
- projecting professionalism is good, but too much legal jargon is not[61]

That being said, giving out free legal information on a website is risky for numerous reasons. First, it can be misconstrued as legal advice[62]. Second, if, for example, a lawyer posts an analysis of a recent decision that is later overturned, the information, when consulted months or years later, could steer the reader in the wrong direction.[63] Finally, as discussed further in the next section, a reader from another jurisdiction might access and rely on the information resulting in accusations of the unauthorized practice of law in jurisdictions where you are not licensed.[64] Such accusations could also stem from making available automated tools that help individuals draft their own legal documents.[65]

Although these tools and free legal information help promote access to justice, administrators of the some sites have been found guilty of unauthorized practice of law.[66] All law firm websites should include an appropriate disclaimer in the terms of use or elsewhere on the site.[67]

---

60 William R. PETERSON, and Clark E. SMITH, "Law Firm Websites: An Ethical Minefield", (2013) *The Bencher*.

61 SPHERE UP, "5 Tips That Can Help Your Law Firm Website Attract Clients", (2013).

62 William R. PETERSON, and Clark E. SMITH, "Law Firm Websites: An Ethical Minefield", (2013) *The Bencher*; James E. CABRAL *et al.*, "Using Technology to Enhance Access to Justice", (2012) 26(1) *Harvard Journal of Law & Technology*, 241, 317.

63 William R. PETERSON, and Clark E. SMITH, "Law Firm Websites: An Ethical Minefield", (2013) *The Bencher*.

64 William R. PETERSON, and Clark E. SMITH, "Law Firm Websites: An Ethical Minefield", (2013) *The Bencher*; James E. CABRAL *et al.*, "Using Technology to Enhance Access to Justice", (2012) 26(1) *Harvard Journal of Law & Technology*, 241, 317.

65 James E. CABRAL *et al.*, "Using Technology to Enhance Access to Justice", (2012) 26(1) *Harvard Journal of Law & Technology*, 241, 317.

66 James E. CABRAL *et al.*, "Using Technology to Enhance Access to Justice", (2012) 26(1) *Harvard Journal of Law & Technology*, 241, 319.

67 For a template, see CANADIAN BAR ASSOCIATION, "Model Law Firm Website Terms of Use and Disclaimer", (2008).

Does your use of electronic communications for marketing purposes comply with anti-spam legislation?

If you choose to use email or social media for marketing purposes, be familiar with the requirements of Canada's Anti-Spam legislation and regulations, which are applicable to lawyers and govern unsolicited commercial electronic communications (or "spam").[68]

Are you aware of the diverse ethical risks related to marketing through social media?

As the Law Society of Upper Canada has observed, "social media can provide helpful marketing tools – but lawyers must play by the rules."[69] The term "social media" can refer to a wide array of technologies[70], each of which presents its own risks when used for marketing purposes. Take the time to understand the differences between these technologies and their associated risks[71], and guard against the tendency to relax standards when marketing within these more informal environments (compared to official law firm websites), which may lead to prohibited conduct.[72]

---

68 SC 2010, c 23. For further discussion on this topic, see Ava CHISLING, "What's it all about? How anti-spam legislation can affect your firm" *CBA PracticeLink*. The Governement of Canada and the CRTC both have websites that allow organizations to test whether their email marketing policies conform with the Act. See: Canada's Anti-Spam Legislation and Canadian Radio-television and Telecommunications Commission.

69 LAW SOCIETY OF UPPER CANADA, "Social media can provide helpful marketing tools – but lawyers must play by the rules" (2010) *Ontario Lawyers Gazette* 10.

70 Phil BROWN and David WHELAN, "The Ethics of Social Media for Lawyers" (2012). For example, the LAW SOCIETY OF ENGLAND AND WALES ("Social Media" (December 20 2011)) lists eight different types of social media tools: (1) forums and comment spaces on information-based websites; (2) social networking websites such as Facebook and LinkedIn; (3) video and photo sharing websites such as Flickr and YouTube; (4) weblogs, including corporate and personal blogs; (5) micro-blogging sites such as Twitter; (6) forums and discussion boards such as Yahoo! Groups or Google Groups; (7) online wikis that allow collaborative information sharing such as Wikipedia; and (8) any other websites that allow individual users or companies to use simple publishing tools.

71 There are a number of helpful resources available online that explain how different forms of social media work and what ethical risks might arise with each. See, for example: Phil BROWN and David WHELAN, "The Ethics of Social Media for Lawyers" (2012); MERITAS, "Social Media Guide for Lawyers" (2011); Dan PINNINGTON, "Social Media: How? - A primer on using social media in a law firm" (2009) 8(4) *LawPRO Magazine* 12; Ernie SVENSON, *Blogging in One Hour for Lawyers*, Chicago, American Bar Association, 2013; Dennis KENNEDY and Allison C. SHIELDS, *Facebook in One Hour for Lawyers*, Chicago, American Bar Association, 2012; Ruth CARTER, *The Legal Side of Blogging for Lawyers*, Chicago, American Bar Association, 2014; Dennis KENNEDY and Allison C. SHIELDS, *LinkedIn in One Hour for Lawyers*, 2nd Edition, Chicago, American Bar Association, 2013; and Jared CORREIA, *Twitter in One Hour for Lawyers*, Chicago, American Bar Association, 2012.

72 Types of prohibited conduct include: stating an amount of money that the lawyer has recovered for a client or referring to the lawyer's degree of success in past cases, unless such statement is accompanied by a further statement that past results are not necessarily indicative of future results and that the amount recovered and other litigation outcomes will vary according to the facts in individual cases; suggesting qualitative superiority to other lawyers; raising expectations unjustifiably; suggesting or implying the lawyer is aggressive; disparaging or demeaning other persons, groups, organizations or institutions; taking advantage of a vulnerable person or group; and using testimonials or endorsements that contain emotional appeals. See FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, Commentary to r. 4.2-1.

Does your use of social media put you at risk of inadvertent disclosure of confidential information?

One risk when using social media is the inadvertent disclosure of confidential information.[73] For example, creating networks through social media sites (by "friending" or "following") risks disclosing that a client has retained a particular lawyer. Also some social media services have the capability of publicizing the location of users (displaying when a lawyer is in the same city or in the same block as the client's place of business).[74]

Do you have a social media policy?

For these and other reasons, law firms should adopt a social media policy.[75] Such a policy can help to ensure that firm members are aware of standards and protocols for the use of social media and to avoid damage to the firm's reputation from the inappropriate use of social media.[76]

---

73 There are a number of resources that offer tips for protecting confidentiality when using social media. See, for example: Dan PINNINGTON, "The Dangers of Social Networking and How to Avoid Them" (2014) 2 *LawPRO Magazine Student Issue* 18; David WHELAN, "The Practical and Ethical Use of Social Media" (2012); MERITAS, "Social Media Guide for Lawyers" (2011).

74 These two examples are discussed in David WHELAN, "The Practical and Ethical Use of Social Media" (2012).

75 Doug CORNELIUS, "Top Ten Mistakes Lawyers Make with Social Media" (2009) *CBA PracticeLink*.

76 These benefits are derived from LAW SOCIETY OF ENGLAND AND WALES, "Social Media" (2011). For more on the components of an effective social media policy, see, for example: LAW SOCIETY OF BRITISH COLUMBIA, "Model Policy – Social Media and Social Networking"; LAWYERS' INSURANCE ASSOCIATION OF NOVA SCOTIA, "Social Media in the Workplace"; and MERITAS, "Social Media Guide for Lawyers" (2011).

3. Providing services electronically

- ✓ Are you careful not to inadvertently form lawyer-client relationships when communicating online?
- ✓ Do you ensure that "know your client" requirements are met when communicating solely online?
- ✓ Do you take steps to avoid the conflict of interest risks that can arise from your online presence?
- ✓ Do you ensure that your clients can correctly identify you in online communications?
- ✓ Do you take steps to avoid the unauthorized practice of law in another jurisdiction?
- ✓ Do you ensure that your clients are informed of , and accept, the risks associated with communicating by email?
- ✓ Do you ensure that your clients are informed of, and accept, the risks associated with videoconferencing tools?
- ✓ Do you comply with your supervision obligations online?
- ✓ Do you ensure that "human help" is available for clients and potential clients without the means or ability to take advantage of technological options?

Providing legal services electronically (i.e. using email, social media, videoconferencing solutions or other telecommunication services to interact with potential or current clients) expands client development opportunities and has the potential to improve access to legal services by those underserved by the legal profession.

It also raises numerous compliance risks related to previously addressed issues such as confidentiality, as well as additional risks such as forming unintended client-lawyer relationships; inadvertent conflicts of interest and unauthorized practice of law;[77] inadequate client identification and verification, and inadequate supervision; and the potential negative impact on access to legal services for clients and potential clients without the means or ability to take advantage of technological options.

Are you careful not to inadvertently form lawyer-client relationships when communicating?

Providing legal information online can be a useful marketing strategy. However, when doing so, you need to ensure that you don't inadvertently establish a lawyer-client relationship. Remember that a lawyer-client relationship can be formed without a formalized written agreement; the Federation of Law Societies of Canada's *Model Code*, for example, simply defines a "client" as "a person who, having consulted the lawyer, reasonably concludes that the lawyer has agreed to render legal services on his or her behalf."[78]

---

77 For further discussion of these risks and others, see Dan PINNINGTON, "The Dangers of Social Networking and How to Avoid Them" (2014) 2 *LawPRO Magazine Student Issue* 18.

78 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 1.1-1.

Online communications such as web postings or tweets can be misconstrued as a consultation and create, in the mind of the "client", a lawyer-client relationship.[79] These types of situations were highlighted in a recent ABA publication: "The interactive nature of social media (e.g., inviting and responding to comments to a blog post, engaging in Twitter conversations, or responding to legal questions posted by users on a message board or a law firm's Facebook page) creates a real risk of inadvertently forming attorney-client relationships with non-lawyers, especially when the objective purpose of the communication from the consumer's perspective is to consult with the lawyer about the possibility of forming a lawyer-client relationship regarding a specific matter or legal need."[80]

Measures you can take to avoid this situation include the use of a disclaimer when posting information online (discussed also in the previous section), and keeping a record of online communications to defend against a claim that legal advice was given.[81]

Do you ensure that "know your client" requirements are met when communicating solely online?

Communicating with your client electronically, through email or other means, can cut costs and avoid delay, facilitating access to justice. Unfortunately, practices such as email spoofing[82], phishing[83] and spear phishing[84] can lead lawyers to share confidential information with a malicious third party posing as a client, making it necessary, in certain cases, to adopt strong identification methods (i.e. digital signatures) that go beyond simply relying on the address indicated in the "from" window of the sender's email. When providing services online, be sure you are familiar with, and comply with, the client identification and verification rules in your

---

79 William R. PETERSON, and Clark E. SMITH, "Law Firm Websites: An Ethical Minefield", (2013) *The Bencher*.

80 Christina VASSILIOU HARVEY, Mac R. MCCOY, and Brook SNEATH, "10 Tips for Avoiding Ethical Lapses When Using Social Media" (2014) *Business Law Today*.

81 These measures are discussed in Dan PINNINGTON, "The Dangers of Social Networking and How to Avoid Them" (2014) 2 *LawPRO Magazine Student Issue* 18.

82 "Spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Spoofing is often used by spammers and can be accomplished by changing your "FROM" e-mail address." See NEWS EDITOR, "The Big Three Email Nuisances: Spam, Phishing and Spoofing" (2014) *Lavasoft*.

83 "Phishing is a special type of spam that is intended to trick you into entering your personal or account information for the purpose of breaching your account and committing identity theft or fraud." See NEWS EDITOR, "The Big Three Email Nuisances: Spam, Phishing and Spoofing" (2014) *Lavasoft*.

84 "Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc. The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive." See FBI, "Spear Phishers Angling to Steal Your Financial Info" (2009) *FBI.gov*.

jurisdiction. In particular, follow applicable procedures for verifying client identity when not receiving instructions face-to-face.[85]

Do you take steps to avoid the conflict of interest risks that can arise from your online presence?

The somewhat informal nature of electronic communications, combined with the fact that many people operate online under a false name, presents a risk of inadvertently finding yourself in a conflict of interest when offering services online. To mitigate this risk, take reasonable steps to determine the actual identity of the people you are dealing with and, as mentioned, be very careful about the information you share online.[86]

Do you ensure that your clients can correctly identify you in online communications?

In addition to taking all reasonable steps to identify a client, you should also ensure that you are properly identified in your own electronic communications[87]. For example, section 5.8.2 of LSUC's *Technology Practice Management Guideline*[88] provides: "Lawyers making representations in generally accessible electronic media should include the name, law firm mailing address, licensed jurisdiction of practice, and email address of at least one lawyer responsible for the communication."[89]

Providing this information also alleviates the risk of being accused of practicing law in another jurisdiction.

---

85 For a general discussion, see Bob TARANTINO, "Pleased to Meet You: The New 'Know Your Client' Regime" (2009) *CBA PracticeLink*. For examples of specific provincial and territorial procedures, see, for example, Client Identification and Verification – Frequently Asked Questions (British Columbia); Client Identification and Verification Flowchart (Alberta); Client Identification and Verification – Frequently Asked Questions (Saskatchewan); Client Identification and Verification – Frequently Asked Questions (Manitoba); By-Law 7.1, s. 23(8) (Ontario); Nouvelles exigences en matière d'identification et de vérification de l'identité des clients (Québec); and Some Questions and Answers about the new Client Identification and Verification Regulations (Nova Scotia).

86 Dan PINNINGTON, "The Dangers of Social Networking and How to Avoid Them" (2014) 2 *LawPRO Magazine Student Issue* 18.

87 Dan PINNINGTON, "The Dangers of Social Networking and How to Avoid Them" (2014) 2 *LawPRO Magazine Student Issue* 18.

88 LAW SOCIETY OF UPPER CANADA, "Technology Practice Management Guidelines".

89 LAW SOCIETY OF UPPER CANADA, "Technology Practice Management Guidelines".

Do you take steps to avoid the unauthorized practice of law in another jurisdiction?

Because the internet provides easy reach across jurisdictions, and the potential for inadvertently establishing a lawyer-client relationship, providing online legal services may lead to the unauthorized practice of law.[90]

One way of protecting against this risk is to advise clients (or potential clients) of the jurisdictions where you are authorized to practice law. For example, the "Rules and Guidance" of the Law Society of Scotland suggest that: "If the solicitor is based at an office in another EU state, the client must be told that the service is provided by a Scottish solicitor, registered with (for example) the Athens Bar, and how to access the rules of that Bar. It is recommended that all e-mails providing electronic services (as opposed to merely communicating by email) include this information or a link to it."[91] With a few obvious adaptations, Canadian lawyers should consider following this advice.

Do you ensure that your clients are informed of, and accept, the risks associated with communicating by email?

Although they are often greatly exaggerated, there are numerous risks associated with online communications with clients, especially email communications. An email to a client might never reach its destination, be intercepted by a third party, or be mistakenly blocked by the client's spam filter.

For these reasons, it should be agreed upon with a client beforehand that email will be used.[92] Clients should also be made aware that the providers of free webmail services, [93] or employers if a work email is used,[94] are often contractually permitted to access their private conversations. The use of encryption software, although not mandatory[95], may be warranted for particularly sensitive communications.[96]

---

90 For further discussion, see Dan PINNINGTON, "The Dangers of Social Networking and How to Avoid Them" (2014) 2 *LawPRO Magazine Student Issue* 18; LAW SOCIETY OF UPPER CANADA, "Technology Practice Management Guidelines"; and William R. PETERSON, and Clark E. SMITH, "Law Firm Websites: An Ethical Minefield", (2013) *The Bencher*.

91 Division B: Electronic Communications, section 4.4.

92 BARREAU DU QUÉBEC, "IT Guide - Technology management and security for the lawyer and his team".

93 See, for example, the Google Terms of Service as applicable to Gmail.

94 Daniel LUBLIN, "Employee Email and the Attorney-Client Privilege" (2007).

95 LAW SOCIETY OF UPPER CANADA, "Five Questions about Encryption".

96 LAW SOCIETY OF UPPER CANADA, "Technology Practice Management Guidelines". For more on the subject, see, for example: David J. BILINSKY, "Protect Your Data (from Snoops and others…)" (2013) *SlawTips*; Catherine SANDERS REACH, "Easy Encryption for Email – Not an Oxymoron" (2013) *Slaw.ca*; and John W. SIMEK & David G. RIES, "101: Encryption Made Simple for Lawyers" (2013) *Wisconsin Lawyer*.

It should also be explained to clients that copying others on an email can be interpreted as a waiver of privilege.[97] And be cautious when replying to emails yourself – lawyers have been reprimanded for sending an email to the wrong address, or for clicking on "reply all" rather than "reply" in connection with a confidential discussion.[98]

Do you ensure that your clients are informed of, and accept, the risks associated with videoconferencing tools?

As with email, telecommunication services such as Skype usually insert clauses in their user agreements that allow them to access the content of your conversations, making the use of such tools contrary to a lawyer's confidentiality obligations. Clients can relieve their lawyers of those obligations, but only if they are aware of, and accept, the risks.

In the same vein, certain teleconferencing tools allow for the recording of conversations. Rule 7.2-3 of the Federation of Law Societies of Canada's *Model Code* provides: "A lawyer must not use any device to record a conversation between the lawyer and a client or another lawyer, even if lawful, without first informing the other person of the intention to do so."[99] Determine whether there is a chance the teleconference will be recorded and if so (and subject to the rules in your jurisdiction), ensure that your client is aware of that possibility and has agreed to the use of the tool.

Do you comply with your supervision obligations online?

Although, when offering services electronically, it might be tempting to delegate certain online tasks to more tech-savvy members of your firm's staff, keep in mind your ethical obligation regarding supervision of these employees. Rule 6.1-1 of the Federation's *Model Code* provides: "A lawyer has complete professional responsibility for all business entrusted to him or her and must directly supervise staff and assistants to whom the lawyer delegates particular tasks and functions."[100] Further, some tasks simply cannot be delegated. For example, real estate lawyers are prohibited from allowing others to access land registry systems using the lawyer's registration credentials.[101]

---

97 Although this situation has seldom been addressed by Canadian courts, American case law has established rules regarding when cc'ing a third party to an email will affect privilege. See Jane T. DAVIS and Matthew E. BROWN, "United States: Protecting The Attorney-Client Privilege In The Digital Age" (2012) *Mondaq*.

98 For example, a Quebec lawyer was found to have acted unethically for copying all of her clients' email addresses in the "to" window of an email announcing that she was moving her practice, therefore letting every client learn the identity and address of all other clients. See *Smith* v. *Teixeira*, 2009 QCCQ 3402.

99 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 7.2-3.

100 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 6.1-1.

101 For further discussion, see, for example: Kathleen WATERS, "Want trouble? Let someone access the land registry system using your credentials" (2014) *Avoid-a-Claim*.

Do you ensure that "human help" is available for clients and potential clients without the means or ability to take advantage of technological options?

While providing services electronically has the potential to improve access to legal services, it may inadvertently restrict access for those clients or potential clients without the means or ability to take advantage of technological options or with insufficient literacy skills to comprehend the online information[102]. Ensure that "human help" is available as an alternative or, if offering electronic services exclusively, ensure that you can readily refer a potential client to a legal service provider that offers human help.

---

[102] 42% of Canadian adults between the ages of 16 and 65 have low literacy skills. CANADIAN LITERACY AND LEARNING NETWORK, "Literacy Statistics in Canada…", (2005).

4. Other uses of technology

- ✓ Are you discerning when you use online research tools?
- ✓ Are you discerning in your choice of online references?
- ✓ Do you adhere to courtesy and civility rules when communicating with the court or opposing counsel electronically?
- ✓ Does your use of technology respect courtroom rules and decorum?
- ✓ Are you in compliance with your ethical obligations when operating a paperless office?

Security, marketing, and interacting with clients (providing services electronically) do not constitute the only areas of a legal practice where technology can present new ethical dilemmas. Here is a sample of other situations in which use of technology can impact your ethical obligations.

Are you discerning when you use online research tools?

a. Legal research

Online legal research tools such as CanLII, Westlaw, or Quicklaw allow lawyers to access and search through more case law and legal doctrine than was possible mere decades ago. Although this may allow you to be more prepared for trial (for example), avoid overkill. Where a point of law could be argued using just one or two references on point, resist the urge to offer dozens of additional supporting cases.

The abundance of choice available through online legal research tools means lawyers must be more discerning when choosing which cases to plead, to avoid wasting the the court's time or their clients' money. Remember that while pleading a mountain of decisions can be construed as thorough, it can also be seen as an affront to the proportionality principle which, the Supreme Court of Canada has stated, "can act as a touchstone for access to civil justice."[103]

Are you discerning in your choice of online references?

As for other online documents, it should be remembered that "[translation] the ease with which one can upload a text imposes great prudence on the reader's part, especially when this information is to be used as evidence in front of a court."[104] Unsubstantiated or unreliable sources should not be used, while online references such as Wikipedia that can easily be modified by interested parties should be used sparingly, and only when the entries are shown to be well documented and reliable.

---

103 *Hryniak* v. *Mauldin*, [2014] 1 SCR 87, par. 30 and 31.

104 *Bélec* and *Groupe Domotec inc.*, [2004] AZ-50253111 (CLP), par. 53.

Do you adhere to courtesy and civility rules when communicating with opposing counsel electronically?

b. Communicating with opposing counsel

The speed and ease of online communications sometimes make it easy to forget that rules of common courtesy still apply. Rule 7.2-1 of the Federation of Law Societies of Canada's *Model Code* provides: "A lawyer must be courteous and civil and act in good faith with all persons with whom the lawyer has dealings in the course of his or her practice."[105] Take the same care in drafting emails as you would with any other letter. When possible, wait a few hours before sending an email to allow time for reflection.

In addition to basic courtesy, online courtesy, also known as "netiquette", includes specific rules when sending electronic communications. For example, lawyers should avoid "using the 'urgent' flag unless [their] message is both important and time-critical", and avoid typing in all caps as it is considered equivalent to shouting.[106]

Do you adhere to courtesy and civility rules when communicating with the court electronically?

c. Communication with the Court

Technology should be used to alleviate paperwork, not generate more. More paperwork means more time wasted on reading and filing hard copies of documents usually available, and often already received, electronically. As one of the goals of using technology is to cut down on court delays to help increase access to justice and the courts, make sure a paper version of an electronic document is required before sending it to the court. Other common complaints by members of the judiciary regarding online communications from lawyers include being copied in inconsequential exchanges between lawyers, receiving poorly drafted emails or receiving emails that were not sent to opposing counsel.[107]

The use of social media to interact with judges can also raise ethical questions. As one author puts it, "counsel should not, unless invited or directed by the court, [use social media to] communicate directly with a judge out of court about a pending case; contact a judge regarding administrative matters; contact a presiding judge during the course of a hearing; or communicate with a judge following a hearing or during deliberations."[108]

---

105 FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 7.2-1.

106 Virginia SHEA, *Netiquette*, Albion Books, 2004.

107 The Cyberjustice Laboratory at the University of Montreal recorded complaints by judges during working seminars with a focus on the use of technology by lawyers.

108 See Leonard POLSKY, "Will you be my learned friend?"(2014) *The Lawyers Weekly* 14; and Christina VASSILIOU HARVEY, Mac R. MCCOY, and Brook SNEATH, "10 Tips for Avoiding Ethical Lapses When Using Social Media" (2014) *Business Law Today*.

Are you in compliance with your ethical obligations when operating a paperless office?

d. Paperless office

There are numerous benefits associated with adopting a paperless office, such as:

- reduced environmental impact
- productivity gains (spend less time looking for documents)
- cost savings (space, paper, printing, storage)
- remote access with proper security
- easier disaster recovery planning.[109]

These benefits, particularly the productivity gains and cost savings (if transferred to the client in whole or in part) can have the added benefit of increasing access to justice. It is critical that the technology used and the policies in place are well adapted to your practice and respect the applicable privacy laws, codes of professional conduct and security guidelines.

There are a number of resources that provide advice on operating a paperless law office.[110] Before going down that road, ensure that you have an adequate infrastructure in place to keep client information confidential and secure, and that complies with records retention requirements in your jurisdiction. Remember your obligation to "care for a client's property as a careful and prudent owner would when dealing with like property"[111] and that some original documents will still have to be kept in paper form.

Finally, although this is not necessarily limited to paperless offices, lawyers should be mindful of versioning practices. Version control measures should be adopted to limit the risk of two lawyers working on different versions on the same document.[112]

Does your use of technology respect courtroom rules and decorum?

e. Technology in the courtroom

Although more and more courts are now equipped with computers and other related technology[113], lawyers should be mindful of how their use of technology impacts courtroom decorum. Also take into account court rules that may prohibit certain technologies such as iPads or other technologies that allow lawyers to record a

---

109 LAWYERS' INSURANCE ASSOCIATION OF NOVA SCOTIA, "Going Paperless".

110 See, for example: LAWYERS' INSURANCE ASSOCIATION OF NOVA SCOTIA, "Going Paperless"; David BILINSKY, "Going Paperless – Techshow Style" (2014) *Slawtips*; CANADIAN BAR ASSOCIATION, "CBA Law Office Sustainability Challenge"; Adriana LINARES, "Paperless in 12 Steps" (2012) *Law Technology Today* ; Sheila M. BLACKFORD and Donna S. M. NEFF, *Paperless in One Hour for Lawyers*, Chicago American Bar Association, 2014.

111 See FEDERATION OF LAW SOCIETIES OF CANADA, *Model Code of Professional Conduct*, r. 3.5-2.

112 See Patricia J.F. WARSABA, "Electronic Issues for the Commercial Lawyer", 6.

113 See Jane BAILEY, "Digitization of Court Processes in Canada" (2012).

proceeding.[114] Even if no such restrictions exist, proceedings should only be recorded with the court's knowledge and consent.[115]

Furthermore, as pointed out in the *Washington State Access to Justice Technology Principles*, "[i]ntroduction of technology [into the courtroom] or changes in the use of technology must not reduce access or participation and, whenever possible, shall advance such access and participation"[116]. Once again, the proportionality principle, which implies that a fair and just process also needs to be "accessible — proportionate, timely and affordable"[117] should be taken into account. After all, "[t]he overriding objective of the justice system is a just result achieved through a just process by impartial and well-informed decision makers. The justice system shall use and advance technology to achieve that objective and shall reject, minimize, or modify any use that reduces the likelihood of achieving that objective."[118]

Technology should be used in the courtroom not to impress, but to increase access to justice and help the Court better understand the facts.

---

114 See for example, the Cour du Québec's "Lignes directrices concernant l'utilisation des technologies en salle d'audience", or the Provincial Court of Alberta's "Electronic and Wireless Devices Policy". See also *Director of Child and Family Services* v. *D.M.P. et al.*, 2009 MBQB 193.

115 See, for example, Alberta's "Media Audio Recording Policy".

116 WASHINGTON STATE SUPREME COURT, "Washington State Access to Justice Technology Principles", (2004).

117 *Hryniak* v. *Mauldin*, [2014] 1 SCR 87, par. 28.

118 WASHINGTON STATE SUPREME COURT, "Washington State Access to Justice Technology Principles", (2004).