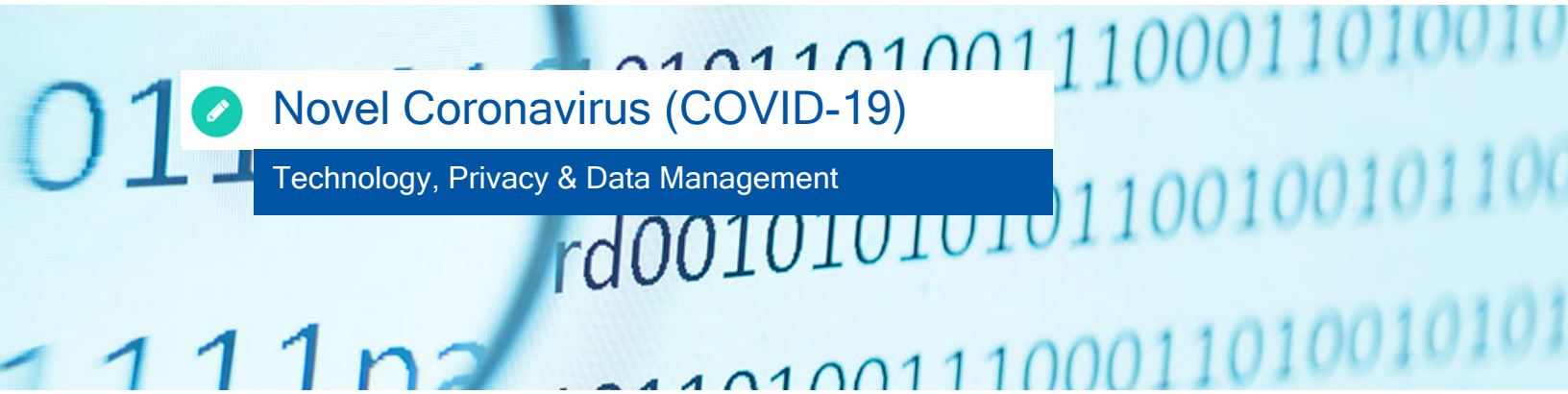
Torkin Manes
Barristers & Solicitors



Novel Coronavirus (COVID-19)

Technology, Privacy & Data Management

May 2020

Lawyering in the time of pandemic

Working from home and using videoconferencing services means lawyers must be more vigilant than ever

By Lisa R. Lifshitz

In July I wrote a column for *Canadian Lawyer* in which I argued that, as a basic tenet of our profession, Canadian lawyers should actually be required to have a minimum understanding of technology, privacy and cybersecurity in order to adequately serve their clients.

While there still no mandatory legal duty of technological competence required of lawyers by our law societies, Canadian lawyers practising law during this time of pandemic now have an even greater duty to understand and deploy the necessary technological measures and practices to protect client data from unwanted intrusion.

In Ontario, s. 3.1.1. of the Rules of Professional Conduct sets out the various positive duties of competence that lawyers are supposed to possess. For example, a "competent lawyer" means a lawyer who has and applies relevant knowledge, skills and attributes in a manner appropriate to each matter undertaken on behalf of a client, applying appropriate legal skills, pursuing appropriate professional development to maintain and enhance legal knowledge and skills, and otherwise adapting to changing professional requirements, standards, techniques and practices.

As I discussed in a recent column, the global ascendance of COVID-19 has only spurred the activities of phishing, malware and ransomware attacks. Rob Lefferts, corporate vice-president of Microsoft 365 Security, reported in an April 8, 2020 blog that every country in the world has seen at least one COVID-19-themed attack with China, the United States, and Russia have been hit the hardest.

Given the heightened security risks of working during a pandemic, technological competence must be read into the "duties of competence" that lawyers are supposed to possess, even if our regulators haven't caught up with this new reality.

What does technological competence look like for lawyers practising during a pandemic?

First and foremost, lawyers must ensure they have in place reasonable physical measures to protect client data against unauthorized access. Technology containing client data should be braced against the increased threat of third-party hackers and malware by using firewalls, encryption tools, up-to-date anti-virus technology/URL threat protection, and other security software. Outdated legacy software and free, unsupported versions of software should be shelved, and all security patches and updates received from vendors should be implemented in a timely fashion. Lawyers should also always access critical networks using dedicated VPNs and secured Wi-Fi.

Additionally, lawyers wishing to protect their clients should consider the following tips.

Zoom wisely. Videoconferencing has been a boon to organizations that have traditionally relied on face-to-face meetings to get things done, but as anyone following recent headlines regarding the vulnerabilities of videoconferencing services can attest to, it is not without privacy or security risks.

The Office of the Privacy Commissioner of Canada (OPC) recently provided a series of privacy tips for using videoconferencing services. For example, the OPC recommends that users that sign up for a new videoconferencing account should use unique passwords and not existing social media accounts to sign into a new service. Meetings should be made private or only accessible to invited participants, and not publicly posted to social media in order to help ensure unwanted guests are prevented from joining. Disable features such as "join before host," screensharing or file transfers to minimize the threat of "Zoombombing," gatecrashing and more. Video conferencing calls should be protected with a password, if possible, especially if the parties intend to discuss sensitive personal information. Each call should have its own password to prevent unwanted participants from joining, and lawyers who host should consider disabling participants' ability to record the call.

Other useful advice from the OPC includes being careful about where one sits during the call, as background can reveal information that you may not want to share. Anyone using a web browser for the video call should open a new window with no other browser tabs and close other applications to avoid inadvertently sharing notification pop-ups (e.g., incoming emails) with other participants and the videoconferencing service provider. All personal home assistants (e.g., Alexa, Siri, Google Home) and smart speakers should be turned off during videoconference to avoid accidentally triggering the assistant and/or recording the call.

Retain and dispose of confidential information securely. Now is not the time to toss out highly sensitive client confidential information with your used coffee grounds and pet litter. Significant data breaches have occurred when documents containing health and other personal information were found tumbling around alleyways and on city streets. Sensitive information should be securely stored in locked cabinets, boxes or otherwise. Invest in a decent home shredder and use it. Period. Or, save all of your confidential information until you can return it your office to be disposed of securely.

Have adequate (and secure) backup. It's critical for lawyers and their firms to invest in the acquisition of professional backup, recovery and restore software, and to establish a relationship with reputable backup/data recovery providers, so that if confidential or client data is lost the organization can seek to recover it with a minimum of panic and fuss. Law firms and lawyers should never rely on free backup software downloads to protect sensitive client data. As not all backup and restore software is created equal, lawyers should choose vendors whose software i) can verify that the backups do not contain malware or other viruses, and ensure that any restored files are clean to forestall additional infections; ii) has two-factor authentication enabled to prevent credential theft leading to unlawful access and deletion of backup data; and iii) has the backup data stored on immutable storage media.

Develop and maintain data/cyber breach incident response plans. All law firms should ensure that they have privacy/cybersecurity incident response plans in place that identify the contact information for the individuals/committee initially tasked with investigating/containing/managing the breach, and engaging in risk evaluation and mitigation practices. If you do inadvertently expose client data you will need to know who to contact internally, as it's much too late to try to figure this out in the middle of the incident. To avoid the loss of valuable time, this incident response plan should be crafted in advance and approved by firm management, and all lawyers and staff should be made familiar with it. It's also critical to have such a plan in place to forestall internal confusion that may lead to inadvertent disclosures of such incidents on social media or elsewhere.

It is worth reminding lawyers that law firms may have to comply with mandated, time-sensitive reporting obligations to federal and provincial privacy regulators, and potentially other regulators, individuals and third-party organizations. Additional service providers such as security cybersecurity experts, credit monitoring services and media firms should also be retained in advance. Plans should be reviewed at least yearly and updated as required in order to stay current. Smaller firms and solo practitioners should adopt modified versions of these plans as relevant to them.

Regardless of whether lawyers are now formally obliged to check off one more box on their yearly law society annual reports, one may argue that lawyers today already have a positive and meaningful duty of technological competence. Our clients deserve nothing less.

This article was originally published in Canadian Lawyer magazine.

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the immediate past president of the Canadian IT Law Association.