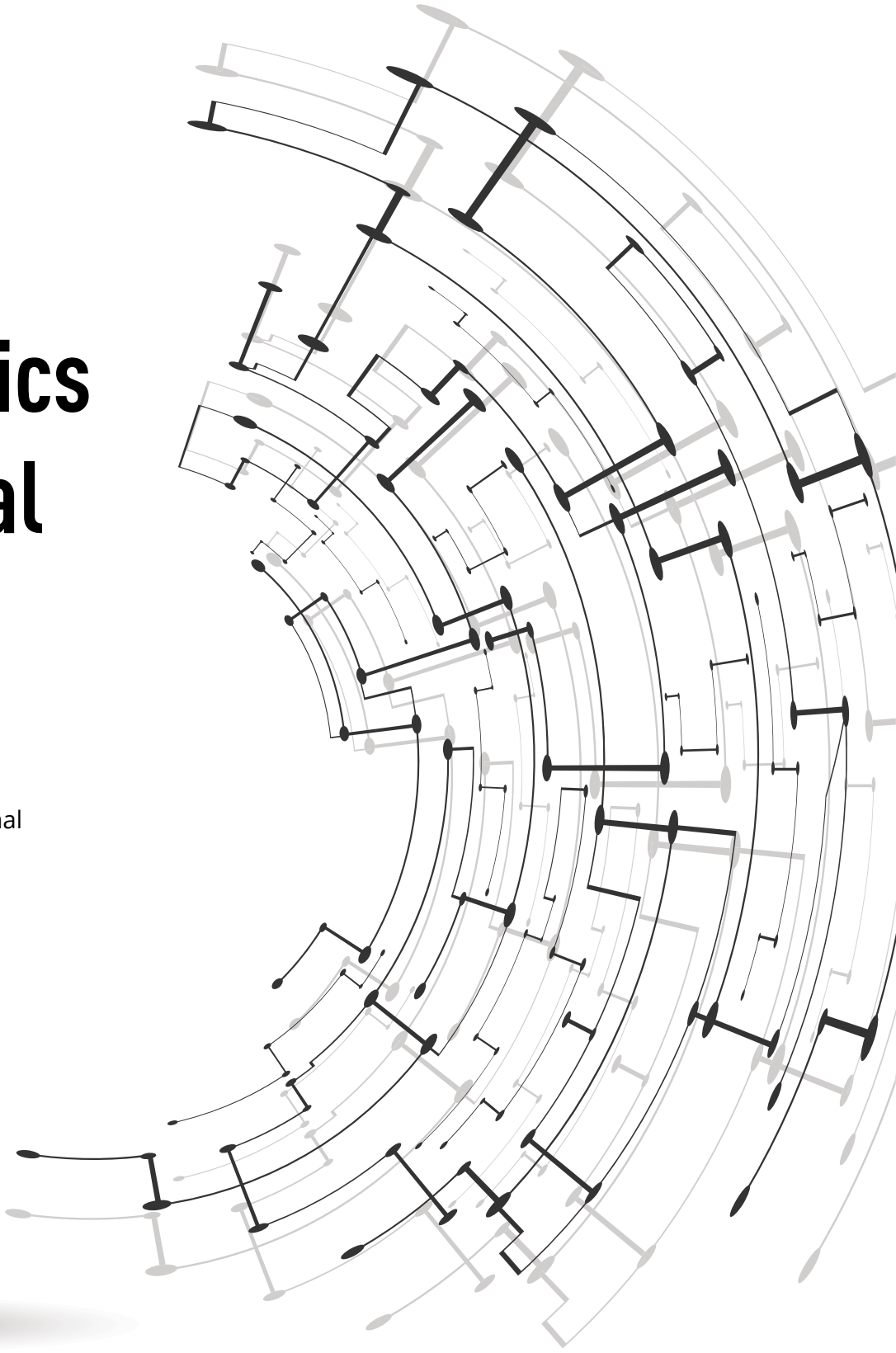
THE CANADIAN
BAR ASSOCIATION

Legal Ethics in a Digital Context

Prepared by Amy Salyzyn
and Florian Martin-Bariteau
for the Ethics and Professional
Responsibility



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, the 2014 Practising Ethically with Technology guidelines, and the 2015 Legal Ethics in a Digital World.

The new version, from content to format, builds on comments and suggestions received by various stakeholders (lawyers, law societies, insurers) in fall 2020. We would also like to acknowledge very helpful feedback received on early drafts in winter 2021, and notably Juda Strawczynski, practicePRO; Naomi Horrox and Will Morrison, Law Society of Ontario; Glenn Tait, Law Society of the Northwest Territories; Barbara Buchanan QC, Law Society of British Columbia; Darcia Senft, Law Society of Manitoba, Elaine Cumming and Code of Professional Conduct Committee, Nova Scotia Barristers' Society; Michael Joyce and Fyscillia Ream, SERENE-RISC; Yuan Stevens, Ryerson Leadership Lab/Cybersecure Policy Exchange; Monica Goyal, Caravel Law; the Canadian Bar Association, Access to Justice Subcommittee; and as well as staff lawyers from the Law Society of Alberta; the Law Society of Newfoundland and Labrador; and the Direction du droit des technologies de l'information et de la propriété intellectuelle, ministère de la Justice du Québec.

We thank the CBA Ethics and Professional Responsibility Subcommittee 2020-2021: Craig Yamashiro, Chair; Jennifer Biernaskie; Charles B. Côté; Colin Ouellette and Leslie Walden.

We also thank Scotiabank Fellows Jacob Racine, Rachael Ostroff, and Samarra D'Souza for their assistance in the research and copyediting of the document.

Table of Contents

Introduction

Technology has long been a part of legal practice. Many years ago, for example, lawyers began to capitalize on the availability of tools like typewriters and dictation machines to offer better and more efficient legal services. Later, the advent of faxing gave lawyers a quick and relatively secure way to communicate with clients and courts. The introduction of computers into legal workplace brought even more changes.

But much has changed in a relatively short period of time. Lawyers now find themselves practicing in a context that is necessarily digital. *Legal Ethics in a Digital Context* aims to address the new opportunities and risks that lawyers face in our current digital context, when vast amounts of data can be stored and shared electronically, and new tools are continually emerging to empower lawyers and their clients in unprecedented ways.

The purpose of this document is to help lawyers productively and responsibly interact with technology in their legal practices. Areas of potential benefits and risks are identified, as well as best practices and further resources.

Embracing the use of relevant technological tools is no longer optional for Canadian lawyers. As discussed in the following section, professional conduct rules both implicitly, and, in some cases, now explicitly, require lawyers to use technology competently.

Apart from the rules, harnessing relevant technological tools can bring significant benefits to both lawyers and clients. For example, there are gains to be had in relation to efficiency and effectiveness. Likewise, being able to protect one's practice and clients from technology-based risks is now a key part of prudent and responsible lawyering.

On a systemic level, the appropriate and equitable use of technological tools by lawyers can help facilitate increased access to justice and improve the administration of justice. That said, it must also be recognized that technological tools are not equally accessible and available to all lawyers and clients. In some cases, using or mandating technology can generate new barriers. The topic of technology, access to justice and the delivery of legal services requires a contextual and nuanced discussion.

In general, the references to rules throughout this document are to the Federation of Law Societies of Canada's *Model Code of Professional Conduct*. When reviewing this document and suggested resources, lawyers should remember that their ethical and legal obligations are governed by the code of professional conduct, law society rules and regulations and applicable laws in their jurisdiction (references to *Model Code*'s rules are hyperlinked to its interactive version that includes reference to equivalent rules for the different law societies).

Additionally, the content in this document should be evaluated for its currency—changes in technology and associated law society rules and guidance can occur rapidly. Lawyers are encouraged to reach out to their law society if they are uncertain about the regulatory applicability of a particular practice or resource.

Understanding Ethical Duties in a Digital Context

Before proceeding to discuss specific practical issues, this section pauses to explain, with more precision, how technology can intersect with lawyers' obligations under professional codes of conduct.

First, to the extent that a lawyer's understanding and use of technology can lead to the more **efficient** delivery of legal services, a lawyer's duty to provide efficient legal services under Rule 3.2-1 and Rule 4.1-1 is engaged. Additionally, Rule 3.6-1 "Reasonable Fees and Disbursements" also indirectly implicates efficient work practices in mandating that "a lawyer must not charge or accept a fee or disbursement, including interest, unless it is fair and reasonable and has been disclosed in a timely fashion." A lawyer's fee might not be considered "fair and reasonable" if the lawyer charges a higher fee as a result of not using a relevant technology that could have generated efficiencies, or fails to pass on cost savings from technology use to clients.

Second, if a technology is needed to produce appropriate outputs for clients, the use of this technology implicates a lawyer's obligation to provide **competent** legal services under Rule 3.1-2. Acting as a "competent lawyer," as defined in professional conduct rules, also includes "managing one's practice effectively" and "otherwise adapting to changing professional requirements, standards, techniques and practices" (Rule 3.1-1 [i], and [k]). Notably, in October 2019, the Federation of Law Societies of Canada added the following commentary on technological competence to the *Model Code*:

> [4A] To maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3.
>
> [4B] The required level of technological competence will depend on whether the use or understanding of technology is necessary to the nature and area of the lawyer's practice and responsibilities and whether the relevant technology is reasonably available to the lawyer. In determining whether technology is reasonably available, consideration should be given to factors including

a) The lawyer's or law firm's practice areas;

b) The geographic locations of the lawyer's or firm's practice, and

c) The requirements of clients.

Several provincial and territorial law societies have already adopted this commentary into their professional codes of conduct with more likely to follow. Further discussion on this commentary can be found in the "Learn more" section below.

A duty of competence in relation to technology not only involves *using* technology that is appropriate to one's practice and a particular client matter, but also *understanding* the technology being used, including being aware of any limitations or risks.

Third, and as suggested in the above commentary, a lawyer's understanding and use of technology can intersect with their duty to **protect confidential client information** under Rule 3.3-1. If a lawyer does not take appropriate steps to protect their digital files from cybersecurity risks, confidential client information and documents in their possession may be inappropriately accessed by malicious third parties. Incorrect or careless use of technology can also lead to the inadvertent disclosure of confidential materials.

Fourth, and related to the above points, there are some cases in which the appropriate use of relevant technology can assist lawyers in **competently meeting their other professional obligations**, such as

- using technological tools to assist in screening for potential conflicts of interest (Rule 3.4-1);
- putting appropriate technical safeguards in place in order to appropriately preserve and protect client property and funds (Rule 3.5 and relevant law society by-laws and regulations);
- using technological tools to assist in complying with time-keeping, record-keeping and accounting obligations (Rule 3.5, Rule 3.6 and relevant law society by-laws and regulations)
- using electronic communications tools such as virtual meetings platforms, digital messaging tools and client portals to meet obligations to communicate with clients in a timely and effective manner (Rule 3.1-1 [d] and Rule 3.1-2)
- adopting appropriate digital marketing and social media practices (Rule 4.2 and Rule 7.2-1).

Fifth, and finally, a lawyer's obligation **to encourage public respect for and try to**

improve the administration of justice under Rule 5.6-1 also suggests a responsibility on lawyers to be attentive to the potential systemic benefits (and risks) of using technology in the justice system as part of their obligation as champions and caretakers of the equal and fair administration of justice in Canada.

Learn more:

- Federation of Law Societies of Canada, "Interactive Model Code of Professional Conduct" (November 2020).
- Amy Salyzyn, "A Taxonomy for Lawyer Technological Competence", *Slaw* (December 18, 2020).
- Amy Salyzyn, "Its Finally (Sort of!) Here!: A Duty of Technological Competence for Canadian Lawyers", *Slaw* (November 26, 2019).
- Jason Morris, "Duty of Technical Competence: Missing the Point", *Slaw* (December 10, 2020).
- Law Society of Alberta, "Code of Conduct Changes" (February 27, 2020).

1. Using Technology to Provide Efficient, Effective and Ethical Legal Services to Clients

Using relevant and appropriate technological tools can result in less expensive, more accessible, and improved legal services. Technology can also be a key tool in meeting other professional obligations, such as avoiding acting in a conflict of interest and complying with record-keeping and accounting requirements. However, when considering the use of a technology, a lawyer should also be attentive to the possibility that its use may create barriers for certain members of the public and take steps to either alleviate such barriers or provide an alternative process or mode of delivery.

Lawyers should also take care to perform their own due diligence before adopting any particular technological solution in order to ensure that the technology is reliable and appropriate for their practice.

Objective: Technology is optimally used to provide efficient, effective, and ethical legal services

Below are a number of questions to ask in assessing compliance and the potential systems and practices to fulfill said compliance.

Q: Have technological tools been adopted where appropriate?

Consider whether using the following types of technology would be helpful and appropriate:

- ✓ Practice management tools (e.g. time and billing software, file management, conflicts checking systems);
- ✓ Document management and storage tools;
- ✓ Client relationship management tools (e.g. client communication portals, online payment options);
- ✓ Security software;
- ✓ Remote access tools;
- ✓ Automated forms and documents;
- ✓ Sanctions and watch lists screening software.

Q: Before adopting a technology, has there been appropriate due diligence?

Where possible, conduct the following research before adopting a technology:

- ✓ Review the vendor's track record (e.g. how long the vendor has been in business, their business model and other customers);
- ✓ Consider security features;
- ✓ Consider level and nature of ongoing support;
- ✓ Review the applicable terms of service and consider any risks arising therefrom (including, for example, whether the lawyer will be able to retain custody and control of confidential records);
- ✓ Review law society's practice advice material or contact law society practice advisors for general advice;
- ✓ Look for recommendations and information in continuing education events and bar association publications.

Q: Are technological processes adopted sufficiently inclusive?

- ✓ If a technology is used, ensure adequate alternatives are in place where there are barriers to access for clients.
- ✓ Adopt applicable accessibility standards in relation to electronic documents and processes.

Using Appropriate Legal Technology

Lawyers need to consider whether they have adopted appropriate technological solutions for their legal practice.

The term "legal technology" is broad and encompasses many different types of physical and digital tools. As a foundation, having appropriate hardware, such as properly functioning computers and computer systems, is obviously key to providing competent and efficient legal services. The nature of the hardware that will be appropriate will vary considerably between legal practices.

There is no list of "mandatory" legal technologies that lawyers must adopt. Additionally, as noted by the Law Society of Alberta, the new *Model Code* commentary on technological competence "does not require lawyers to purchase the latest and most expensive technological solutions." Indeed, the cost of a technological tool in relation to the potential benefits it may provide—such as improved quality or cost-savings—is an important factor to consider when deciding whether or not to adopt a particular tool.

In some contexts, however, the use of a particular technology may be required because of existing regulations or court rules. Some courts, for example, now mandate electronic filing. In real estate practices, it may be necessary to electronically register property.

In litigation contexts, courts may issue directions on a case-by-case basis as to how technology should be used by lawyers. Lawyers will be expected to have a comfort and basic skill set in relation to commonly used technological tools.[1] While they need to comply with any directions from the court, lawyers may also want to proactively suggest particular technologies at case management or pre-trial stages—as simple as electronic submissions of authorities and other documents to the courts—when this can be more efficient, and reduce costs for their clients, as well as other actors involved in the case.

In criminal matters, courts have ruled that the Crown has discretion to disclose material electronically so long as it is reasonably accessible.[2] Although courts will consider the circumstances and sophistication of the accused and their lawyer when determining if electronic evidence is "reasonably accessible", courts will also hold counsel to a minimum level of technological competence. [3]

---

[1] See, e.g., *Arconti v. Smith*, 2020 ONSC 2782 at para. 33 (stating "in 2020, use of readily available technology is part of the basic skillset required of civil litigators and courts. This is not new and, unlike the pandemic, did not arise on the sudden. However, the need for the court to operate during the pandemic has brought to the fore the availability of alternative processes and the imperative of technological competency. Efforts can and should be made to help people who remain uncomfortable to obtain any necessary training and education. Parties and counsel may require some delay to let one or both sides prepare to deal with unfamiliar surroundings.").

[2] See, eg., *R. v. Therrien,* 2005 BCSC 592, at paras 27-28, *R v. Sawchuk*, 2019 ABQB 252 at para. 30, *R. v. Cuffie,* 2020 ONSC 4488 at paras. 27-33.

[3] For authority relating to courts adopting a contextual analysis, see, e.g., *R. v. Sawchuk*, 2019 ABQB 252 at para. 30 and *R. v. Cuffie*, 2020 ONSC 4488 at para. 32; *R. v. Piaskowski et al*, 2007 MBQB 68 at para. 43. For judicial comments on minimal technological competence, see, e.g., *R. v. Oszenaris*, 2008 NLCA 53 at para. 20 (stating, "In today's world, it is not unreasonable to expect that counsel will be in a position to utilize a computer for the management of large volumes of material.") and *R. v. Beckett*, 2014 BCSC 731 at para. 8 (stating "[t]he current absence of computer skills of an accused or counsel is not a bar to electronic disclosure, if those skills can be acquired relatively easily.")

A requirement to use a particular technology can also be inferred from general practices, in some cases. For example, in litigation, it is accepted that lawyers need to conduct legal research using electronic databases and can potentially expose themselves to negligence claims or law society complaints if the quality of legal services they provide is inadequate as a result of only relying on print reporters.[4] More recently, courts have also suggested that AI-empowered legal research tools can be one way for a lawyer to reduce costs when acting on a litigation file.[5]

Additionally, the use of appropriate technological tools can be inferred, at times, from the rules in professional codes of conduct. For example, while virtually all lawyers are already available to their clients through the telephone and emails, lawyers should consider whether using additional digital communications tools—such as private messaging services or client communication portals—would assist in timely and appropriate communications to clients (Rule 3.1-1 [d] and Rule 3.1-2. When using additional digital communications tools, however, lawyers need to take care to ensure that all communications, regardless of platform, are properly included in the client file and that proper security measures are taken *(issues of data security are discussed in Section 2, Appropriately Safeguarding and Managing Digital Data and Electronic Records).*

Lawyers may want to consider using automation as a means to facilitate more efficient and improved legal services to clients (Rule 3.1-1, Rule 3.2-1 and Rule 3.6-1). Adopting automated processes benefits both lawyers and their clients. By automating administrative tasks, lawyers can free up their time to focus on more substantive legal work which is likely to be both more financially and mentally rewarding. In some cases, automated processes can also reduce opportunities for human error—for example, if a practice management software automatically populates a client's personal information in multiple parts of a law firm's information management system, this can avoid mistakes such as a client's name or telephone number being inaccurately entered. Key areas to consider automation include practice management (for example, client intake and billing) and document creation. At the same time, lawyers should be mindful that tools processing data on the cloud (from copy-editing assistance to analytics) may present concerns for the confidentiality of client information.

Finally, lawyers should consider how technology may help them comply with their duty to

[4] See, e.g., *Aram Systems Ltd. v. NovAtel Inc.*, 2010 ABQB 152 at para. 23 (stating "[T]he view of computerized legal research as a mere alternative is no longer consonant with the reality of current legal practice. Such research is now expected of counsel, both by their clients, who look to counsel to put forth the best possible case, and by the courts, who rely upon counsel to present the most relevant authorities. Indeed, it might be argued that a lawyer who chooses to forgo computerized legal research is negligent in doing so...The practice of law has evolved to the point where computerized legal research is no longer a matter of choice.")

[5] See, e.g., *Cass v. 1410088 Ontario Inc.*, 2018 ONSC 6959 at para. 34 (stating, "[t]here was no need for outsider or third party research. If artificial intelligence sources were employed, no doubt counsel's preparation time would have been significantly reduced.")

avoid acting where there is a conflict of interest and to meet other compliance obligations. For example, moving to a computerized database conflict checking system is generally an improvement over a paper-based system as it can allow for quick input and retrieval of data and can also better manage and analyze large amounts of information. Likewise, it is generally recommended that lawyers use electronic financial systems to assist in complying with record-keeping and accounting requirements. In some cases, lawyers may want to use technological tools to assist in screening clients against sanctions regulations and watch lists that prohibit or restrict dealing with specific persons or entities.

Learn more:

- Michelle Wong, "A Beginner's Guide to Law Office Automation", Clio (last updated 2021).
- Heidi Alexander, "The Advantages of Automation: Experienced Practitioners Discuss their Successful Solutions for Automating Their Practice", ABA (January 1, 2020).
- Law Society of Ontario, "Practice Management Guidelines: Technology" (last updated 2020).
- Canadian Bar Association, *Conflicts of Interest Toolkit* (2020).
- Sharon D. Nelson, John Simek and Michael Maschke, *The 2020 Solo and Small Firm Legal Technology Guide* (ABA Book Publishing: 2019).

Choosing Legal Technology and Due Diligence

Not all legal technologies will be suitable for every legal practice. Moreover, while many, if not most, commercially available legal technologies come from reputable vendors, not all tools are necessarily of the same quality or provide the same protections for lawyer and client data. There are no authoritative lists of "approved" legal technologies to which Canadian lawyers can refer. As such, lawyers need to ensure that they conduct appropriate due diligence, including understanding the vendor's track record as well as the security features and support provided. Before adopting a technology, lawyers should also review the applicable terms of service and consider any risks arising therefrom.

When deciding on a technological tool to use, lawyers may want to review their law society's practice advice material or contact their law society's practice advisors to obtain advice about technology use. However, Canadian law societies do not generally approve or otherwise endorse lawyers' use of any particular technological tool.[6] Increasingly,

[6] One exception is BC *Law Society Rules,* r. 10(3)(5), under which the Law Society of British Columbia may declare that lawyers are not permitted to use a specific "storage provider" (including a cloud storage provider).

continuing education events and bar association publications contain helpful information about specific technological tools and can be good resources of reference for lawyers. Compatibility of the technological tools with other lawyers and law firms practicing in the same area is also an important factor to consider, where compatibility of tools is a relevant factor (e.g. video-conferencing platforms).

Learn more:

- Nicole Black, "Vetting Legal Technology and Software: 3 Tips from the Experts", *My Case* (last updated 2021).
- Derek Bolen, "What Technology Does Your Law Firm Actually Need?", *Clio* (last updated 2021).
- LawPRO, "Technology Products for Lawyers and Law Firms" *PracticePRO* (updated November 2020).
- Sharon D. Nelson, John Simek and Michael Maschke, *The 2020 Solo and Small Firm Legal Technology Guide* (ABA Book Publishing, 2019).

Access to Justice Considerations

There has been a significant increase in the use of technology in legal practice and in the courts. In some cases, using technology in the delivery of legal services can enhance meaningful access to justice. For example, if automation is used to reduce the cost of handling client matters, these savings can be translated into lower fees for clients. Another example is that some clients may find using a communication portal is easier and provides more meaningful information about the status of their matter as compared to calling their lawyer or sending an email.

At the same time, lawyers should be cautious—in particular, in relation to using client-facing technologies—not to unintentionally introduce new barriers to access. Not every client or potential client will have reliable access to the Internet. There are well-documented issues of inadequate access to Internet connectivity in Canada's Northern, rural and otherwise remote communities. Additionally, financial constraints can impact an individual's ability to afford adequate access to the Internet in their home or the necessary hardware (e.g. computers, tablets, and smartphones) to use client-facing technologies. Some clients may not be sufficiently "technologically literate" or be comfortable with all technological tools that a lawyer might use. For those clients, having alternative processes in place can be important.

While lawyers' duties rest primarily with their clients, lawyers also have obligations in relation to improving the administration of justice generally, and should consider the

implications of their choices toward other actors of the justice system (Rule 5.6-1). Rather than increasing access to justice, use of technology can create barriers for opposing parties—especially for self-represented litigants and marginalized communities. While lawyers may want to recommend technologies to the court to be more efficient, lawyers should also reject, minimize, or modify any use of technology that might impede on the fair and affordable justice system for Canadians.

Learn more:

- Jena McGill, Amy Salyzyn, Suzanne Bouclin and Karin Galldin, "Emerging Technological Solutions to Access to Justice Problems: Opportunities and Risks of Mobile and Web-Based Apps" (October 13, 2016).

Accessibility Standards

Lawyers should also make sure that documents and communications are accessible to persons with disabilities, whether colleagues, clients or potential recruits. For example, some clients may request or require a specific manner of communication as a result of a disability.[7] Law society rules acknowledge that lawyers have a "special responsibility" to respect human rights laws (Rule 6.3-1, Commentary [1]). Accessibility standards—specifically as they pertain to electronic documents—differ from one province to the next. You should be aware of the applicable standards and assess your compliance *(issues of web accessibility are discussed below in Section 4, "Lawyers' Online Presence.").* Where possible and relevant, lawyers should also consider adopting inclusive or "universal" design approaches, which emphasize designing processes or materials for inclusiveness from the outset, rather than reactively removing barriers or making individual accommodations.

Learn more:

- Access Forward, *Information and Communications Standard Module* (last accessed January 29, 2021).
- Government of Canada, *Digital Accessibility Toolkit* (last updated September 12, 2020).
- ARCH Disability Law Centre, Tips for Lawyers and Paralegals on Providing Accessible Legal Services to Persons with Disabilities in Ontario (January 2019)

[7] ARCH Disability Law Centre, *Fact Sheet – Tips for Lawyers and Paralegals in Ontario: Accommodating clients by communicating via email* (October 1, 2019)

- Ontario Human Rights Commission, "Policy on ableism and discrimination based on disability" (2016)

2. Appropriately Safeguarding and Managing Digital Data and Electronic Records

Lawyers have ethical duties to protect clients' confidential information and to safeguard client property in their possession, including client funds. Lawyers are also required to comply with privacy legislation in managing their practices. Technologically based risks—from both malicious and benign sources—can frustrate lawyers' efforts to fulfill these obligations and, in some cases, lead to ethical or regulatory breaches. Such breaches can result in negative monetary and reputational consequences for lawyers. By being aware of, and taking steps to protect against, technologically based risks, lawyers can guard against such negative consequences and give current (and prospective) clients confidence that their information and property will be properly secured and maintained.

As legal practice increasingly moves toward digitalization, it is important for lawyers to understand key security and privacy risks and adopt good cybersecurity hygiene. For lawyers less familiar with technology, there are many resources that can be consulted to better understand those concepts. Notably, leading Canadian cybersecurity scholars have developed free online training modules, with videos, lexicon, as well as cheat sheets and handouts—these are available at **www.cybersec101.ca**. These resources might also be useful for law firms to provide essential cybersecurity training to all individuals in their organization.

Objective: Digital Data and Electronic Records are Appropriately Safeguarded and Managed.

Below are a number of questions to ask in assessing compliance and the potential systems and practices to fulfill said compliance.

Q: Are appropriate security measures adopted?

Consider equipping all digital devices with:

- ✓ Password protection;
- ✓ Full-disk encryption;
- ✓ Firewalls;
- ✓ Anti-virus/anti-malware software, and intrusion detection software;
- ✓ Encryption solutions to send sensitive information;
- ✓ Device location tracking software, with remote wipe capabilities.

Ensure to continuously update:

- ✓ Operating systems of all devices, from servers to routers to smartphones (if possible, automate security updates);
- ✓ All third-party software, from anti-virus and firewalls to office management to word processor.

Ensure that all individuals practice good password hygiene:

- ✓ Passwords are not shared or disclosed;
- ✓ Use of strong and unique passwords;
- ✓ Use of password managers where appropriate;
- ✓ Two-step or multi-factor authentication.

Q: Are appropriate measures adopted to monitor the integrity of the data collected or held?

Consider using the following tools to ensure the integrity of data:

- ✓ Digital signatures;
- ✓ Archival policies;
- ✓ Metadata comparison;
- ✓ Ensuring that documents are backed up so that a corrupted file can be replaced by an untouched copy.

Q: Is data adequately accessible over time?

Ensure that appropriate backup practices are followed:

- ✓ Have a backup and disaster recovery plan for all data;
- ✓ Maintain several backups;
- ✓ Consider using an automated backup process;
- ✓ Stagger and separate backups from the rest of the network.

Q: Are appropriate practices adopted for data deletion?

Ensure that any data is deleted in a manner that is consistent with professional obligations:

- ✓ Before deleting data, ensure that the proposed deletion is consistent with records retention obligations;
- ✓ When deleting data, ensure compliance with client confidentiality obligations (this requires an understanding of how to adequately delete data from a digital device).

Q: Has the use of cloud-based storage and tools been considered?

Consider the potential benefits of cloud-based solutions:

- ✓ Access to new software services and applications;
- ✓ Off-loading hardware and software maintenance;
- ✓ Easy virtual access to data;
- ✓ Automated backup of data.

If considering a cloud-based solution, conduct appropriate due diligence:

- ✓ Review the Law Society of British Columbia's *Cloud Computing Checklist* (noting any necessary modifications given the jurisdiction in which you practice).

Q: Is there sufficient awareness of data security risks, and preparedness in case of exposure to an attack or a natural event?

Develop an information security management framework, including:
Information security policy;

- ✓ Privacy policy;
- ✓ Incidence response plan;
- ✓ Data security literacy plan so all individuals working in the organization receive ongoing education in relation to cyber-dangers, including management of sensitive information, phishing, ransomware, and password hygiene;
- ✓ Cybercrime/digital risk insurance.

Q: Is there a sufficient understanding of metadata and how to guard against its inappropriate disclosure?

- ✓ Steps should be taken to minimize the creation of metadata or to wipe it from sent files or materials uploaded to a web platform (except where there is a legal requirement to retain and disclose metadata, e.g. discovery obligations);
- ✓ Understand when metadata embedded in an email or social media post might contain location information and take necessary steps to avoid disclosing locational data where this is sensitive information.

Q: Are best practices adopted when travelling with electronic devices across borders?

- ✓ Review the guidance documents prepared by the CBA and FLSC on the issue of travelling with electronic devices across borders.

Data Security

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." (Rule 3.3-1) Lawyers must also abide by privacy and information security regulations for private sector actors on how to properly manage information, and comply with their reporting obligations in case of data breaches. This implies an underlying obligation to adopt security measures to protect that data (e.g. device tracking, firewalls and intrusion detection software, also called Endpoint Detection and Response software). Law firms should also adopt organizational measures, including providing relevant information and training to individuals in their organization.

Security measures should be put in place to guard against third-party access to confidential data during its lifecycle. This implies that information should be protected from its creation to its destruction, and through every intermediary phase.

Just as it is essential that lawyers take measures to control and restrict access to physical files (such as taking security measures in relation to offices and file cabinets), measures must also be taken to control and restrict access to digital information. As such, lawyers should enable password protection on all their devices, and equip all their electronic devices with appropriate security software, including firewalls, and anti-virus/anti-malware software, and make sure to update them on a regular basis. All electronic devices should be controlled through device location tracking systems (e.g. "Find My Device" app) that allow for emergency information on locked screens, and remote wiping should the device be lost or stolen.

To protect client's information, access to any electronic devices and to any data on hard drives or share drives should be restricted by control access (e.g. passwords), and on a "need-to-know" basis. Similarly, any electronic device should be encrypted—preferably through full disk encryption, as well as any data on hard drives, shared drives or external drives (e.g. USB key).

When browsing on the Internet, make sure you consult or input sensitive information (e.g. online payments) only on secured websites delivered through an HTTPS connection,[8] so no third party can eavesdrop on your Internet traffic.

Encryption Essentials

Data breaches have become a common occurrence. Malicious actors can not only obtain confidential details about past and ongoing client matters but may also steal your client's sensitive personal information (e.g. date of birth, banking information, contact information). To limit the impact of a data breach or data interception, all lawyers should

[8] Most browsers display a lock next to the web page address in the address bar to signal that the web page is delivered through a secure connection. You can also look at the address and note that it starts by "https://" rather than "http://".

have at least a general understanding of encryption. They should have encryption solutions available for use when appropriate and make informed decisions about when it should be used and when it may be avoided. As a rule, all data should be stored in an encrypted manner, and electronic correspondence containing confidential or sensitive information should be sent encrypted.

When reviewing solutions and their practices, lawyers should make sure that data containing sensitive information are encrypted both *at-rest* and *in-transit*. The data should be encrypted at-rest—i.e. stored fully encrypted on your hard drives or cloud services—so a third party that is able to access the storage system would not be able to read it. The data should also be encrypted end-to-end while in transit—i.e. while it "travels" between your device and another, either to a cloud service or to another mailbox—so a third party that might attempt to intercept Internet traffic cannot read it.

Password Hygiene

Even the strongest encryption and secured system might be moot if there is not good password hygiene by authorized users. To ensure data security, it is critical for lawyers to maintain good password hygiene. Indeed, poor password habits (e.g. sharing or reusing passwords, use of personal information, using simple passwords such as "1234" or "password," or keeping the default passwords) are often one of the weakest links in data security practices.

Credentials should never be shared and disclosed, even internally, to ensure that users can be segregated in case of a cyber-attack and to allow access to be swiftly revoked when an individual leaves an organization. Passwords should not be written down in plain sight, either on paper (e.g. note on your monitor or nearby) or even saved in your computer.

While it does not eliminate all password-related risks, lawyers should consider relying on password managers that generate unique randomly created passwords and store them in a single, secure place. Most managers also provide alerts in case of password reuse, or if some platforms have known security risks. You need to remember only one password to access the application. This means, of course, that one needs to be extremely careful in choosing and protecting this master password.

Lawyers should use two-step authentication (also called multi-factor authentication) where available. Beyond your password, you will need a second token to be authenticated (e.g. a code generated by an app on your phone, or a code generated by a physical token, or a fingerprint). It is recommended to avoid utilizing codes sent by mobile text message for sensitive systems, as SIM card hacking and swapping are increasingly common.

If a lawyer suspects that they've been hacked, they should change their password immediately, and inspect the recent activity on their system or account. The lawyer should also ensure that they comply with any reporting obligations *(see below section titled "Preparedness, Incident Response, and Digital Risk Insurance").*

Learn more:

- Canadian Centre for Cybersecurity, *Baseline Cyber Security Controls for Small and Medium Organizations* (February 2020).
- LawPRO, "Cybersecurity and Fraud Prevention Tips" *PracticePRO* (2021)
- Derek Bolen, "What Lawyers Need to Know about Encryption", *Clio* (last updated 2021).
- Lawyers Insurance Association of Nova Scotia, "Data Security" (last updated 2021).
- Law Society of Ontario, "Technology" (last updated 2020).
- Matt Burges, "How to Know If You've Been Hacked, and What to Do About it", *Wired* (July 19, 2020)
- Serene Risc, "Cybersecurity Tips" (last updated 2019).
- LawPRO, "Fraud Fact Sheet: Cybercrime and Bad Cheque Scams" *PracticePRO* (2018).
- LawPRO, "Encryption Made Simple for Lawyers", *PracticePRO* (December 15, 2017).
- Barreau du Québec, *Guide des TI* (2016).
- Office of the Privacy Commissioner of Canada, "PIPEDA and your legal practice" (last modified 2015).

Data Integrity and Accessibility

Lawyers must guarantee the integrity and accessibility of documents and data in their files.

In order to ensure data integrity, lawyers need to take steps to guard against their data being modified, altered or destroyed—intentionally or otherwise. 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.

Lawyers also need to ensure their data is accessible over time, and at any time. Meaningful access to data requires that the information and files be intelligible for the individual who

requires access. This entails the individual having access to the software necessary to read a given file (e.g. a file created with an older or different version of word processing software such as WordPerfect). When possible and compatible with rules regarding data integrity, long-term accessibility may require lawyers to consider a backup in a format that is open (i.e. not subject to license, or use of proprietary software) and multiplatform.

Not only is ensuring data integrity and accessibility necessary under several regulatory and statutory frameworks, it goes to the heart of a lawyer's duties in relation to competence and quality of service, which includes managing one's practice effectively and giving a client complete and accurate relevant information about a matter (Rule 3.1-1 [d] and [i] and Rule 3.2-1, Commentary [5]). Inaccessible, incomplete or corrupted data can result in a lawyer giving inaccurate information or advice to a client or other third parties to whom they may be required to give information. For example, altered data can interfere with a lawyer's obligation to reply promptly and completely to requests for information and documents from their law society. (Rule 7.1-1)

Safeguard of Data Over Time (Backups)

Lawyers must be aware of risks relating to potential data loss and guard against such risks. For example, a physical hard drive can become inaccessible and data may be lost. This can happen for many reasons, including cyber-attacks, but even more likely from non-malicious sources ranging from lack of server maintenance, power failures, water damage or aged hard drives that limit access to computerized files.

Backing up files is a necessary and essential component of competent data and file management. Lawyers should have backup and disaster recovery plans for all data that they manage and need to retain, either from a practice management perspective or as required by law. It is recommended that lawyers have several backups, and that the backup process is automated, if possible, in real time. It is good practice to stagger your backups, and keep several different versions of the backup, each saved at different points in time—and to routinely check that backup data can be restored.

The full backups should be kept separated from the rest of the network. If your backups are connected to your system, they are subject to the same risks of data loss as the other computers on your network. While an automated backup might be on the same network, a full backup should regularly be moved off the network ("air gapped"), if possible, to a secure off-site location (notably to reduce risks in case of physical intrusion or damage to your primary work location). In any case, your backup should also be fully encrypted.

Learn more:

- Law Society of Ontario, "Technology" (last updated 2020).
- LawPath, "Data Integrity: Why Does It Matter for Businesses?" (November 3, 2020).
- Canadian Centre for Cybersecurity, *Baseline Cyber Security Controls for Small and Medium Organizations* (February 2020)
- Barreau du Québec, *Guide des TI* (2016).

Data Deletion

Once data is no longer needed and is no longer required to be kept in accordance with a lawyer's professional or other statutory obligations, it should be properly deleted. One benefit of deleting unneeded data is that it can minimize the potential impact of any security breach in relation to the lawyer's files.

Before deleting any data, lawyers should familiarize themselves with the relevant professional conduct rules (see, for example, Rule 3.5) and law society rules and regulations in their jurisdiction that relate to record retention.

When deleting data, lawyers must also ensure that they comply with their client confidentiality obligations. For example, 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. Several file wiping tools exist for this purpose. When deleting data, lawyers should not overlook hard drives in copiers and printers that store images of documents.

Learn more:

- Lawyers Insurance Association of Nova Scotia, "File/Record Retention" (last updated 2021).
- Law Society of Ontario, "File Management" (last updated 2020).
- Law Society of British Columbia, "Closed Files—Retention and Disposition" (August 2017).
- Barreau du Québec, *Guide TI* (2016).
- Law Society of Ontario, "LSO Guide to Retention and Destruction of Closed Client Files for Lawyers" (last updated 2014).

Cloud-based Storage and Tools

Cloud-based tools and services offer many benefits to lawyers and enable access to an array of new software services and applications. They also allow lawyers to offload hardware and software maintenance and upkeep to cloud providers. Finally, they allow access to data from virtually everywhere and for the reduction of large capital outlays.

Cloud-based storage and tools may also help resolve some of the previously mentioned risks. However, storage or transmission of information with third-party providers can also bring new risks with respect to the confidentiality of information and solicitor-client privilege as the lawyer is placing data in the hands of third parties. It raises issues of security and privacy, regulatory compliance and risk management, among others.

Confidentiality is of particular 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. Even servers situated in Canada could fall under foreign jurisdiction if they are operated by providers with foreign interests.

In addition to it being a good practice to keep data on Canadian servers, some records (e.g. corporate and fiscal books) are required to be kept in Canada by law.[9] The fact that data be *accessible* from Canada doesn't meet the requirement. As such, lawyers should enquire about data location with their cloud storage provider, and contractually require that their data be stored on servers located in Canada.

Unless otherwise instructed by the client, confidential information sent through the Internet to a server or to another person should be encrypted—including to cloud services. When reviewing cloud solutions, lawyers should confirm whether the data is encrypted at-rest or in-transit *(see above section on "Encryption Essentials")*.

Lawyers should also read the terms of service for information on when or how a cloud service responds to a legal notice or request for the release of data. To avoid possible confidentiality breaches, lawyers should prefer services where they can be the sole owner of the encryption keys. Indeed, cloud services may be compelled by law to release data, which may include being forced to decrypt data and release it, possibly without notifying anyone. If the encryption keys are managed by the cloud service, then the service also has the ability to decrypt and access the information in question at any time—as well as any third party that could, legally or maliciously, obtain access to the data stored.

Finally, lawyers should look for cloud services that permit a "local" backup, where the lawyer can keep a backup on their own computer. With this feature, if the Internet or

[9] See, e.g., Canada Revenue Agency's guidance notice regarding digital storage of fiscal books.

the cloud service becomes unavailable (e.g. connectivity issue, late payment, contractual disputes, third party request), the local backup will allow the lawyer to continue working.

Learn more:

- Law Society of British Columbia, "Cloud Computing Checklist v. 3.0" (last updated April 2020).
- Derek Bolen, "What Lawyers Need to Know about Encryption", *Clio* (last updated 2021).
- Canadian Centre for Cybersecurity, *Baseline Cyber Security Controls for Small and Medium Organizations* (February 2020)
- LawPRO, "How to Safely Put Your Data in the Cloud", *PracticePRO* (January 1, 2018).
- David Fraser, "Cloud computing: A Privacy FAQ", National Magazine (2014).

Email

Email is an easy way of sharing information and communicating with others but there are numerous risks associated with using email, especially with respect to preserving the confidentiality of the correspondence. Additionally, emails are often the first and easiest point of attack for cyber-criminals.

Confidentiality

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 on with a client beforehand that email (or another medium of communication) will be used. When speaking to a client about a medium of communication, they should be made aware of and agree to the risks associated with that medium. For example, clients should be made aware that the providers of free webmail services, or employers if a work email is used, are often contractually permitted to access their private conversations. It should also be explained to clients that copying others on an email can be interpreted as a waiver of privilege. A lawyer should also be cautious when replying to emails themselves—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.[10]

[10] See, e.g., *Smith v. Teixeira*, 2009 QCCQ 3402, where a Quebec lawyer was found to have acted unethically for including all of their clients' email addresses in the "to" field of an email announcing an office move, therefore letting every client see the identity and address of all other clients.

Likewise, a lawyer who receives an email communication from an opposing party or their lawyer by mistake needs to act cautiously and comply with applicable professional conduct rules regarding the receipt of inadvertent communications. (see Rule 7.2-10)

The ease of email also makes it an attractive target for cyber-criminals. To protect themselves and their clients, lawyers should send confidential and sensitive information by encrypted email *(see above section "Encryption Essentials").* Although lawyers should remember that encryption of emails only hide the content of the emails; metadata, including from who to whom, could still be visible *(see below section "Metadata")*.

Electronic Impersonation and Phishing

Phishing involves the use of an email, text message or phone call that appears to come from a trusted source or institution, vendor or company, but is actually from a third-party impostor. Phishing attacks are increasingly used against law firms and other legal organizations.[11] These attacks are also becoming more sophisticated—for example, they are often targeted toward a specific person and tailored to reference activities (like fund transfers) that the person is engaged with. Phishing messages are intended to trick you into giving fraudsters information by asking you to update or confirm personal or online account information. All lawyers and staff working in the organization need to be educated about the potential for, and nature of, phishing attacks to make sure they will not fall for them. In law firms, staff and junior lawyers are common targets—for example, in a practice known as the "Boss Scam", someone contacts an employee impersonating their superior and asking for urgent help with a payment.

As noted above, phishing emails are becoming increasingly elaborate, but red flags of phishing scams include generically addressed messages, different email signatures, or different email addresses. In most cases, the email will be sent from a free email service (e.g. Gmail or Outlook/Hotmail), even when the email is purportedly sent on behalf of a business entity, and the email headers are not consistent (e.g. name and/or email address in the "FROM"; email is sent "on behalf" from another domain).

In many cases, an email will request money or goods (e.g. gift cards) with a sense of urgency (with the goal of trying to avoid usual compliance checks with accounting). A person stating that they prefer email communication due to time zone differences or claiming not to have access to a phone at the moment are indicative of a potential scam.

Similarly, beware if there is a requirement to click on a link to an action or to continue the conversation. Verify that the link is to a legitimate website and that the link points to

[11] There are several reports of law firms being victim of phishing attacks, of being impersonated to defraud clients or contacted by fake lawyers, or clients' being hacked and sending improper wire transfer instruction.

the same URL as noted in the message (place your mouse pointer over the link). If any credentials are asked upon clicking on the link, confirm in the URL bar that you are on the actual website. It is usually recommended not to click on links in emails, but to go to the website through one's usual manner.

Beware that sometimes the email can be seen as coming from the correct email address, but invites the recipient to click on a link, or reply to a different email address. In more advanced attacks, the message can come from the actual email accounts, after hacking into email accounts of third parties including clients, lawyers, staff within a firm, opposing counsel, and opposing parties. The fraudster will monitor the emails of the hacked party to determine if there is a legal matter of interest. When the matter is completed and money is about to change hands, such as following a litigation settlement, real estate closing, or other transactions, the fraudster, posing as the legitimate party awaiting the funds, will send an email with instructions to redirect where the funds should go. If followed through, the money will go to the fraudster.

New instructions for payment (e.g. different amounts, new bank account) are often a sign of potential fraud. In case of doubt, it is safer to confirm with the person through another medium of communications (such as a telephone call) that you used before with them.

Malicious Attachment, Hacking, Spyware and Ransomware

Phishing attacks may also be more sophisticated and go beyond "simply" trying to retrieve credentials and steal money. Upon clicking on a link, users may inadvertently download malware on their computer. Malware could also be contained in an email attachment, such as a fake invoice. Beyond viruses that would corrupt data, malware can include spyware that would allow third parties to access your computer, look into all your files, your emails, and act on your behalf on your network (including sending messages to clients, colleagues, judges). The data collected can be used to defraud you or your clients.

Another increasingly common type of attack involves ransomware.[12] Ransomware attacks usually result from a phishing, where an email containing an infected link is sent to a lawyer or staff. Once the link is clicked on, the ransomware is installed on the victim's computer. It starts to work in the background while the computer is on, encrypting documents and making them inaccessible. The individual(s) who initiated the ransomware attack will then request large payments of money to release the data back to the organization.

Users should have an anti-virus tool that can live-scan web traffic and email, notably any

[12] There have been several reports in recent years of lawyers becoming victims of ransomware attacks at all levels of practice, from major national law firms, to a law society, to firms in Manitoba and Alberta.

attachments and any content downloaded from the Internet. Security and privacy settings in computers should prohibit any software to run automatically after download.

As previously mentioned, backup data should be separated from the rest of the network. This is a good way not only to prevent an attack but also to be able to retrieve data and restart work once locked out by a ransomware.

Learn more:

- Lawyers Indemnity Fund, "Fraud Prevention" (last accessed March 14, 2021)
- Juda Strawczynski, "Wire Fraud Scams on the Rise: 5 Tips to Reduce Your Risk" (2021).
- Derek Bolen, "What Lawyers Need to Know about Encryption", *Clio* (last updated 2021).
- LawPRO, "Paying Attention to the Fraud Behind the Curtain", *PracticePRO* (January 1, 2020).
- Canadian Centre for Cybersecurity, *Baseline Cyber Security Controls for Small and Medium Organizations* (February 2020).
- Raymond G. Leclair, "Firm Websites Being Impersonated by Fraudsters", *AvoidAClaim* (July 8, 2020).
- Serene-Risc, "Cybersecurity Tips: Phishing" (last updated 2019).
- LawPRO, "Fraud Fact Sheet: Cybercrime and Bad Cheque Scams" *PracticePRO* (2011).
- LawPRO, "Avoid (and Recover From) a Ransomware Attack", *AvoidAClaim* (November 15, 2017).

Disclosure of Metadata

Beyond their own contents, electronic documents contain metadata—information about other data (in this case, information about the file). 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 location of the stored file.

Except where a lawyer is legally required to retain or communicate metadata (e.g. discovery obligations), steps should be taken to minimize the creation of metadata or to wipe it from sent files. When sharing documents online, notably by email, ensure that documents sent via email do not contain metadata with confidential information.[13] This should also be considered when uploading a file on a web platform, even for personal purposes, as metadata could disclose information about your location, and thus your client and activities.

Beyond the attachment, the email itself will contain metadata, notably to ensure its authenticity. However, metadata in the header of the email could also disclose your location and the networks to which you are connected, and thus unintentionally disclose potential confidential information and relationships to third parties.

Learn more:

- Administrative Office of the U.S. Courts, "Guidelines for Editing Metadata" (September 2018).
- LawPRO, "Beware of the Dangers of Metadata" *PracticePRO* (2004).
- Office of Privacy Commissioner of Canada, "Metadata and Privacy" (October 2014).

Travel with Electronic Devices

It is important for lawyers to understand how the privacy interests of their clients—and their obligation to protect confidential client information—may be affected by lawyers crossing international borders with an electronic device. On crossing international borders, including to or from Canada, lawyers may not be able to rely on claims of solicitor-client privilege to adequately protect clients' confidential information due to border agencies' broad interpretation of the "goods" they have the authority to examine.[14] Officers may examine the data stored on any electronic device in the actual possession of, or in the accompanying baggage of, a traveller. They may also request passwords for the devices.

Searching the electronic device (i.e. phones, tablets, laptops, or USB keys) of a lawyer when

[13] While some commercial tools offer to scrub metadata from files, most PDF and word-processing software also offer an option to remove metadata when saving the document (e.g., under the "protect" or "inspect" documents options in Microsoft Word; under the "redact" options in Adobe Acrobat).

[14] Note that, in *R. v. Canfield*, 2020 ABCA 383, the Alberta Court of Appeal held that s. 99(1)(a) of the *Customs Act* is unconstitutional to the extent that it imposes no limits on the searches of electronic devices at the border, and is not saved by s. 1 of the *Charter.* The Court further declared the definition of "goods" in s. 2 of the *Customs Act* to be of no force or effect insofar as the definition includes the contents of personal electronic devices for the purpose of s. 99(1)(a) but suspended the declaration of invalidity for one year to give Parliament the opportunity to amend the legislation to determine how to address searches of personal electronic devices at the border. Leave to appeal to the Supreme Court of Canada was sought but dismissed in the matter.

the lawyer crosses an international border may infringe solicitor-client privilege and result in a breach of Rule 3.3-1 that requires lawyers to protect clients' confidential information. In addition to obligations found in professional codes of conduct, lawyers may also have obligations under rules of their respective law societies and applicable privacy legislation.

Several practical steps have been suggested to lawyers to mitigate the risk that confidential and privileged client information will be exposed when crossing the border. The safest practice is to cross the border without confidential and privileged client information. This can be done by taking "clean" or "blank slate" devices that do not contain any client information, putting the device in "airplane mode" (and disconnected from cloud services), and then accessing any needed information or files once crossed through a secure remote connection. It is also recommended that, if lawyers do travel with confidential or privileged client information, they carry identification that indicates that they are a licensed lawyer. Lawyers may want to include the relevant information in their retainer letters about protecting privileged information during travel. They should discuss the issue with their clients, and provide the appropriate guidance in the circumstances.

Learn more:

- Canadian Bar Association, "Privilege at the Border Toolkit" (May 13, 2019).
- Federation of Law Societies of Canada, "Crossing the Border with Electronic Devices: What Canadian Legal Professionals should Know" (December 14, 2018).

External Data Protection Services

Law firms may also want to consider retaining external data protection services as it can be challenging for firms to develop and implement their own cybersecurity policies and infrastructure, from the cost of hardware to making sure it remains up to date. Beyond reducing costs of infrastructure and staffing by sharing them, outsourcing also allows lawyers to have adaptative protection, and scale it up as they grow and take on more sensitive clients or files. Service providers can also support lawyers in case of cyber incidents, ranging from recommending and installing preventative measures to dealing with insurers in the event of a breach.

Learn more:

- LAWPRO, "Outsourcing your law firm's cybersecurity", *PracticePRO* (August 1, 2017).

Preparedness, Incident Response, and Digital Risk Insurance

Notwithstanding all the security measures put into place, there will always be a risk that clients' data could be disclosed, destroyed or modified. Beyond cybersecurity risks, data can also be destroyed or compromised as a result of natural events, such as floods or fires. It is part of lawyers' duties to develop an information security management framework, from information security, devices and privacy policies, to an incident response plan in order to be prepared for such events.

To ensure that best practices relating to data security, integrity and accessibility are adopted and continuously followed in a legal workplace, it is recommended that lawyers ensure that they have an information security policy in place. Guidance should be given to lawyers and staff on the use of personal equipment for work, or use of work devices and networks for personal purposes. In certain contexts, it can be good practice to limit access to sensitive files or information, to specific devices or on specific networks.

Legal workplaces should have a list—and remote control—of all devices with access to the network, on-device/site and cloud software and solutions used, and where different data are located. The information security framework should also include a list of all individuals with access to data, and which data. Should a user credential or a device become compromised, or a solution have a security vulnerability, it can then be quickly removed or segregated from the network.

The information security framework should also include regular audits, from checking that only people that should have access to files have access to them, to confirming all devices run the latest security patches.

As most cybersecurity risks come through errors made by individuals, the information security framework should include training, and simulation of cybersecurity attacks that are run with or without the knowledge of individuals in the organization (e.g. an organization can run a fake phishing campaign as an educational measure), to confirm individuals' preparedness.

To allow for quick mitigation and solutions, the information security management framework should also include an incident response plan with the different measures to be taken. The incident response plan should include reference to any reporting obligations that lawyers may have, such as duties to report security breaches to clients, law societies or insurance providers (see, e.g., Rule 7.1-3, Rule 7.8-1, and Rule 7.8-2) in addition to statutory reporting obligations in provincial or federal data protection legislation.

Within organizations, the framework should include assigning information security as a responsibility to one person (and a deputy in case of incapacity or leave), with the power

to approve or reject usages, answer client and stakeholder questions, and to activate and coordinate an incident response within the organization.

Lawyers should also be aware that, while their professional insurance may cover some issues related to the delivery of professional services, it generally does not cover data loss or breach, lost income or equipment after a cyber-attack, or a natural event. Optional cybercrime or data security insurance may be available in some jurisdictions.

Learn more:

- Canadian Centre for Cybersecurity, *Baseline Cyber Security Controls for Small and Medium Organizations* (February 2020).
- LAWPRO, "Does your firm need cybercrime insurance?", *PracticePRO* (January 1, 2018).
- Lawyers Financial, "Cyber Risk—Is your Law Firm Protected?", *Canadian Lawyer* (September 4, 2018).
- LAWPRO, "The LAWPRO $250,000 cybercrime coverage: What it covers and why", *PracticePRO* (December 1, 2013).
- Law Society of British Columbia, *What to do Before and After a Disaster Strikes*.

3. Working Remotely with Clients, Collaborators and Courts

Adopting remote work practices, such as working from home or from a virtual office, providing remote commissioning services to clients, and attending virtual meetings and hearings, can result in more efficient and accessible services to clients. Moreover, to the extent that remote processes and tools become mandatory or even widely used in certain legal processes and practice areas, their appropriate use can also be characterized as a matter of competence.

Objective: Ensuring that one's professional obligations are met when working remotely

Below are a number of questions to ask in assessing compliance and the potential systems and practices to fulfill said compliance.

Q: When working in a virtual office, are professional obligations in relation to confidentiality and supervision complied with?

Avoid using unsecure public Wi-Fi networks, and ensure use of:

- ✓ Highest level of encryption available on wireless router
- ✓ Strong password
- ✓ Disable guest networks
- ✓ Disable remote administration
- ✓ Change default administration credentials

If confidential data is carried out of the office:

- ✓ Encryption mechanisms should be adopted to secure it during transport;
- ✓ Consider whether it is possible to access information through a secure encrypted or VPN connection as this is safer than carrying files on a laptop hard drive or USB key.

Working on confidential matters in public spaces should generally be avoided but where done take steps to maintain confidentiality by:

- ✓ Using privacy screens on all electronic devices to restrict who can see your screens;
- ✓ Using headphones;
- ✓ Being careful not to speak too loudly.

When supervising colleagues who are working remotely, ensure that they are aware of their confidentiality obligations and best practices when operating in a virtual office.

Q: When engaged in virtual commissioning or witnessing are all applicable legislative and regulatory requirements complied with? Are best practices adopted?

- ✓ Confirm that virtual commissioning or witnessing is permitted in your jurisdiction.
- ✓ Review and follow your jurisdiction's rules and regulations regarding virtual commissioning or witnessing.

Take steps to guard against key risks, including:

- ✓ Fraud and identity theft
- ✓ Undue influence
- ✓ Adverse impacts on client service
- ✓ Verification challenges arising from poor quality or unreliable technology.

Q: Are applicable law society rules and regulations followed if using a virtual means of identifying or verifying the identity of a client?

- ✓ Review your law society's rules regarding client identification and verification rules.

Where client verification rules require "face to face" verification and the relevant law society permits such verification to take place in a virtual meeting:

- ✓ Be alert to potential red flags;
- ✓ If caution is warranted, consider using a different accepted method of verifying identity;
- ✓ If engaging in virtual identity verification (where permitted) consider obtaining a high-resolution image of the identification document prior to the virtual meeting as a reference.

Q: Are best practices for virtual meetings and hearings adopted?

In circumstances where the lawyer has flexibility in choosing a platform:

- ✓ Consider whether the meeting will require true end-to-end encryption;
- ✓ Use access controls such as a password or virtual waiting room.

If considering recording a meeting:

- ✓ Comply with professional conduct rules regarding recording conversations
- ✓ Comply with any applicable tribunal or court rules.

Adopt confidentiality best practices:

- ✓ Where needed, headphones should be used to prevent third parties from listening to the meeting.

Be aware of, and guard against, risks relating to third parties influencing testimony:

- ✓ Ascertain if there is anybody else present with the witness or listening on a device that might be providing the witness with information during the interview.

Q: Is there appropriate understanding of when and how electronic signatures can be used to execute documents?

- ✓ Review legislative requirements before using electronic signatures.

If an electronic signature is permitted ensure:

- ✓ The electronic signature reliably associates the person with the signature, and reliably associates the signature to the document;
- ✓ Security measures have been put in place to prevent unauthorized access, use, or copying.

Considering using best practices, including:

- ✓ Public-key cryptography that is uniquely associated with the document.
- ✓ Adopting more advanced electronic signature systems that include timestamping and fingerprinting of the document through a third party that could attest to the time, authenticity, and integrity of the signed documents.

If the lawyer is using an electronic signature themselves ensure:

- ✓ Access is strictly controlled (lawyers should have full control and knowledge).

Virtual Office

When using a virtual office—either working from home or a location that is not a dedicated office space for their practice—lawyers need to ensure that they take adequate steps to comply with their confidentiality (Rule 3.3-1) and supervision (Rule 6.1-1) obligations.

Virtual Private Networks (VPN) and Remote Desktop Applications can give lawyers a secure way to connect to files and client information. If confidential digital data is physically carried out of a lawyer's dedicated office, encryption mechanisms should be adopted to secure it during transport. When possible, it is safer to access information through a secure encrypted or VPN connection than to carry files on a laptop hard drive or USB key.

When using Wi-Fi networks, lawyers should use the highest level of encryption available on their wireless networks' routers (at least WPA2, if possible WPA3) and use a strong password. They should also disable guest networks and remote administration, as well as change the default administration credentials of their router (often "admin/admin") in accordance with best password practices mentioned earlier. For added security, lawyers should change the public name of their Wi-Fi network and hide it to non-authenticated devices by disabling the broadcasting of their Wi-Fi network's name ("SSID Broadcasting"). Lawyers can also limit the ability of devices to connect to the network by activating "MAC address filtering" which will only authorize a series of specific devices to connect based on their unique identifiers.

Lawyers should remember that if they are able to connect to a Wi-Fi network without a password, the network is unsecured. Lawyers should not use unsecured Wi-Fi to connect to a work server, do banking, or send any type of confidential or personal information.

Lawyers should also ensure that any voice-enabled devices they have, such as smart speakers and virtual assistants, are muted or shutoff when discussing client matters or sharing any other confidential information. Lawyers should consider removing these devices from their workspaces where possible, and from their surroundings when meeting with clients.

Generally, working on confidential matters in public spaces should be avoided, as third parties may be able to view screens and printed documents or overhear conversations. In public settings (shared spaces, coffee shops, trains, airplanes, etc.), lawyers should use privacy screens on all their electronic devices to restrict who can see their screens. Similarly, lawyers should use headphones, and be careful not to speak too loudly to maintain confidentiality.

When supervising colleagues who are working remotely, ensure that they are aware of their confidentiality obligations and best practices when operating in virtual offices. Courts have recognized a risk that virtual working situations can deprive students and junior lawyers of steady and informal contacts with supervising and mentoring lawyers and this can result in inadequate instructions and inadequately reviewed materials being released.[15]

Learn more:

- Ontario Bar Association, *Online Lawyering Checklist* (2020).
- Juda Strawczynski, "Work-from-home Technology Tips", *PracticePRO* (2020).
- LAWPRO, "Beware of cybersecurity risks during COVID-19 and working from home", *AvoidAClaim* (March 20, 2020).
- Law Society of Ontario, "How can I ensure that client confidentiality is protected while working remotely?" (2021)
- Law Society of Ontario, "Do my confidentiality obligations prevent office support staff from working remotely?" (2021)
- Law Society of Manitoba, "What should I consider when working from home?" (2020)
- Crystal Tse and Jonathan Browning, "Locked-Down Lawyers Warned Alexa Is Hearing Confidential Call", *Bloomberg* (March 20, 2020)

Virtual Commissioning and Witnessing

In many jurisdictions, lawyers are now permitted to engage in virtual commissioning, and virtual witnessing is authorized in a few jurisdictions. Virtual commissioning refers to the signing of affidavits and statutory declarations that takes place in a different physical location than the commissioner (i.e. the lawyer) by using audio-visual technology. Virtual witnessing is similarly defined, but references the remote signing of wills and powers of attorney. Different jurisdictions have different rules for virtual commissioning and

[15] *Polgampalage v. Devani,* 2021 ONSC 1157 at paras. 40-43.

witnessing, and some do not allow for virtual commissioning or witnessing. Lawyers need to review and follow the applicable rules in their jurisdiction.

In many instances, permissions for virtual commissioning and witnessing were specifically introduced in response to the COVID-19 pandemic. Although some jurisdictions have indicated an intent to extend the measures post-pandemic, lawyers need to pay particular attention to ensure that they are following the current rules applicable in their jurisdiction.

There are several risks in relation to virtual commissioning. The Law Society of Ontario has identified four major risks and issued practice tips in relation to each risk:

> **Risk 1—Fraud and Identity Theft**
> Where in-person meetings between the commissioner and the client are reduced or eliminated, there are greater risks of fraud and identity theft.

Practice Tip
Consider whether there are red flags of fraud in the matter. To review these red flags, see the Federation of Law Societies' Risk Advisories for the Legal Profession resource.

Risk 2—Undue Influence:
With remote commissioning, there is a greater risk that undue influence will go undetected. The commissioner may not be able to sufficiently assess whether there are any off-screen influences or other persons coercing the deponent.

Practice Tip
Assess whether there is a risk that the client may be subject to undue influence or duress. If there is such a risk, consider if you can assist the client at this time without meeting in person.

> **Risk 3—Reduced Level of Client Service**
> Without safeguards in place, there is a risk that the client is left without copies of documents they have executed remotely. There is also a risk that the client may not feel they have had an adequate opportunity to ask questions or request clarifying information about the documents they are executing, which risk is heightened by the lack of physical proximity.

Determine how to provide the client with copies of the document executed remotely.

Confirm your client's understanding about the documents they are executing and provide adequate opportunity for them to ask questions during the video conference.

> **Risk 4—Technological Limitations/Uncertainty**
> Given varying video quality and network connections, as well as the fact that

> live-streaming video and audio can be manipulated, it may be very difficult for a commissioner to confidently verify the distinct attributes of the document commissioned.

Practice Tip
Use best practice resources to guide and document your remote commissioning process.

Learn more:

- Law Society of Ontario, "Remote Commissioning" (last updated 2020).
- FLSC Anti-Money Laundering and Terrorist Financing Working Group, *Risk Advisories for the Legal Profession* (December 2019)
- Law Society of Ontario, "Is Remote Execution and Witnessing of Wills and Powers of Attorney Permitted in the Context of COVID-19?" (last updated February 19, 2021).
- Law Society of Ontario, "Best Practices for Remote Commissioning" (last updated August 1, 2020)
- Law Society of Ontario, "Remote Commissioning Checklist" (last updated August 1, 2020)
- Law Society of British Columbia, "COVID-19 Response" (last updated January 25, 2021).
- Law Society of Alberta, "COVID-19 FAQs" (last updated November 27, 2020).
- Law Society of Manitoba, "Can I use Virtual Commissioning in the Context of COVID-19?" (last accessed March 14, 2021).
- Law Society of Newfoundland and Labrador, "Guidance to the Membership: Temporary Alternate Witnessing of Documents Act" (May 2020).

Virtual Client Identification and Verification

Lawyers need to ensure that they are complying with the client identification and verification rules in their jurisdiction that have been adopted by law societies in order, notably, to combat money-laundering and terrorist financing.

In response to the COVID-19 pandemic, some law societies have indicated that they will permit client verification, where it is required, to take place in a virtual meeting. However, law societies have also cautioned that virtually verifying client identity should be

considered a "last resort" and lawyers need to be alert to potential red flags (see the FLSC's Risk Advisories for the Legal Profession). As alternatives to virtual identity verification, lawyers should consider other options for verifying identity such as the dual-process method (i.e. referring to two reliable sources), or by reviewing the Canadian credit file to confirm name, address and date of birth. In some cases, lawyers may be able to rely on the previous verification by another person or verification by an agent. If engaging in virtual identity verification (where permitted), lawyers should consider obtaining a high-resolution image of the identification document prior to the virtual meeting as a reference when viewing the original identification document during the virtual meeting. Lawyers should be mindful of privacy or other statutory provisions that may apply to the processing and recording of virtual client identification.[16] It has also been recommended that, if a lawyer does verify client identity through virtual means, the transaction be treated as a high-risk and that the lawyer document the efforts made to verify the client's identity in accordance with the existing rules and the reasons why they were unable to verify the client's identity in accordance with the existing rules.

As with virtual commissioning and witnessing, this is an area where lawyers need to be particularly alert to changing rules and approaches as COVID-19 pandemic restrictions evolve.

Learn more:

- Law Society of British Columbia, "COVID-19 Response" (last updated January 25, 2021).
- Law Society of Ontario, "LSO COVID-19 Response—FAQs: Practice Management" (last accessed January 29, 2021).
- Law Society of Alberta, "COVID-19 FAQs" (last updated November 27, 2020).
- Barbara Buchanan, "Knowing Your Client—Guidance and Rules during Covid-19" Law Society of British Columbia, *Benchers' Bulletin* (Summer 2020).
- FLSC Anti-Money Laundering and Terrorist Financing Working Group, *Risk Advisories for the Legal Profession* (December 2019).
- Law Society of Saskatchewan, "Client Identification and Verification" (last accessed March 14, 2021).
- Law Society of Saskatchewan, Client Identification and Verification (December 19, 2019).

[16] See, e.g., Québec's *An Act to establish a legal framework for information technology*, CQLR c. C-1.1, s. 44 provides that express consent is required prior to verifying a person's identity through a process that allows biometric data to be recorded.

Virtual Meetings, Hearings and Interviews

Virtual meetings, including virtual court hearings, may seem more casual. However, like in any other electronic communication, lawyers are still required to comply with the usual professional conduct rules, notably civility (Rule 7.2-1) and confidentiality (Rule 3.3-1).

In some contexts, a lawyer will not have an option as to what platform is used (e.g. court hearings). Where there is flexibility as to the platform being used, lawyers should consider what security measures are necessary or otherwise prudent to ensure client confidentiality and effective client services and communication (Rule 3.3-1, Rule 3.1-2 and Rule 3.2-1).

In circumstances where a lawyer has flexibility on which platform is used, they should consider whether the meeting will require true end-to-end encryption, where even the software provider will not have access to the content of the conversation. As with email, telecommunication services usually insert clauses in their user agreements that allow them to access the content of your conversations, making 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. Often, the confidentiality of communication is already guaranteed in the paid version of the platforms. As with emails and files, for extremely sensitive communication, lawyers should choose a platform on which they can control the encryption keys.

In any case, access to the virtual meeting room should be subject to access control. A common access control is to require a password for entry to the meeting. Lawyers should also consider using a virtual waiting room, where attendees will log in and wait until they are specifically granted access by the host.

Certain tools allow for the recording of conversations (either audio, video or the chat). Rule 7.2-3 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." 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.

The same goes for court and tribunal proceedings. Court and tribunal rules may prohibit the recording of a proceeding. Even if no restrictions exist, proceedings should only be recorded with the court's knowledge and consent.

If lawyers (and clients) cannot guarantee the confidentiality of their surroundings, headphones should be used to prevent third parties listening in on the meeting. The possibility of third parties being on the other side of a screen of a client or a witness in an interview is something to consider. Especially in case of an interview or witness testimony,

lawyers should ascertain if there is anybody else present with the witness or listening on a device who might be giving the witness information during the interview (while being mindful of the person's privacy and that not everybody can fully isolate themselves).

Lawyers should also be mindful of what can be seen in the background of their video, and ensure it does not disclose any confidential information (e.g. location, client name, ongoing file). A good practice is to direct the camera to a plain or curated background, or to use a virtual background. However, lawyers should also be aware that use of virtual backgrounds can generate risks in certain contexts: e.g. a virtual background could potentially obscure a client's or witness's location, or hide from view individuals who may be improperly influencing a client or witness.

Finally, as in any other meeting, the lawyer should memorialize the meeting immediately after it ends, and to put any instructions received or advice given in writing.

Learn more:

- Law Society of Ontario, "LSO COVID-19 Response—FAQs: Practice Management" (last accessed January 29, 2021).
- The Advocates' Society, *Best Practices for Remote Hearings* (May 13, 2020).
- LawPRO, "Ten Tips for Effective Video-Conferencing", *PracticePRO* (April 8, 2020).
- LawPRO, "Video Conferencing Checklist" *PracticePRO* (March 2020).
- Ontario Superior Court of Justice, "Best Practices and Etiquette for Remote Hearings" (2020).
- CBA British Columbia Branch, *Best Practices in a Zoom Courtroom* (2020).
- Law Society of British Columbia, "Video Conferencing Technology Information" (last accessed March 14, 2021).
- Law Society of British Columbia, "Risks and Tips when using Video-Conferencing Technology" (last accessed March 14, 2021).

Electronic Signatures

Electronic signatures can be used to ensure the authenticity, non-repudiation and traceability of documents. Whether an electronic signature is permitted is a substantive issue governed by provincial and territorial legislation as well as any applicable court rules and practice directions. Lawyers need to review legislative and other applicable

requirements before using electronic signatures. Even if a jurisdiction permits electronic signatures in certain contexts, it may not permit them for all documents.

Assuming an electronic signature is permitted, some best practices should be followed. An electronic signature needs to reliably associate the person with the signature and reliably associate the signature to the document. The very definition of an electronic signature varies from one jurisdiction to the next. Across jurisdictions, an electronic marking is generally considered a legitimate signature in the business context. This is usually the most cost-effective option but reliability concerns might be raised because the links between the signatory and document can create plausible deniability along with a heightened risk of fraud. A digital signature can facilitate verification that a signature took place. When authentication and documentation are essential (e.g. when notarizing documents), lawyers should consider using more advanced electronic signature systems that include timestamping and fingerprinting the document through a third party that could attest to the time, authenticity and integrity of the signed documents.

Access to electronic signatures, from the simplest to most advanced ones, should be strictly controlled. Lawyers should have full control and knowledge as to how, when and to whom their proof of signature is shared and therefore guarantee protections to the client's privacy and security, since everything is in the lawyer's control. If you use an electronic signature, you should ensure that security measures have been put in place to prevent unauthorized access, use or copying.

Learn more:

- Law Society of Ontario, "LSO COVID-19 Response—FAQs: Practice Management" (last accessed January 29, 2021).
- Peter A. Aziz, Marissa Daniels and Hailey Schnier, "Canada : COVID-19 And Electronic Signatures: A Guide for Organizations", *Mondaq* (June 14, 2020).
- LAWPRO, "Understanding e-signatures", *PracticePRO* (June 2, 2020).

4. Lawyers' Online Presence

Many lawyers have an online presence in the form of law firm websites or social media accounts. Some lawyers also use email for marketing purposes, in addition to using email to communicate about legal matters. When marketing through online means, lawyers must ensure that they are complying with the applicable ethical rules relating to lawyer marketing. (see Rule 4.2) It is also prudent for lawyers to take steps to guard

against conflicts of interest that can be generated if a prospective client sends unsolicited confidential information. Lawyers must also follow applicable legislation and governing body rules and regulations on unsolicited commercial emails, such as Canada's Anti-Spam Legislation.

Increasingly, lawyers have an online presence through social media platforms. A lawyer's use of social media is subject to law society marketing rules but can also raise unique risks relating to client confidentiality and civility that lawyers should be aware of and take steps to avoid.

Finally, in creating their online presence, lawyers should be aware of and adopt best practices in relation to accessibility. In some jurisdictions, there are statutory requirements on accessibility that are relevant to lawyers.

Objective: Maintaining an ethical and otherwise appropriate online presence

Below are a number of questions to ask in assessing compliance and the potential systems and practices to fulfill said compliance.

Q: Are appropriate measures taken to make sure electronic communications are accessible?

- ✓ Any online professional presence should follow the Web Content Accessibility Guidelines (WCAG) 2.0, notably making sure all content is fully readable in text (including images).

Q: Are applicable professional conduct rules followed when engaging in online marketing?

Any online marketing should:

- ✓ Be demonstrably true, accurate and verifiable;
- ✓ Not be misleading, confusing or deceptive, nor likely to mislead, confuse or deceive;
- ✓ Be consistent with a high standard of professionalism.

Lawyers should be aware that the following practices may contravene law society marketing rules:

- × 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.

Q: Are measures taken to avoid receiving unsolicited confidential information or materials or otherwise inadvertently creating lawyer-client relationships or the impression thereof?

- ✓ Include terms of use and disclaimer statements that warn site visitors to refrain from sending unsolicited information or materials to the firm or leaving confidential information on voicemail; and that access to or use of the firm's site or voicemail does not create a lawyer-client relationship.

- × Avoid answering specific legal questions or otherwise providing legal advice on social media.

Q: Is any use of social media consistent with a lawyer's ethical obligations in relation to confidentiality, integrity, courtesy, discrimination and harassment and encouraging respect for the administration of justice?

- ✓ Clients or client matters are not mentioned in social media posts, either directly or indirectly, without client consent.
- ✓ Caution is taken before using social media platforms to communicate or otherwise connect with clients.
- ✓ Do not post discriminatory material or material that amounts to harassment.
- ✓ With respect to civility obligations, exercise judgment before engaging in criticism of other lawyers or the judiciary.

Q: When sending marketing emails, are the requirements of Canada's Anti-Spam legislation and regulations complied with?

- × No commercial electronic message should be sent to a third party without their prior consent.

- ✓ Commercial electronic messages must provide the identity and contact information of the person who sent the message and, if applicable, of the person on whose behalf it is sent; set out an unsubscribe mechanism, at no cost and as easy as the subscription mechanism.

Web Content Accessibility

Websites and web content can pose access challenges to persons with disabilities. For example, accessibility issues commonly arise when documents are formatted using styles that impede accessibility for individuals using assistive devices like screen readers.

All public communications by lawyers should be accessible and follow accessibility best practices such as the Web Content Accessibility Guidelines (WCAG) 2.0 issued by the World Wide Web Consortium (W3C) (ISO/IEC 40500). In some provinces, this is now a statutory requirement (e.g. in Ontario, as of January 1st, 2021, all firms of more than 50 employees shall respect those guidelines).

Learn more:

- W3C, "Web Content Accessibility Guidelines (WCAG) Overview" (last updated October 17, 2020).
- Government of Ontario, "How to Make Websites Accessible" (last updated October 19, 2020).
- ARCH Disability Law Centre, Tips for Lawyers and Paralegals on Providing Accessible Legal Services to Persons with Disabilities in Ontario (January 2019).

Law Society Marketing Rules

When engaged in online marketing—either through law firm websites, social media accounts or emails—lawyers need to comply with their professional code of conduct rules. Many jurisdictions have adopted Rule 4.2-1 of the *Model Code*, which states that a lawyer's marketing must be: (a) demonstrably true, accurate and verifiable; (b) neither misleading, confusing or deceptive, nor likely to mislead, confuse or deceive; and (c) in the best interests of the public and consistent with a high standard of professionalism.[17] Rule 4.3-1 also says "[a] lawyer must not advertise that the lawyer is a specialist in a specified field unless the lawyer has been so certified by the Society."[18] It is also recommended that where lawyers make representations in generally accessible electronic forums or formats, they should include the name, law firm mailing address, licensed jurisdiction of practice, and email address of at least one lawyer responsible for the communication.

[17] For law society disciplinary cases deal that with Rule 4.2-1 in the context of a lawyer's online presence, see, for example, *Law Society of Ontario v. Goldfinger*, 2018 ONLSTH 10, appeal allowed in part 2020 ONLSTA 3; *Law Society of Ontario v. Weinles*, 2018 ONLSTH 105; and *Law Society of Ontario v. Forte,* 2019 ONLSTH 9

[18] For law society disciplinary cases that engage with Rule 4.3-1, see, for example, *Law Society of Ontario v. Goldfinger,* 2020 ONLSTA 3 and *Law Society of Ontario v. Mazin,* 2019 ONLSTH 35

This is an area, however, where lawyers should have regard to the relevant rules in their jurisdiction. For example, the Law Society of Ontario's *Rules of Professional Conduct* have additional commentary on the use of awards, rankings and third-party endorsements in lawyer marketing, and specific requirements when advertising a price to act on a residential real estate transaction.

Learn more:

- Law Society of Ontario, "Technology", *Practice Management Guidelines* (last updated 2020).
- Law Society of Alberta, "Effective and Ethical Advertising" (last accessed March 14, 2021).

Avoiding Inadvertent Lawyer-Client Relationships

Receiving confidential information from an individual through a law firm's website, email or a social media account can trigger conflict of interest issues even if the individual does not become a client. Relatedly, because a lawyer-client relationship can be established without a formal retainer (see, e.g., Rule 1.1-1, definition of "client"), lawyers also need to take care that their online presence does not inadvertently create a lawyer-client relationship or give an individual the impression that it does.

To avoid problems, lawyers should consider including, on their websites, terms of use and disclaimer statements that warn site visitors to refrain from sending unsolicited information or materials to the firm or leaving confidential information on voicemail; and that access to or use of the firm's site or voicemail does not create a lawyer-client relationship. To avoid the inadvertent creation of lawyer-client relationships, lawyers should also take care not to answer specific legal questions on social media platforms.

Learn more:

- CBA, "Avoiding Phantom Clients", *Conflicts of Interest Toolkit* (2020).

Ethical Issues Arising from Social Media Use

When using social media, lawyers need to take care not to reveal confidential client information (Rule 3.3-1). Obviously, explicitly referring to clients and client matters should be avoided. Additionally, as noted in professional conduct rules, a lawyer "should avoid indiscreet conversations and other communications … about a client's affairs and should shun any gossip about such things even though the client is not named or otherwise

identified" (Rule 3.3-1, Commentary [8]).

Lawyers should also be aware of risks related to social media use and the inadvertent disclosure of confidential client information. For example, messaging services offered by social media platforms are generally not secure and caution should be taken before using the services to communicate with clients. Additionally, by connecting with a client through social media—by, for example, "friending" or "following" a client—it is possible that the client's retention of a lawyer's services will be inferred. Lawyers should guard against social media applications viewing or publicizing to others their contact lists in their electronic devices, as this can also amount to a breach of confidentiality.

Several features of social media—the relative informality, speed of communications, and potential blurring between the personal and the professional—can also generate risks for lawyers in relation to their civility obligations (see, e.g., Rule 7.2-1 and Rule 7.2-4). It is now well known that social media platforms can, at times, be sites of extreme conflict and unnecessarily rude and even discriminatory or harassing comments. At the same time, it is also well recognized that law societies must consider the expressive freedom of lawyers when regulating lawyer civility and that lawyers have an important leadership role to play in educating the public and seeking improvements in the legal system.

For example, as noted in Rule 5.6-1, a lawyer has an obligation to "encourage public respect for and try to improve the administration of justice." The Commentary to this Rule further elaborates that "[a] lawyer, by training, opportunity and experience, is in a position to observe the workings and discover the strengths and weaknesses of laws, legal institutions and public authorities … [and] should, therefore, lead in seeking improvements in the legal system, but any criticisms and proposals should be bona fide and reasoned." It should also be noted, however, that, under Rule 5.6-2, "[a] lawyer who seeks legislative or administrative changes must disclose the interest being advanced, whether the lawyer's interest, the client's interest or the public interest."

A lawyer should also have regard to Rule 7.5 ("Public Appearances and Public Statements") and the commentary thereunder which states, among other things, that "[a] lawyer's duty to the client demands that, before making a public statement concerning the client's affairs, the lawyer must first be satisfied that any communication is in the best interests of the client and within the scope of the retainer" and that "[p]ublic communications about a client's affairs should not be used for the purpose of publicizing the lawyer and should be free from any suggestion that a lawyer's real purpose is self-promotion or self-aggrandizement."

As such, lawyers should not be afraid of participating in social media discussions, including those which involve controversial matters. At the same time, care needs to be

taken and judgment needs to be exercised with a view to acting consistently with one's professional obligations in relation to confidentiality, integrity, civility and discrimination and harassment. In terms of specifics on the balance to be struck, it has been recently suggested that lawyers "should avoid posting critical comments about an identifiable opposing counsel on social media" or refrain from "engag[ing] in personal attacks on the judiciary or unfairly criticize judicial decisions in their public statements, including on social media."

Learn more:

- The Advocates Society, *Principles of Civility and Professionalism for Advocates* (February 20, 2020).
- Robyn Schleihauf, "Conduct Unbecoming: What should the Society do when it comes to gossip, online posts and bad behaviour on social media?", *Nova Scotia Barristers Society* (February 2020).
- EPIQ, "Social Media Ethical Obligations for Lawyers" (2019).
- State Bar of Michigan, "Ethics of Social Media—LinkedIn Frequently Asked Questions", (May 2017).
- ABA, "The Minefield of Social Media and Legal Ethics" (March 24, 2017).
- Stacey McPeek, "Lawyers and Social Media", *Law Society of Saskatchewan* (February 8, 2017).

Unsolicited Email Messages and Anti-Spam Laws

When sending emails or other electronic messages, lawyers should also be familiar with the requirements of *Canada's Anti-Spam Legislation* that apply to electronic messages with commercial purposes, notably messages that offer to provide services, and advertise or promote such services, or a person who provides such services. No commercial electronic message should be sent to a third party without their prior consent. While consent should usually be express, it can be implied if there is an existing business relationship, or if the recipient posted their contact information online, or directly to the sender, without mentioning they did not wish to be solicited. Beyond consent, the message must state the identity and contact information of the person who sent the message and, if applicable, of the person on whose behalf it is sent; and set out an unsubscribe mechanism, at no cost, that is as easy as the subscription mechanism.

Learn more:

- "*Canada's Anti-Spam Legislation*", SC 2010, c. 24.
- ISED, Canada's Anti-Spam Legislation Resource Centre (last updated April 21, 2020).
- Ava Ghisling, "What's it all about? How anti-spam legislation can affect your firm?", *CBA Practice Link* (March 18, 2019).