Asper Review of International Business and Trade Law

VOLUME XXI
2021

SPECIAL EDITION:
CYBSERCURITY AND
LAW FIRMS

ASPER REVIEW OF INTERNATIONAL BUSINESS AND TRADE LAW

VOLUME XXI
2021

SPECIAL EDITION:
CYBERSECURITY AND LAW FIRMS

PUBLICATION INFORMATION

Copyright © 2021 Asper Review of International Business and Trade Law
ISSN 1496-9572
Cite as (2021) XXI Asper Rev Int'l Bus & Trade L
Printed on recycled and acid-free paper.
Published annually on behalf of the Faculty of Law, University of Manitoba.
Printed in Canada.

Annual Subscription Rate: Canada: $56.00 CDN; Foreign: $56.00 U.S.

Back issues available from:

Asper Review of International Business and Trade Law
4th Floor Robson Hall, Faculty of Law
University of Manitoba
Winnipeg, Manitoba R3T 2N2
E-mail: asperreview@gmail.com

ACKNOWLEDGEMENTS

The *Asper Review of International Business and Trade Law* gratefully acknowledges the support of the Asper Chair of International Business and Trade Law and the Canadian Credit Management Foundation. The *Asper Review* is equally appreciative of its patrons in the legal community. Appreciation is also extended to the plethora of anonymous internal and external referees who were generous with their valuable time and insights.

THE ASPER CHAIR OF INTERNATIONAL BUSINESS AND TRADE LAW was established in 1999 at the Faculty of Law of the University of Manitoba. Its mandate includes teaching, research and publication.

INFORMATION FOR CONTRIBUTORS

Manuscripts and communications should be directed to:

Editor-in-Chief
Asper Review of International Business and Trade Law
466 Robson Hall, Faculty of Law
Phone: 204.474.6159
University of Manitoba
Fax: 204.480.1084
Winnipeg, Manitoba R3T 2N2
E-mail: asperreview@gmail.com

EXTERNAL PEER REVIEW PROCESS

All the articles in the *Asper Review of International Business and Trade Law* are externally refereed by independent academic experts after being rigorously peer reviewed by Manitoba faculty editors, as well as reviewed by student staff.

The authors chose to publish this material in the Asper Review of International Business and Trade Law and thereby enhance the ability of legal academics and students throughout the world to find and access through the specialized databases that are routinely used for scholarly publications.

This is an area where law and practicalities evolve rapidly. We used the beginning of 2020 as our cut-off for trying to keep up with developments, as time was needed to complete the peer-review and editing process, and like almost everyone, we were delayed in this respect by COVID related lockdowns. The authors hope that this contribution will encourage and assist others to comment on developments in this area, and that other others, including those with a scholarly connection, will embrace the opportunity to provide commentary in a format that is free and readily accessible to the Canadian public.

LEGAL DISCLAIMER

This is a generalised discussion of legal issues; it is not intended as legal advice for any person. Legal advice with respect to any problem depends on specific circumstances at any given time. As such, for advice with respect to one's particular person's circumstances, one should contact a qualified professional in the relevant jurisdiction.

The information in this book is current as of January 1st, 2020, the authors cannot guarantee that changes to applicable laws and guidelines have not occurred since this time.

CYBERSURITY AND LAW FIRMS

DR. BRYAN P. SCHWARTZ

MONICA ADELER

MIKE MYSCHYSHYN

ROBERT WALICHNOWSKI

About the Authors

Bryan Schwartz has been a member of the Faculty of Law at the University of Manitoba since 1981, and in 1999 became the inaugural Asper Professor of International Business and Trade Law. He is also an author/contributor of 27 books and has over 200 publications in all.

Monica Adeler is an associate lawyer at Wolseley Law LLP.

Mike Myschyshyn is a student-at-law currently pursuing his J.D. at the University of Manitoba.

Robert Walichnowski is an associate lawyer at Gange Collins who primarily practices in the areas of civil litigation and administrative/regulatory law.

CONTENTS

Preface

Several years ago, I came across an American Bar Association guide to cybersecurity for lawyers. It occurred to me that there should be a Canadian equivalent. With the help of my student co-authors, we have attempted to do just that by providing and collating expertise on a wide range of matters, some background information about the security issues involved, and information about the legal norms implicated. We do not presume to offer legal advice as counsel about any particular situation, but rather compose a reference work that can help both lawyers and citizens better recognize and manage various cybersecurity issues. The overall perspective embodied in this book is briefly stated in this preface:

A key aspect to our overall approach is that lawyers consider the whole range of professional obligations and legal norms bearing on cybersecurity issues, as opposed to a narrowminded perspective. Client privacy and security are legally protected and morally compelling, but there are trade-offs with other norms – for instance, the ethical duty to serve a client efficiently and effectively. Near-perfect cybersecurity might be achieved by avoiding the use of emails or text messages to contact a client; however, it would then be difficult to communicate on a timely and effective basis with many clients. Furthermore, there may be some added security risks when a lawyer working at home is able to access their office computer remotely but prohibiting such access might then interfere with the lawyer's ability to serve the client's needs, especially urgent ones. Security might be enhanced by limiting information to a few key personnel, but if those personnel quit, become ill or die, the organization may find that information becomes inaccessible to itself as well as potential wrongdoers.

Sometimes security norms are in tension with other norms including those under law society rules requiring retention of client files (for purposes such as holding lawyers accountable in case of client complaints).[1]

---

[1] The Supreme Court of Canada has relieved lawyers of another source of tension; it found that lawyers are constitutionally exempt from duties to make confidential

The challenge for a lawyer is to recognize all the applicable norms involved in addressing cybersecurity and use the necessary ingenuity to comply with all of them to every reasonable extent.

Another dimension of the overall approach recommended in this volume is to view cybersecurity in the framework of risk management generally. A sophisticated literature in risk management in many contexts alerts us to the need to address the following dimensions of a challenge:

Risk assessment: what and where are the actual risks involved? Without a systematic assessment, a lawyer may overlook some traps, such as disposing of printers or photocopies that still retain information, or not recognizing the risks involved with allowing employees to insert and remove flash drives in their system.

Avoidance: what activities should be avoided altogether? A lawyer might decide that using unsecured wireless networks (e.g, those at airports) carries risk that are likely to occur, are serious in the damage they cause, and that various risk-management measures, such as trying to prevent interception by encrypting messages, are too costly or ineffective. An analogy to driving might be to never drive at night in a snowstorm, but that driving in the daytime during a moderate rain may be tolerable if the car is equipped with windshield wipers and quality tires.

Prevention: a lawyer who communicates with clients via email should make sure that the messages are encrypted and sent through secure networks. A lawyer could invite experts to engage in "ethical hacking:" tests to determine if there are security weakness in a system, followed by taking steps to prevent these weaknesses from being exploited by an unauthorized person. An analogy with driving a car might be to ensure that the car you are driving is mechanically inspected and fit for the road and contains all the reasonable affordable accident-avoidance technologies (such as warning signals when another car is in the driver's blind spot).

Mitigation: breaches of security can still occur, even with reasonable prevention efforts. Mitigation efforts include regular monitoring of systems to try to detect breaches and setting up systems that provide various lines of defense, so that even if there is a limited breach somewhere, the rest of the system remains safe. For example, with a properly deployed mitigation strategy, if a single employee is phished, the hacker might be able to see some

---

disclosure of client information under laws dealing with money laundering and financing of terrorism. *Canada (attorney General) v Federation of Law Societies of Canada*, 2015 SCC 7

information that the employee is currently using, but not access the majority of data held at a workplace.

Risk-sharing: lawyers can consider sharing the risks with companies that sell dedicated cybersecurity insurance, as well as other kinds of insurance. Firms providing such insurance might be a useful source of guidance and feedback in managing risk. Another way to share risk is to obtain the informed consent of clients for procedures used by the lawyer. A retainer agreement might, for example, identify what kind of communications will be used. Such an agreement should be tailored to limit the lawyer's liability to security breaches that resulted from the use of technology not agreed upon or contemplated by the client.

A third dimension of the approach recommended here is that lawyers should see cybersecurity as a challenge involving all aspects of their office, including human resources, and not relegate the issues to information technology (IT) experts. A highly sophisticated IT-based security system may be catastrophically compromised by an employee who is phished, or who uses a cell phone to screen-capture sensitive information, or who saves data on a removable flash drive, or who prints a hardcopy and sneaks it out of the office.

A fourth dimension of the challenge is to recognize that cybersecurity is analogous to warfare; it involves a struggle with intelligent opponents who are constantly looking for new ways to exploit technology users. There are many paradoxes in warfare. Initial success can lead to overextended supply lines and a failure to critically evaluate operations to date so as to obtain even better performances; initial failure can increase the desperation of the defender, teach critical lessons for the long run, and create a compact space for operations in which logistics and maneuver is facilitated. In the cyberworld, an apparent step forward can produce surprising and negative effects and countermeasures. Making a back-up of data may help to preserve it against accidental or willful corruption, but every back-up copy is another thing to be potentially hacked. Using fingerprints or eye scans may seem more secure than having staff think of passwords and trying to remember them, but what if a malfeasor makes a copy of someone's fingerprint or retinal image? You can change a password more easily than your fingerprint or retina. A good way to keep on top of security risks is to engage in "war games;" invite an expert "ethical hacker" to have a go at uncovering the vulnerabilities in your system.

We recognize how quickly the law and technology develops in the area of cybersecurity. We hope that this book can be steadily updated and hope that other members of the legal community can help us do so. We have made this book open access and as such, we invite our readers to send us comments or even articles in specific areas so we can try to update this book from time to time (as well as fixing any errors or omissions).

Introduction

Technological progression in many industries is evolving at an exponential rate and will probably continue to do so in the near future.[2] The growth rate of the IT sector is no exception to this trend.[3] IT enables more efficient data management through the use of computational methods. Indeed, technology can streamline mundane business protocols and provide convenient business practices for the client and the corporation. Paradoxically, new methods to exploit sensitive information managed by organizations are being developed as well. Though there are a few areas that have been the aim of data threats, the legal industry is emerging as a major target of cyber-related data exploitation.

Technology has created new dilemmas and paradigms for the legal profession. The ethical obligation of the lawyer to keep "abreast of developments" in new technology in order to maintain a reasonable degree of competence can seem to be at odds with the obligation of confidentiality in the context of preserving the integrity and privacy of a client's information. Using any information technology to communicate with the client and to store their data exposes the legal practice to potential cybersecurity risks. On the one hand, lawyers have embraced technology to serve the client more efficiently, and on the other hand those technologies bring new cybersecurity risks to the duty of maintaining confidentiality and privacy of the client's information.

Most technology comes with embedded risks to cyber threats that lawyers have to assume. There is no perfect solution to cybersecurity issues because there is no such thing as perfect technology. By adopting risk management techniques and best practices, legal practitioners can avoid

---

2 Bela Nagy et al, "Statistical Basis for Predicting Technological Progress" (2013) 8:2 PLoS ONE e52669.

3 "IT Industry Outlook 2019" (January 2019), online: *CompTIA* <https://www.comptia.org/resources/it-industry-trends-analysis> [perma.cc/5RXE-LDAX].

certain cybersecurity risks, reduce others, and mitigate losses when a cyber breach inevitably does happen. Doing so will make a firm more efficient and will help to ensure legal staff comply with their professional obligations. The paradoxical nature of cybersecurity makes it difficult to propose a one size fits all approach to computer security. Rather, the general concepts and strategies discussed here should offer a foundation for readers to build a cybersecurity management plan specific for the needs of their own firm.

It is important to think carefully about a suitable cybersecurity management plan. Too often do businesses react instinctively, without deliberation, to get the deal done. One must approach the issue of cybersecurity in a rational manner, keeping note that it is an issue of human vulnerability as much as it is one of technological vulnerability. Critical planning is the first step in avoiding the systematic bias of unplanned decision making.[4] Upper management that is well organized can thoughtfully design strategies that will improve the security of technological methods used within a firm and also train staff to avoid the psychological tricks played by hackers.

This research first explores current cybersecurity problems that have co-evolved along with the development of technology. Various cyber threats are categorized with a discussion of why lawyers, in particular, are attractive targets to such threats. Next, the costs of cybersecurity breaches for legal professionals, both financial and in terms of reputation damage, are analysed. Various professional and ethical obligations require lawyers to take cybersecurity into account. Moreover, the failure to protect certain types of data can result in the breach of various privacy statutes, exposing one to a number of remedial penalties. Lastly, a practical guide on how law practitioners should deal with cybersecurity issues is presented. A number of possible solutions to protect lawyers' practices and clients' data and privacy are explored including risk management techniques. Overall, this manuscript offers specific insight on cybersecurity issues that lawyers face within Canada in response to the increasing cybersecurity threats to which the legal profession is exposed.[5]

---

4 Daniel Kahneman, *Thinking, Fast and Slow*, (New York: Farrar, Straus & Giroux, 2011).

5 For a cybersecurity handbook targeted towards the American legal professionals, see: Jill Deborah Rhodes & Vincent I Polley, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* (Chicago: American Bar Association, 2013) [*ABA Handbook*].

CHAPTER I: Understanding Cyberattacks and Breaches to Cybersecurity

The purpose of this chapter is twofold. First, it illustrates the scale and scope of the cybersecurity problem for the lay audience, namely that the increasing reliance upon information technology has exposed the modern workplace to an increasing number of threats from any number of vectors, including competitors, cybercriminals, hacktivists, nation-states, and disgruntled employees. The second purpose is to demonstrate how vulnerable some of these systems are to malfeasance and to expose the heightened risk law practitioners face by virtue of the information they come to possess during the ordinary course of practice.

I. INTRODUCTION

The commercialization of the information technologies in the 1990's introduced the Internet to the business world and regular households, creating myriad benefits for people around the world. Cost efficiencies, increased productivity, elimination of distances in communication, access to a vast amount of information, and flexibility in an ever-changing environment are some of the advantages of IT. An important feature of the Internet was its openness in its structural design through the flexibility of communication protocols, and in its social/institutional organization that allowed for constant improvements to the technology. The Internet's early beginnings in American universities in the 1960's and 1970's amidst a "culture of freedom" contributed to the idea of using computer networking as a tool of free communication and political liberation. However, the initial claims of freedom, openness, accessibility and flexibility that the information technologies purported to provide to society have been a double-edged sword. While the benefits of the Internet are undeniable, its

risks and vulnerabilities such as cyberwar, cyberespionage and cybercrime remain, to a large extent, unsolved.

In the 1990's and early 2000's, most computer and Internet security problems were due to human error in defective computer configuration, employee misdemeanour, and to a lesser extent random individuals trying to test government defences.[6] Those few attacks had limited impact and did not target corporations or law firms specifically.[7] However, as the use and versatility of IT has grown, so too has the vulnerability of corporations and law firms through cyber-attacks which have become more sophisticated, organized and systematic. In a speech at Stanford University, former U.S President Obama, pointed out that "it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm."[8] The majority of services, such as financial systems, the power grid, health systems, administration, and the military run on networks connected to the Internet, which have created significant benefits to society but leave us vulnerable to attacks as never before.

The paradoxical nature of cybersecurity is a recurring concept throughout this manuscript. As Edward Luttwak elegantly demonstrates in his book, "Strategy: The Logic of War and Peace," conflict is riddled with paradox.[9] Improving cybersecurity is a game of strategy. Much like military tactics, the goal of cybersecurity is to outwit the opponent. Employing non-canonical cybersecurity strategies can give a firm an edge over hackers. Such methods introduce the element of surprise, making it more difficult for hackers to discover valuable information. This may require one to employ cybersecurity strategies that are inconvenient. A firm must consider the inconvenience associated with particular cybersecurity methods and choose to employ the tech methods that display a suitable balance between security and efficiency that is best for the particular needs of the business.

---

6 *Ibid.*

7 *Ibid.*

8 "Remarks by the President at the Cybersecurity and Consumer Protection Summit" (13 February 2015), online: The White House <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit> [perma.cc/PS33-LRJX].

9 Edward N Luttwak, Strategy: The Logic of War and Peace (Cambridge: The Belknap Press of Harvard University Press, 2001).

Much attention has been devoted to governments and large corporate groups suffering from cyber-attacks while less attention has been given to consumers and small firms who are regularly affected by cyber threats.[10] Many cyber breaches go unreported, either due to their small magnitude or the fact that companies fear the consequences of a tarnished reputation. Companies are exposed to having trade secrets, business strategies and intellectual property stolen. People shop, pay bills, bank, and manage their private information online at the click of a mouse, something that was unthinkable a few decades ago. Although convenient, these benefits put consumers at risk of identity theft, which can damage one's credit score and personal reputation.

New information technologies have created unprecedented challenges for legal professionals. Law firms have become attractive targets for cyberattacks as lawyers have access to and store clients' confidential information. Several prominent Bay Street law firms working on a PotashCorp takeover were attacked by hackers, apparently based in China, in an attempt to frustrate the deal.[11] The attackers used phishing techniques to send emails to law firms and government officials purporting to be from trusted officials' accounts. Once the attachments were opened, they spread malware in the computer network designed to gather and leak information on the potash transaction. The Boston Business Journal highlighted the potential risks the ten largest Boston intellectual property law firms face to cyberattacks and the leakage of sensitive data.[12] The journal pointed out that law firms are increasingly at risk of cybersecurity breaches. Notably, Cisco's 2015 Annual Security Report ranked law firms as the seventh highest sector to be a target of cyberattack in 2014.[13]

---

10 Scott Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations* (Cambridge: Cambridge University Press, 2014).

11 Greg Weston, "Foreign hackers targeted Canadian firms" (29 November 2011), online: *CBC News* < https://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810> [perma.cc/2JYJ-ESWB].

12 Mark Stevens, "Guest commentary: Boston's law firms are targets for cyber criminals" (22 April 2015), online: *Boston Business Journal* <http://www.bizjournals.com/boston/blog/techflash/2015/04/guest-commentary-boston-s-law-firms-are-targets.html?page=all> [perma.cc/Y6VU-GCQY].

13 "2015 Annual Security Report" (2015) at 14, online (pdf): *Cisco* <https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf> [perma.cc/M7BD-JEU5].

Lawyers have underestimated the cyber risks and the consequent liability arising from cyberattacks. Naturally, lawyers are generally not experts in computer technology. They have widely embraced technology and adopted mobile devices, Internet networks, and cloud services (among others) to work more efficiently and reduce costs, but further still, they have an obligation to protect clients' data. Breaches of this data could expose lawyers to potential suits from clients. Despite this, Canadian Bar Association reports show that law firms generally place low emphasis on cybersecurity.[14]

Hacking into the cloud or the providers of network services such as Google or Microsoft would give hackers access to vast amounts of sensitive data. In the wake of former U.S. intelligence contractor Edward Snowden's confessions about the National Security Agency prying into citizens' private communications, there are concerns about governments eavesdropping on private personal information.[15] Greater risks for law firms are the cyberespionage operations perpetrated by state-sponsored bodies and private hackers with the aim of obtaining trade secrets for their own benefit. A large law firm working with the stock market may harbour several confidential transactions at one point that if successfully hacked, could destabilize public markets.[16] Placing more attention and resources on security has become imperative for law firms.

The purpose of this chapter is to introduce the reader to the many types of cyber-threats that exist, the vectors that they can be advanced from and just how vulnerable most users are to these threats. Additionally, it will introduce and explain why law firms and lawyers are such high value targets. In short, this chapter explains the "what" of the problem.

---

14 Fuchs, Pablo and Sopora, Christine, "On guard" (25 September 2013), online: *Canadian Bar Association National Magazine* <http://www.nationalmagazine.ca/Articles/Sept-Oct-2013/On-guard.aspx> [perma.cc/45QQ-9PEW].

15 Fuchs, Pablo and Sopora, Christine. "Leaking information" (25 September 2013), online: *Canadian Bar Association National Magazine* <http://www.nationalmagazine.ca/Articles/Sept-Oct-2013/Renseignements-sous-surveillance.aspx> [perma.cc/3KHZ-W4BH].

16 *Ibid.*

II. CYBERSPACE, INFORMATION TECHNOLOGIES AND THE CYBERSECURITY IMPERATIVE

Cyberspace is claimed to be a virtual and borderless terrain that coexists with physical space.[17] Cyberspace is not the Internet or the web. The Internet is the "networked physical infrastructure of interconnected computer networks that allows information to move through cyberspace"[18]. The web is "a service that runs on the Internet" or on the network.[19] In this way, cyberspace encompasses the Internet and the web.

Although cyberspace is intangible to some extent, it does not exist without physical components, such as a computer, a mobile device or a telecommunications plant.[20] Physical components, which enable digital communication, allow nations to claim jurisdiction over the virtual activities performed within their borders. Since almost any computer is a potential border entry point, cybersecurity has become a primary concern.[21] A cyberattack may originate in a computer located in one country and its consequences may be felt in the territory of several other countries. Territoriality and jurisdiction remain relevant, although, the challenges to regulation of cyberspace and effective law enforcement are numerous in this fast-changing environment.

The Internet is a massive human phenomenon that engages billions across the globe. Users are the driving force of the information technologies that shape and give life to it. As people use and engage in the network, criminals strive to take advantage of them. Indeed, without users there would be no cyber-attacks.[22] Consequently, understanding the nature of the attack and the motivations of the perpetrators is essential to forming effective cybersecurity policies that can protect legal professionals and their firms.

---

17 Matthew E. Castel, "International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors" (2012) 10 CJLT 89; See also Paul Rosenzweig, "International Governance Framework for Cybersecurity" (2012) 37:2 Can-US LJ 405.

18 *Supra* note 10 at 55.

19 *Ibid*.

20 Castel, *supra* note 17 at 2.

21 Rosenzweig, *supra* note 17 at 1.

22 *Supra* note 10 at 56.

The term cybersecurity is increasingly being used in legal settings and boardroom discussions. However, there is still poor understanding of what this term means for the private sector, and more specifically for the legal practice. Many think it refers to technological measures put in place towards protection of a network and virtual communications. Others attribute it exclusively to IT experts or the workings or methods employed to protect against hackers. In fact, cybersecurity "is the deliberate synergy of technologies, processes, and practices to protect information and the networks, computer systems and appliances, and programs used to collect, process, store and transport that information from attack, damage, and unauthorized access."[23] As such, cybersecurity involves a whole range of activities to protect private records such as the processes used to create, manage, share and store information, and the practices to train lawyers and staff in the protection of the firm's data.[24]

Effective cybersecurity should preserve the confidentiality and integrity of the information from damage and unauthorized access.[25] In his pivotal book, "Thinking, Fast and Slow," Daniel Kahneman highlights the importance of slow and rational thinking.[26] In the time of a crisis, humans are likely to think in a fast and error prone manner. Thus, the preparation of a cybersecurity management plan, including a cyber-threat reaction plan, made thoughtfully and in advance of any crisis provides a resource to staff that is more reliable to follow when a crisis does occur. Kahneman's behavioural science research suggests that cybersecurity strategies are best when they are planned and deliberate.

Questions about cybersecurity necessarily require engagement with the computer engineering community. The Internet was designed to be an open and free communication system that nobody really owns or operates. The rules to determine how the Internet works are heavily influenced by the Internet Engineering Task Force (IETF), an "open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architectures and the smooth operation of the

---

23 Gregory J Touhill & C. Joseph Touhill, *Cybersecurity for Executives: A Practical Guide* (Hoboken: John Wiley & Sons, Inc, 2014) at 2.

24 *Ibid.*

25 *Ibid.*

26 *Supra* note 4.

Internet," headquartered in California.[27] IETF is a self-organized group of computer engineers preoccupied with the better functioning of the Internet from a technical point of view. They do not control or patrol cybercriminal activity on the net as they are not a law enforcement group.[28] Better communication and collaboration between the computer engineering community and law enforcement agencies would be helpful to ensure more technically effective cybersecurity measures.

III. CAUSES OF CYBERATTACKS AND DATA BREACHES

Like many other businesses, many law firms have adopted internal computer networks to work more efficiently. Attackers often target entry points in the network that are poorly guarded and then use one host to infect others on the closed network. Cyber threats are numerous and the terminology to define them is not standardized, as the kinds of threats are constantly evolving alongside the technologies that are exploited.[29]

A computer hacker is someone who has the expertise to infiltrate the security of a computer system. Hackers' motivations to exploit computer systems may be numerous. The reasons may range from pure financial motives to political or simply egotistical reasons. The British law firm, ACS: Law, was attacked in September 2010 by hackers that disliked its practices of impeding illegal file sharing.[30] Hackers employed distributed denial-of-service (DDoS) attacks to crash the law firm's website and access thousands of people's names, addresses and a list of pornographic films illegally downloaded. The law firm was fined for the breach of clients' privacy and closed down as a consequence of the public exposure.

The ways in which cyber threats present themselves in law firms are various. Some basic cyber weapons and tools are:

---

27 "Overview of the ITEF" (2009), online: *IETF* <http://www.ietf.org/old/2009/overview.html> [perma.cc/C7YE-7PTJ].

28 *Rosenzweig, supra note 17* at 3.

29 Pauline Reich, "To Define or Not to Define: Law and Policy Conundrums for the Cybercrime, National Security, International Law and Military Law Communities" in Pauline C. Reich & Eduardo Gelbstein, eds, *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization* (Hershey: Information Science Reference, 2012).

30 "ACS:Law fined over data breach" (11 May 2011), online: *BBC News* <http://www.bbc.com/news/technology-13358896> [perma.cc/Y5P6-G5KE].

Spear Phishing emails: these are apparently legitimate emails that mimic a trusted source, which deceives the receiver into sharing personal information or opening malicious files that are attached to the email. Once the attachment is opened, it may release malware that spreads into the computers or servers of the closed network. The malware may be designed to spy on a specific business deal, trade secrets, or intellectual property.[31] Alternatively, any personal information shared with a spear phishing scammer may be exploited in a number of ways depending on the information provided.

Zero-Day Exploits: hackers can exploit vulnerabilities before the software company fixes the error, exposing users to risks.[32]

Malware: are malicious software programs designed to disrupt computer operation, gather private data, or destroy a network.

Rootkit: is software installed and hidden on the victim computer, without the user's knowledge, to access information, monitor user actions, modify programs or other activities.[33]

Botnet: is a large number of compromised computers that are controlled by a hacker. These computers are used to spread worms, spam or launch attacks.[34]

Distributed Denial-of-Service (DDoS) Attacks: these attacks seek to halt normal services by overwhelming the network with traffic. DDoS attacks can crash a website, a server or a network by overloading a specific application.[35]

Spyware: is a malicious program installed on a computer designed to monitor browsing habits, users' personal data, or their general computer use. The information is then transmitted to a third party that may sell it.[36]

Viruses and Worms: viruses are spread by infected websites and email attachments or USBs. They affect the behaviour of the computer,

---

31 ABA *Handbook*, *supra* note 5 at 12.

32 Reich, *supra* note 29 at 155-156.

33 *Ibid*.

34 *Ibid*.

35 *Supra* note 10 at 139.

36 *Ibid* at 137.

causing damage to it or to the entire closed network. Unlike viruses, worms do not require an infected host file to continue replicating.[37]

Wateringhole: cybercriminals infect a popular website that businesses visit frequently. Malicious code can infect a visitor's computer and propagate to the whole computer system.[38]

These cyber-weapons are used by outside threats, which represent approximately 36% of cyber incidents, according to a study by the Open Security Foundation. However, inside threats constitute an important part of the threat analysis. Malicious insider attacks are on the rise. The motivations for employees and partners of a firm to cause data breaches range from pure financial gain to revenge. Organization insiders may also cause leakage of information by mere negligence, accident, technological misinformation or carelessness. A distribution of cyber incidents in all sectors by type of breach in 2015 in the U.S. is shown in Figure 1.

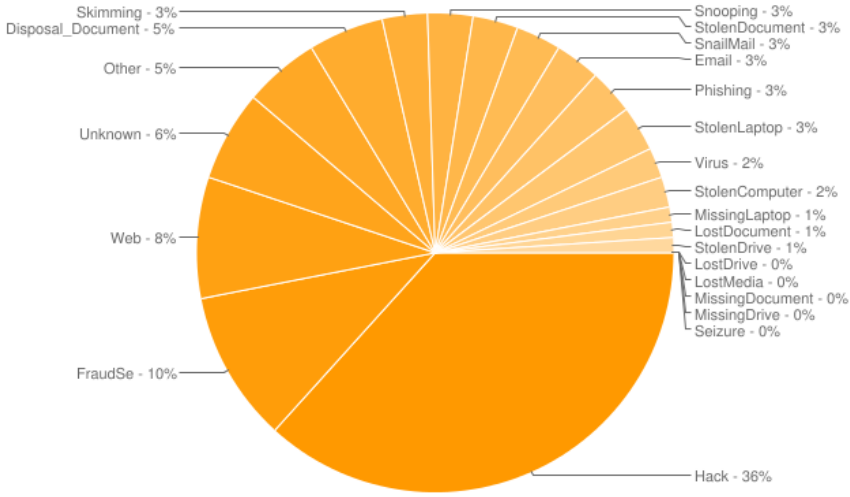

Figure 1. Incidents by type of cybersecurity breach in 2015.[39]

---

37 *Ibid* at 138-139.

38 Matthew Wocks, "Cyberattacks increasingly targeting small businesses, report says" (16 April 2013), online: *Financial Post* <https://financialpost.com/technology/cyberattacks-symantec-report > [perma.cc/UVE9-KXYY].

39 "DataLossDB" (2015), online (blog): *DataLossDB* <https://blog.datalossdb.org/>. Link no longer active.

Cyber-attacks have traditionally been pursued to undermine government defenses. However, today the majority of cyber-threats target the private sector due to the fact that there is a highly lucrative industry behind stealing industrial and personal information. Touhill and Touhill argue that it is not easily justified to invest in "costly and potentially unproductive research and development when you can acquire someone's information at a fraction of the cost" by stealing it on the Internet.[40] According to a 2014 study released by the Center for Strategic and International Studies, the approximate cost to the global economy of cybercrime is more than $445 billion, including the gains to cybercriminals and the costs to companies for recovery and defense.[41] While the U.S. has ranked first in global security threats, Canada has ranked fifteenth worldwide, and sixth in the list of spear-phishing attacks.[42]

The scope and scale of criminal activities extends throughout the commercial domain to all sizes of businesses and sectors. A 2012 report found that small-size firms are being attacked more regularly most likely because they cannot afford large investments in cybersecurity, making them easy targets.[43] Notably, smaller businesses can hold intellectual property belonging to larger corporations when the two are collaborating. By attacking a smaller company connected to a larger business network, hackers can penetrate the major company indirectly and generally with less resistance.

Businesses, including law firms, have begun using remote server services, or cloud services, to be more cost efficient, improve IT management and achieve scalable business protocols. Storing information in the cloud is a double-edged sword, as data breaches can yield interesting results for hackers. Cloud services offer a wealth of personal and commercial data accessible by hacking just one place instead of numerous locations. A hacker can steal credentials of a company to gain access to cloud services, obtain company data, manipulate data, and perhaps direct clients to infected websites wreaking havoc as a consequence.[44]

---

40 Touhill & Touhill, supra note 23 at 16.

41 "Net Losses: Estimating the Cost of Cybercrime and Cyber Espionage" (2014) at 2, online (pdf): McAfee <http://csis.org/files/attachments/140609_McAfee_PDF.pdf> [perma.cc/4CYV-KVDM].

42 *Supra* note 38.

43 *Ibid.*

44 Bob Violino, "11 top cloud security threats" (11 October 2019), online: CSO Online

Smartphones are highly convenient for working more efficiently, but they pose significant security risks. One study showed that 80% of smartphones do not have malware protection, which increases the risk of cyberattacks exponentially.[45] A top secret document leaked by Edward Snowden and obtained by CBC revealed that Canada and other countries exploited smartphone application vulnerabilities to implant spyware and collect data on terrorists and other intelligence targets in late 2011.[46] Although government surveillance agencies knew about the software weaknesses, they did not alert private companies and the public about them, putting users at risk of other governments and cybercriminals accessing their data.[47] This is just one example of the constant tension governments find themselves facing as they choose to sacrifice the rights to privacy and security of citizens' data in the name of protecting national security interests against terrorism.

Cyberattacks may also be perpetrated by nation-states. Countries such as China have been repeatedly confronted with evidence of complicity in cybercrimes, but they have denied any involvement.[48] Mike McConnell, a former director of the American National Intelligence Agency, stated that "the Chinese are exploiting [American] systems for information advantage - looking for the characteristics of a weapons system by a defense contractor or academic research on plasma physics, for example - not in order to destroy data and do damage."[49] McConell states that the Chinese favour the clandestine approach of spyware since they need to export to the U.S. and to maintain a stable currency and global markets. Cybercrime and cyberespionage are not going to decrease any time soon for several reasons;

<https://www.csoonline.com/article/3043030/top-cloud-security-threats.html> [perma.cc/NG5M-L2N7].

45 *Ibid*.

46 "Spy Agencies Target Mobile Phones, App Stores to Implant Spyware" (21 May 2015), online: CBC News <http://www.cbc.ca/news/canada/spy-agencies-target-mobile-phones-app-stores-to-implant-spyware-1.3076546> [perma.cc/AL5N-2CU7].

47 *Ibid*.

48 *Supra* note 23 at 16.

49 Nathan Gardels, "Cyberwar with China: Former Intelligence Chief Says It Is Aiming at America's 'Soft Underbelly'" (9 April 2010), online: Huffington Post < https://www.huffpost.com/entry/cyberwar-with-china-forme_b_452639> [perma.cc/R5K4-WVSQ].

the most important is that it simply has become an extremely lucrative industry with staggering financial gains, which may sometimes have political, social and personal motives as well.

A. Cybercrime and Multi-Jurisdictional Issues

The incentives to steal data are significant yet the deterrents to committing cybercrimes are minimal. This is largely because traditional law enforcement techniques to deter cybercrime face innumerable challenges.[50] Deterrence is not that effective, due to the nature of cybercrime, the speed at which cybercriminals move, and the difficulty in tracking down cybercriminals reliably.[51] It is extremely difficult to prove beyond any reasonable doubt the identity of the source of a cybercrime, as often the perpetrators use intermediate computer systems to disguise their identity. Even in the rare cases where the ultimate computer source of the attack has been identified, it is challenging to prosecute the perpetrators in a transnational context. Attackers act very quickly so as to erase the traces of the crime immediately after the fact. To complicate matters, cyberweapons, regardless of the type, tend to remain undetected by the victim for a long time. If the user is not aware of a cyberbreach, law enforcement cannot do much. Moreover, by the time the victim knows about the data breach, hackers are often gone and have erased their tracks.

In a multi-jurisdictional environment, the applicability of laws, the definitions of crimes and appropriate punishments vary greatly, which creates major legal hurdles to law enforcement. Most procedural criminal law requirements are based on the assumption that the crimes to be investigated and prosecuted have occurred within the geographic boundaries of the country. However, the reality of cybercrime is that it is mostly international in character. Constructing a transnational set of procedural rules for cybercrime could be a start to addressing some of these problems.[52] However,

---

50 Bruce Kobayashi, "Private Versus Social Incentives in Cybersecurity: Law and Economics" in Mark Grady & Francesco Parisi, eds, *The Law and Economics of Cybersecurity* (New York: Cambridge University Press, 2005) at 13.

51 *Castel*, *supra* note 17 at 1.

52 *Rosenzweig*, *supra* note 17*supra* note 17 at 6.

pursuing a common substantive set of laws across national borders may well prove impossible to achieve.[53]

Technology has always advanced more quickly than the law, creating new challenges that the law tries to fix in a continuous race to keep up with the changes. Technology opens up new opportunities for cybercriminals, as they have new tools to commit new crimes and old crimes in new ways. According to the Royal Canadian Mounted Police, the most typical cases of cybercrime in Canada involve:

- Mass marketing fraud
- Money laundering
- Identity theft
- Child exploitation
- Intellectual property infringements
- Internet-based drug trafficking.[54]

Addressing law enforcement challenges "requires broad-based domestic and international law enforcement cooperation, engagement with public and private sector organizations, and integrating new technical skills and tools with traditional policing measures."[55] However, the likelihood of achieving effective domestic and international law enforcement cooperation is low. The Convention on Cybercrime developed by the Council of Europe in 2001 is a modest effort to create a convergence of procedural laws to ensure that there are no safe harbours for cybercriminals and to promote law enforcement cooperation.[56] To date only forty five countries have ratified the Convention, and notoriously China and Russia are not signatories.[57] Despite the laudable efforts of the Convention, it failed at defining cybercrimes, and at answering significant questions of extraterritoriality and jurisdiction. The fact that China and Russia are not signatories of the Convention technically

---

53 *Ibid.*

54 "Cyber Crime: An Overview of Incidents and Issues in Canada" (16 December 2014), online: *Royal Canadian Mounted Police* <http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada> [perma.cc/SU8H-UQDC] [RCMP Cyber Crime].

55 *Ibid.*

56 "Convention on Cybercrime" (23 November 2001), online: *Council of Europe* <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> [perma.cc/GL22-SQEU].

57 *Ibid.*

positions them as potential safe havens for cybercriminals and limits the reach of the Convention.[58]

Beyond the issue of the infancy of cybercrime laws, another problem is how to determine whose law is to be applied in cross-border cyberattacks. Perhaps the law of the country or countries where the crime originated should be applied (also known as the ubiquity doctrine),[59] or the law of the country where the effects of the crime were felt (also known as the effects doctrine),[60] or the law of the country where the servers are maintained, or where the data storage provider is headquartered, or the law of the citizenship of the perpetrator, or all of the above. The problem is that "nobody really knows."[61] Due to the complexity of the issue and the international failures at creating a homogenous set of cybercrime laws, countries have tended to try and maintain their sovereignty and jurisdiction within their borders by using the territoriality principle. In attempting to assert their jurisdiction, countries have argued that the location of the physical infrastructure of the server or where the data is stored will determine the jurisdiction and the laws to be applied to the cybercrime.[62]

Unfortunately, the assertion of jurisdiction specific laws to cybercrimes is a faulty methodology to deter cybercrimes. For example, a Spanish hacker may be using a computer in South Africa with access to a server in American to steal private data of Swiss citizens stored in the cloud. Whose laws will be applied? The territoriality principle does not offer simple solutions to the question of jurisdiction. At the end of the day, cyberattackers may hide in safe havens and if an extradition order is issued, the country where they hide may refuse to hand them over, or in a worst-case scenario, the identity of the hacker is never proved. The Royal Canadian Mounted Police argued that effective law enforcement requires international

---

58 *Rosenzweig*, *supra* note 17 *supra* note 17at 6.

59 "ITU Toolkit for Cybercrime Legislation" (February 2010), online (pdf): *International Telecommunication Union* <http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf> [perma.cc/JD9H-ZESA].

60 *Ibid.*

61 *Rosenzweig*, *supra* note 17 at 422.

62 *Ibid.*

agreement and collaboration as well as engagement with public and private agencies if we are to begin to glimpse a solution.[63]

IV. LAW FIRMS AS HIGH-PRIORITY TARGETS

Law firms are targeted by hackers and state-sponsored organizations because they harbour sensitive client data. Countless cyberbreaches go unreported because law firms fear the effects of the publicity on their practices. A cyberattack on a law firm resulting in a privacy breach of a clients' information may result in the loss of a firm's reputation, lawsuits and fines, which could cause the firm to close its doors. Thus, it is unknown how many successful attacks law firms in Canada have suffered, as firms rarely publicly admit breach of data.

Paradoxically, if law firms were more willing to report cybersecurity breaches, steps may be taken to limit the damage of future attacks. At minimum, diligent reporting of cybersecurity breaches improves statistics, enabling companies to better assess the risks of such attacks within their industries. Notably, the Canadian government has created a platform to report cyberincidents.[64]

Nevertheless, evidence of cyberbreaches in law firms continues to grow, despite the details tending to be concealed. The Maryland-based SANS Institute (an important cybersecurity training and certification organization) recounts an incident where the managing partner and IT partner of a large New York law firm had been told by the Federal Bureau of Investigation (FBI) that all the firm's files had been found on a server used as a way station for sending data to China.[65] The SANS Institute asked about what the lawyers were planning to tell their clients. "Telling them anything would be crazy!" the lawyers responded. "Can you think of a better way to destroy their

---

63 "*Cyber Crime: An Overview of Incidents and Issues in Canada" (16 December 2014), online:Supra.*>.RCMP Cybercrime, *supra*

64 "Cyber Security" (19 November 2018), online: *Public Safety Canada* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-en.aspx> [perma.cc/9KUG-H4GF].

65 "Conversations About Cybersecurity," online: *SANS* <https://www.sans.org/security-resources/cybersecurity-conversations> [perma.cc/7WN9-B4KR].

trust in us than informing them that all the documents they gave us under attorney-client privilege have been stolen?"[66]

In a high profile cyberattack in 2010, hackers breached the cybersecurity of seven major Canadian law firms on Bay Street, in Toronto. The firms were involved in the possible takeover of Saskatchewan's Potash Corp. No client information was compromised according to the law firms breached.[67] Analysis of the malware revealed that it had been created on a Chinese language keyboard and could be traced to servers in China linked to state-owned enterprises. Notably, at the time China feared a potential global potash monopoly.[68]

According to *LawPRO Magazine*, a cybercrime scheme was responsible for the loss of hundreds of thousands of dollars from a small law firm in Toronto in December 2012.[69] Hackers embedded a virus in a computer used by the law firm's bookkeeper. The virus emulated a bank's website on which the bookkeeper typed in the firm's trust account password. The computer of the victim then sent the passwords to the hackers, who could access the account and transfer out money to foreign accounts.[70]

In 2019 in the U.S., courts were targeted by cyber attacks, case management software was hacked, and more than 100 law firms reported data breaches.[71] Moreover, recently Dentons Canada LLP fell victim to a million-dollar cyberscam.[72]

---

66 *Ibid.*

67 Julius Melnitzer, "Law Firms: Cyber Target #1" (1 April 2013), online: *Lexpert Business of Law* <https://www.lexpert.ca/article/law-firms-cyber-target-1/?p=&sitecode=> [perma.cc/5PF8-Y72N].

68 *Ibid.*

69 "Cybercrime and Law Firms" (December 2013) at 6, online (pdf): *LawPRO Magazine* <https://www.practicepro.ca/wp-content/uploads/2017/09/2013-12-lawpro-magazine12-4-dec2013.pdf> [perma.cc/A66S-ANN4].

70 *Ibid.*

71 Victoria Hudgins, "4 Cyberattacks That Hijacked Legal in 2019" (20 December 2019), online: *Law.com* <https://www.law.com/legaltechnews/2019/12/20/4-cyberattacks-that-hijacked-legal-in-2019/> [perma.cc/27MV-MFZA]; Christine Simmons, Xiumei Dong & Ben Hancock, "More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse" (15 October 2019), online: *Law.com* <https://www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse/> [perma.cc/2EGL-ZXJH].

72 Michael McKiernan, "Firm in $1.7-million dispute with insure" (21 January 2019),

The potash incident opened the eyes of the legal community in Canada. The role of legal agencies like the Canadian Bar Association has been instrumental in raising awareness of the problem.[73] Some law firms such as Goodmans LLP and Gowling Lafleur Henderson LLP have tightened cybersecurity by introducing Bit9.[74] This software allows only authorized programs to run on the law firm's system and catches vulnerabilities that anti-virus programs do not.[75] Other firms such as Torys LLP restricted end user privileges on the firm's computers, preventing lawyers and staff from installing unauthorized applications.[76] One of the weakest points of cybersecurity is the human component. Training staff to think before clicking odd emails or surf questionable websites, instituting seminars and other educational strategies may help staff break old habits and form new ones to ensure greater cybersecurity. This human element of cybersecurity will be explored in more detail in chapter 3.

In general, more Canadian lawyers are "increasing cybersecurity resources within their firms in order to keep sensitive data safe from breaches;"[77] however, not all law firms are doing enough to improve their cybersecurity. One expert has compared legal professionals' adoption of technology to a hibernating bear, stuck in deep sleep.[78] [79]

What law firms do regarding cybersecurity stems from the risks they perceive. Law firms need to focus on the reality that cybercriminals will attempt to access their data systems.[80] Thus, raising awareness and investing

---

online: *Law Times* <https://www.lawtimesnews.com/news/general/firm-in-1.7-million-dispute-with-insurer/263383> [perma.cc/33TK-VXZN].

73 "60 Tips in 60 Minutes" (Canadian Bar Association Legal Conference, St. John's, NL, August 15-17, 2014) [unpublished].

74 Melnitzer, *supra* note 67.

75 *Ibid.*

76 *Ibid.*

77 Alexia Kapralos, "Nearly nine in 10 lawyers aim to increase cybersecurity resources, survey states" (29 April 2019), online: Canadian Lawyer <https://www.canadianlawyermag.com/news/general/nearly-nine-in-10-lawyers-aim-to-increase-cybersecurity-resources-survey-states/276075> [perma.cc/D7Y5-UGWA].

78 Melnitzer, *supra* note 67.

79 *Ibid.*

80 *Ibid.*

in education and technology are important measures to mitigate cybersecurity risks – a point that will be discussed in greater detail in chapter 3.

CHAPTER II: Ethical and Legal Obligations of Lawyers to Consider Cybersecurity

This chapter illustrates why those involved in legal work should care about the cyberthreats discussed in the previous chapter. The damages, both pecuniary and reputational, that cybersecurity breaches can lead to will be discussed along with the professional obligations and privacy statutes that could be breached by the careless handling of data. An appendix of privacy legislation that builds upon this chapter's contents is located at the end of this monograph.

I. Introduction

Lawyers should be concerned about the security of their electronic data. Lapses in judgment concerning cybersecurity, or the failure to adhere to certain IT best practices, can result in considerable embarrassment and pecuniary losses for the exposed party. In 2016, a number of well-known examples of such IT failings became prominent features of the U.S. presidential elections. In July 2016, the Democratic National Committee had their emails stolen by an unknown party[81] and released by WikiLeaks, causing considerable embarrassment for the party and resulting in the resignation of their Chairperson.[82] That same summer, the Democratic Party

---

81 David E Sanger & Eric Schmitt, "Spy Agency Consensus Grows that Russia Hacked D.N.C." (26 July 2016), online: *The New York Times* <http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html> [perma.cc/Q3VG-6LSK].

82 Michael D Shear & Matthew Rosenberg, "Released Emails Suggest the D.N.C. Derided the Sanders Campaign" (22 July 2016), online: *The New York Times*

nominee for President, Hilary Clinton, embroiled herself in controversy over the use of a private email while she was Secretary of State,[83] and was verbally rebuked by the head of the FBI over the "extremely careless" use of private email.[84] Other prominent examples of such IT failings come from the world of business, including an incident that came to light in December of 2014 when news broke that Sony Pictures Entertainment's computer network had been compromised.[85] Amongst the leaked stolen data were compromising emails sent between Sony's executives. This leak led to the resignation of the company's top film executive.[86] Several Sony films were also released onto

<http://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html?action=click&contentCollection=Politics&module=RelatedCoverage&region=Marginalia&pgtype=article> [perma.cc/KS9U-EGU7]; Jonathan Martin & Alan Rappeport, "Debbie Wasserman Schultz to Resign D.N.C. Post" (24 July 2016), online: *The New York Times* <http://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html> [perma.cc/D3CX-MDZL].

83 Alicia Parlapiano, "What We Know About the Investigation into Hillary Clinton's Private Email Server" (28 October 2016), online: *The New York Times* < http://www.nytimes.com/interactive/2016/05/27/us/politics/what-we-know-about-hillary-clintons-private-email-server.html"http://www.nytimes.com/interactive/2016/05/27/us/politics/what-we-know-about-hillary-clintons-private-email-server.html> [perma.cc/QFC2-WWM8].

84 Mark Landler & Eric Lichtblau, "F.B.I. Director James Comey Recommends No Charges for Hillary Clinton on Email" (5 July 2016), online: *The New York Times* <http://www.nytimes.com/2016/07/06/us/politics/hillary-clinton-fbi-email-comey.html?action=click&contentCollection=Politics&region=Footer&module=WhatsNext&version=WhatsNext&contentID=WhatsNext&moduleDetail=undefined&pgtype=Multimedia> [perma.cc/2QPZ-SNWY].

85 Elizabeth Weise & Claudia Puig, "Sony hack may be linked to James Franco comedy" (1 December 2014), online: *USA Today* <http://www.usatoday.com/story/tech/2014/12/01/hack-attack-sony-pictures-north-korea-the-interview/19733463/> [perma.cc/95JZ-K87W]; Andrew Griffin, "Sony Hack: It was North Korea, says FBI" (19 December 2014), online: *Independent* <http://www.independent.co.uk/life-style/gadgets-and-tech/news/sony-hack-us-to-officially-blame-north-korea-allege-china-could-have-helped-say-reports-9936438.html> [perma.cc/QN7Z-WPWU]; Michael Hiltzik, "The Sony hack: What if it isn't North Korea?" (19 December 2014), online: *Los Angeles Times* <http://www.latimes.com/business/la-fi-mh-the-sony-hack-20141219-column.html> [perma.cc/B5ZF-CFGU].

86 Michael Cieply & Brooks Barnes, "Amy Pascal Lands in Sony's Outbox" (5 February 2015), online: *The New York Times* <http://www.nytimes.com/2015/02/06/business/amy-pascal-leaving-as-sony-studio-

the internet prior to their theatrical release, potentially costing the company millions in lost ticket sales.[87]

For the practicing attorney, the loss of money, intellectual property and reputation can be devastating to a practice. However, legal practitioners need to be aware that failures in IT security practices can result in other negative consequences for their practice; it is these negative consequences that concern this chapter. This chapter will argue that, as lawyers, both our ethical obligations and various privacy statutes compel us to at least consider the IT security implications of our use of technology and engage in some basal level of cyber protection, and that the failure to do so can result in professional discipline or substantial fines. This chapter is divided into two parts: the first concerns the professional obligations, or legal ethics that govern the practice of law in Canada and argues that our legal ethics and professional obligations compel lawyers to seriously consider IT security practices when serving our clients. The second part of this chapter will discuss the scope and applicability of various legislative privacy regimes throughout Canada. While these regimes are in no way uniquely applicable to lawyers, it is by virtue of the information legal practitioners come to hold during the ordinary course of a legal practice that will likely bring lawyers and law firms within the scope of these laws.

II. PROFESSIONAL OBLIGATIONS

The legal profession in Canada is governed by provincial and territorial law societies that serve as both the licensing and disciplinary authorities for our profession. The codes of conduct and practice directives set by these bodies regulate the practice of law within Canada, and these documents codify lawyers' professional obligations to their clients. While each of the provincial and territorial jurisdictions in Canada have their corresponding law society or *barreau* and code of conduct, there is

chief.html> [perma.cc/R6SE-GG8T].

87 Andrew Wallenstein & Brent Lang, "Sony's New Movies Leak Online Following Hack Attack" (29 November 2014), online: *Variety* <http://variety.com/2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack-1201367036/> [perma.cc/9B3F-7FT6]; James Geddes, "Sony Sued For Revenues Lost When Film Was Released Online In Hack" (31 July 2016), online: *Tech Times* <http://www.techtimes.com/articles/171941/20160731/sony-sued-for-revenues-lost-when-film-was-released-online-in-hack.htm> [perma.cc/9RHA-77Y7].

considerable overlap in terms of the content of most of these codes due to the general acceptance of the Federation of Law Societies of Canada's Model Code of Professional Conduct.[88] As such, in this section, the Model Code will serve as an organizing template.

The Model Code does not impose specific obligations upon lawyers related to their use of IT generally or their treatment of electronic data, nor are there any specific requirements imposed upon lawyers to adopt a *de minimis* level of cybersecurity best practices. In fact, the Model Code only specifically mentions the word "computers" once in its text and this reference is found not in the code itself, but rather in the explanatory commentary that accompanies section 3.6-3. Section 3.6-3 concerns statements of account delivered to clients. Commentary [1] makes reference to "computer costs" as an "Other Charge" which may be itemized when presenting a client with an invoice.

Sections 6.1-5 and 6.1-6 of the Model Code outline recommendations concerning the "Electronic Registration of Documents,"[89] which require lawyers, and their employees, who have "personalized encrypted electronic access to any system for the electronic submission or registration of documents"[90] to not share their password or permit others with said access. However, these sections focus upon a very specific subset of technology usage, and while reflecting certain IT best practices (i.e. not sharing passwords, not sharing access), the Model Code is limited in its application to the electronic registration of documents.

Of course, as was argued in the previous chapter, the practice of law (and of almost every other profession) has been revolutionized by the development of information technology in the last several decades, and the near constant use of computers and smartphones is now considered the norm within our industry. While the Model Code lacks specific reference to information technology and cybersecurity, it would be foolish to assume that the changes in the practice of law did not bring about corresponding changes in our professional obligations to clients. Rather, as will be argued below, certain existing provisions of the Model Code appear to impose minimum

---

88 Federation of Law Societies of Canada, Model Code of Professional Conduct, Ottawa: FLSC, 2017 [*Model Code*].

89 *Ibid*, ss 6.1-5 & 6.1-6.

90 *Ibid*.

standards on lawyers with regard to their use of information technology.[91] A number of specific, and hopefully familiar, duties lawyers owe to their clients and how these duties can, and likely do, impose obligations related to cybersecurity upon lawyers will be discussed. This section is, to some degree, speculative, as there exists very little in the way of practice directives and disciplinary decisions that specifically envision these provisions of the Model Code to be as expansive as we argue below; however, where available, we have offered opinions from other reputable authorities to buttress arguments made.

A. Duty of Competence and Quality of Service

Amongst the foremost professional responsibilities entrusted to lawyers upon being called to the bar is the duty to provide competent service to our clients. This ethical duty is conceptually distinct from malpractice/negligence,[92] as the latter potentially attracts tortious liability while the former attracts disciplinary action on the part of the jurisdiction's law society.[93] While there have been "very few cases where lawyers have been disciplined by a law society for incompetence,"[94] this duty still compels lawyers to uphold a basic level of professional competence with regard to the service that they provide to their clients.

In the Model Code, competency and quality of service are dealt with in two separate sections. Section 3.1-2 of the Model Code provides the foundation for the duty to provide competent service. It reads: "[a] lawyer must perform all legal services undertaken on a client's behalf to the standard of a competent lawyer"[95]; "competent lawyer" is a term defined earlier the Model Code, and amongst the many qualities that a "competent lawyer" should possess is that they must "[adapt] to changing professional

---

91 *Ibid* at preface.

92 Alice Woolley et al, *Lawyer's Ethics and Professional Regulation* (Markham, ON: LexisNexis Canada Inc, 2008) at 173 [*Wooley et al*] posits that the leading case on lawyer malpractice is the SCC's decision in *Central Trust Co v Rafuse*, [1986] 2 SCR 147, 31 DLR (4th) 481.

93 Gavin MacKenzie, *Lawyers and Ethics: Professional Responsibility and Discipline*, 3rd ed (Toronto, ON: Carswell, 2001) at 24-3.

94 *Wooley et al*, *supra* note 92 at 173.

95 *Model Code*, *supra* note 88, s 3.1-2.

requirements, standards, techniques and practices."[96] The Model Code's subsection concerning quality of service follows, and contains nine subsections; the first of which is pertinent. Section 3.2-1 reads: "[a] lawyer has a duty to provide courteous, thorough and prompt service to clients. The quality of service required of a lawyer is service that is competent, timely, conscientious, diligent, efficient and civil."[97] The commentary expanding upon this section of the code provides examples of "expected practices" with regard to standards in practice, including that a lawyer is expected to maintain "office staff, facilities and equipment adequate to the lawyer's practice."[98]

Although sections 3.1-2 and 3.2-1 do not specifically mention technological best practices or cybersecurity, dismissing the applicability of the duties to this topic would be unwise. Scholars have noted that the duties of competence and quality of service concern more than just the knowledge of the law. Gavin MacKenzie has argued that "[c]ompetence in the context of these duties [duty to be competent, and duty to serve clients] ... means more than formal qualification to practice law, and involves more than an understanding of legal principles."[99] Additionally, if we look at other sources for context and guidance for this duty, it becomes apparent that failure to keep abreast of technology in the practice of law clearly impacts a lawyer's ability to provide competent service. Three examples of how this duty is interpreted by sources external to the Model Code support this argument.

First, chapter II of the now-defunct CBA code of professional conduct[100] contained rules that were similar to the Model Code's duties of competence and quality of service. These rules were:

1. The lawyer owes the client a duty to be competent to perform any legal service undertaken on the client's behalf.

---

96 *Ibid*, s 3.1-1(k).

97 *Ibid*, s 3.2-1.

98 *Ibid*, s 3.2-1[5][j].

99 *MacKenzie, supra* note 93 at 24-1; MacKenzie specifically cites to the CBA rules, discussed on this page.

100 Canadian Bar Association, "Codes of Professional Conduct" online: *The Canadian Bar Association* <https://www.cba.org/Publications-Resources/Practice-Tools/Ethics-and-Professional-Responsibility-(1)/Codes-of-Professional-Conduct> [perma.cc/GGP2-EFXE] [*CBA Code*].

2. The lawyer should serve the client in a conscientious, diligent and efficient manner so as to provide a quality of service at least equal to that which lawyers generally would expect of a competent lawyer in a like situation.[101]

While the CBA rules were phrased slightly differently than the provisions of the Model Code reviewed earlier, there are a number of central common elements in these two sets of rules, including the requirements to serve clients at the standard of a competent lawyer while being conscientious, diligent and efficient. The CBA's commentary on its rules makes an important point about maintaining competency with the advancement of technology. Paragraph four in the commentary accompanying the CBA rules reads:

Competence involves more than an understanding of legal principles; it involves an adequate knowledge of the practice and procedures by which those principles can be effectively applied. To accomplish this, the lawyer should keep abreast of developments in all areas in which the lawyer practices. The lawyer should also *develop and maintain a facility with advances in technology in areas in which the lawyer practices to maintain a level of competence* that meets the standard reasonably expected of lawyers in similar practices circumstances.[102]

As stated in the emphasized text above, the CBA rules concerning competence and quality of service envisioned keeping pace with technological changes to be part of a lawyer's duty of competence.

The second source to which we turn is the American Bar Association's (ABA) Model Rules of Professional Conduct. Rule 1.1 of that code concerns competence and reads:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[103]

---

101 *Ibid* at chapter 2.

102 The Canadian Bar Association, *Code of Professional Conduct*, Ottawa: CBA, 2006.

103 American Bar Association, "Rule 1.1 Competence" (16 August 2018), online: *American Bar Association* <https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/> [perma.cc/H4RD-8YK6].

As with the CBA rules referenced above, the ABA's Model Rules contemplates keeping abreast of technological changes as part of the duty of competence. The commentary accompanying Rule 1.1 states:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*.[104]

In their cybersecurity handbook published by the ABA, Jill D. Rhodes and Vincent I. Polley refer to the opinion of the State Bar of Arizona to expand upon this commentary. In this opinion, it was held that:

An attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence.[105]

Upon reviewing this opinion, Rhodes and Polley and others, argue that the American duty of competence lawyers owe to clients requires a "continued vigilance and learning as technology advances."[106]

The third and final source to which we turn is an opinion from the Law Society of Manitoba. In 2012, the Technology Committee of the Law Society of Manitoba published a report concerning, amongst other matters, the use of technology in the legal practice in Manitoba. The report made a number of recommendations to the Benchers, including the publication of practice directives concerning proper use of technology; this section began:

The committee was of the view that although it is every lawyer's own obligation to be competent in utilizing the level of technology he or she chooses to employ, it would be beneficial for the Law Society to provide guidelines/advice/standards/best practice examples to give lawyers some

---

104 American Bar Association, "Rule 1.1 Competence - Comment" (16 August 2018) at commentary 8, online: *American Bar Association* <https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/> [perma.cc/8X3C-XZJL].

105 State bar opinion of Arizona – Opinion 05-04 July 2005 as found in *ABA Handbook*, *supra* note 5 at 65-66.

106 *ABA Handbook*, *supra* note 5 at 66.

direction on what must be done to properly protect electronic data and information.[107]

In summary, the duty to be competent and the duty to provide quality service likely impose upon lawyers a minimum requirement to be competent with regard to the technology they utilize in the service of their clients.

B. Duty of Confidence

The lawyer's duty to maintain the confidentiality of their clients' affairs is a defining feature[108] or central tenet[109] of our field's professional ethics. In *Canada (Attorney General) v- Federation of Law Societies of Canada*, Justice Cromwell began his majority opinion by rightly stating that "[l]awyers must keep their clients' confidences and act with commitment to serving and protecting their clients' legitimate interests. Both of these duties are essential to the due administration of justice."[110] The rationale for why this duty to keep confidences is "essential to the due administration of justice" should be well known to graduates of Canadian law schools and bar admission courses. It is similar to the reasoning underlying solicitor-client privilege; namely, that in order for a lawyer to provide competent service and accurate legal advice, the lawyer must be abreast of all of the necessary facts of the case. Securities afforded both by the duty of confidentiality and solicitor-client privilege seek to facilitate such an honest and open transmission of information from client to attorney. Such legal reasoning has roots in the common law dating to before Confederation, and was accepted by Canadian courts as early as 1876 in *Anderson v Bank of British Columbia*:

litigation can only be properly conducted by professional men, it is absolutely necessary that a man, in order to prosecute his rights or to defend himself from an improper claim, should have recourse to the assistance of

---

107 "Report to Benchers from the Technology Committee" (27 March 2012), online (pdf): *Law Society of Manitoba* <http://www.lawsociety.mb.ca/publications/technology-articles/2011-2012_tech_committee_report.pdf> at 4 [*Law Society of Manitoba*].> [*Technology Committee Report*].

108 Randal NM Graham, *Legal Ethics: Theories, Cases and Professional Regulation*, 3rd ed (Toronto, ON: Emond Montgomery Publications Limited, 2014) at 191.

109 *Wooley et al*, *supra* note 92 at 242.

110 *Canada (Attorney General) v Federation of Law Societies of Canada*, 2015 SCC 7 at para 1.

professional lawyers . . . that he should be able to place unrestricted and unbounded confidence in the professional agent, and that the communications he so makes to him should be kept secret, unless with his consent (for it is his privilege, and not the privilege of the confidential agent), that he should be enabled properly to conduct his litigation.[111]

Justice Cory adopted the above passage in the Supreme Court's 1999 decision concerning solicitor-client privilege, *Smith v Jones*. Of course, solicitor-client privilege and the duty to retain confidentiality are not the same thing,[112] despite having a similar underlying rationale.[113] Solicitor-client privilege is a rule of evidence, disallowing conversations between a lawyer and client for the purpose of securing legal advice from being entered into evidence.[114] The duty of confidentiality is much broader than the privilege, protecting all information concerning a client's affairs which a lawyer may acquire from all sources (i.e., not just the client).[115]

The ethical duty to maintain confidences can be found in two specific entries in the Model Code. The first is found in section 3.3-1, and reads:

A lawyer at all times must 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 unless:

a) expressly or impliedly authorized by the client;
b) required by law or a court to do so;
c) required to deliver the information to the Law Society; or

---

111 *Anderson v Bank of British Columbia* (1876), 2 Ch D 644 (CA) at 649, as cited in *Smith v Jones*, [1999] 1 SCR 455.

112 *Model Code*, *supra* note 88, s 3.3[2].

113 Allan C Hutchinson, *Legal Ethics and Professional Responsibility* (Toronto, ON: Irwin Law, 1999) at 114, says the ethical rule is based upon the privilege. The *Model Code*, *supra* note 88, s 3.3-1[1] states, "A lawyer cannot render effective professional service to a client unless there is full and unreserved communication between them. At the same time, the client must feel completely secure and entitled to proceed on the basis that, without any express request or stipulation on the client's part, matters disclosed to or discussed with the lawyer will be held in strict confidence."

114 David Paciocco & Lee Stuesser, *The Law of Evidence*, 7th ed (Toronto, ON: Irwin Law Inc, 2015).

115 *MacKenzie*, *supra* note 93 at 3-3; Hutchinson, *supra* note 113 at 114-5.

d) otherwise permitted by this rule.[116]

Additionally, section 3.3-2 prevents the use or disclosure of said information:

A lawyer must not use or disclose a client's or former client's confidential information to the disadvantage of the client or former client, or for the benefit of the lawyer or a third person without the consent of the client or former client.[117]

The commentary that accompanies the Model Code expands upon the scope of this duty, indicating that the duty can arise with regard to information shared informally[118] and that the duty "survives the professional relationship and continues indefinitely."[119] Additionally, the commentary on the Code indirectly warns against the inadvertent disclosure of confidential information.[120]

The Model Code does not have any specific mention of IT security or the protection of digital forms of data in its text. Yet, the duty to retain confidence and protect information shared by a client must require some basic level of cybersecurity vigilance on the part of the attorney. This argument can be advanced in two steps. First, it is the information itself that is protected, and this protection is owed irrespective of the medium of storage. Second, as mentioned above, the Model Code's commentary warns against inadvertent disclosure, which suggests that this duty encompasses not only prohibiting the active breaking of confidences by the lawyer, but also that there exists a minimum level of vigilance owed by the lawyer to protect the information itself. If that is the case, then how is failing to protect client information stored upon a computer any different than failing to protect it when it is stored on paper? A lawyer's duty to ensure that confidential papers

---

116 *Model Code*, *supra* note 88, s 3.3-1.

117 *Ibid*, s 3.3-2.

118 *Ibid*, ats 3.3-1[4] states: "A lawyer also owes a duty of confidentiality to anyone seeking advice or assistance on a matter invoking a lawyer's professional knowledge, although the lawyer may not render an account or agree to represent that person. A solicitor and client relationship is often established without formality."

119 *Ibid*, s 3.3-1[3].

120 *Ibid*, s 3.3-1[7] states: "[s]ole practitioners who practise in association with other lawyers in cost-sharing, space-sharing or other arrangements should be mindful of the risk of advertent or inadvertent disclosure of confidential information." It seems unreasonable to argue that the "inadvertent" disclosure of information is only of concern in an office-sharing situation.

are not exposed to the public logically extends to ensure that electronic forms of that same information be protected. It is the information itself that is protected, not the medium in which it is stored. Other professional legal associations have understood the underlying logic of this argument and cautioned about ignoring cybersecurity protections. Below is a list of opinions concerning the applicability of the duty of confidence to the use of technology by various Canadian legal regulatory bodies.

Federation of Law Societies of Canada

As early as 1999, the Federation of Law Societies took the position that lawyers "using electronic means of communication must ensure that communications with or about a client reflect the same care and concern for matters of privilege and confidentiality normally expected of a lawyer using any other form of communication."[121]

Canadian Bar Association

In 2008, the Canadian Bar Association's Ethics and Professional Responsibility Committee published a supplement to the now defunct CBA Code of Professional Conduct,[122] that stated that the rules regarding confidentiality applied:

"to all forms of communication, including electronic communication using new information technologies. Lawyers must display the same care and concern for confidential matters regardless of the information technology being used. Lawyers must ensure that electronic communications with or about a client are secure and not accessible to unauthorized individuals. When communicating confidential information to or about a client, lawyers should employ reasonably appropriate means to minimize the risk of disclosure or interception of the information."[123]

The CBA's Ethics and Professional Responsibility Committee has acknowledged that while the present rules of professional conduct within the Federation of Law Societies of Canada's Model Code do not offer "specific

---

121 "Guidelines on Ethics and the New Technology" (November 1999), online (pdf): *Federation of Law Societies of Canada* <https://www.nsbs.org/sites/default/files/ftp/tech_ethics_guidelines.pdf>.

122 This is distinct from the Model Code discussed previously. A document that is no longer in existence.

123 The Canadian Bar Association, "Information to Supplement the Code of Professional Conduct, Guidelines for Practicing Ethically with New Information Technologies" (September 2008) online (PDF): *Law Society of Nunavut* <https://www.lawsociety.nu.ca/sites/default/files/website-general/cba_supplemental.pdf> at 5.

guidance" regarding cybersecurity, "[c]onfidentiality may be at risk when using technologies, including, e-mail, mobile devices, remote access, online storage of information (e.g. cloud-based services) and social media."[124]

The Law Society of Upper Canada

The Law Society of Upper Canada has published a "Technology Practice Management Guideline," which provides practitioners with guidance regarding the use of technology in the practice of law. While "not intended to replace a lawyer's professional judgment or to establish a one-size-fits-all approach to the practice of law,"[125] the document does advise that lawyers "using electronic means of communications shall ensure that they comply with the legal requirements of confidentiality or privilege."[126] Additionally, the document provides guidance regarding important cybersecurity topics such as the discussion of technological risks with clients, use of firewalls and security software, encryption, and the use of cloud services.[127]

The Law Society of Manitoba

The previously mentioned 2012 report published by the Technology Committee of the Law Society of Manitoba specifically discussed the applicability of the jurisdiction's code of professional conduct to communications made using electronic media.[128] The Report found that:

the Code of Professional Conduct applies to e-mails, text messages, data stored 'in the cloud' and Facebook as much as it applies to paper files and faxes, a traditional brick and mortar law office or a lawyer's conversation at a cocktail party. The principles of client confidentiality and privacy do not change. The only thing that changes is the way in which the information that must be protected is stored and transmitted. The committee recommended that lawyers be made aware that the Code applies to cyberspace and technology.[129]

---

124 *Practising Ethically with Technology*, CBA Ethics and Professional Responsibility Committee, August 2014 at 3.

125 "Technology" (2019), online: *Law Society of Ontario* <http://www.lsuc.on.ca/For-Lawyers/Manage-Your-Practice/Technology/Technology-Practice-Management-Guideline/> [perma.cc/D23D-JA9L].

126 *Ibid*.

127 *Ibid*.

128 *Technology Committee Report*, *supra* note 107.

129 *Ibid* at 4.

In summary, while the model code does not make specific mention of IT best practices and cybersecurity in its text, it must be logically inferred that the duty of confidence requires lawyers to consider some base level of cyberprotection when handling clients' confidential information. Indeed, numerous Canadian law societies and professional organizations have adopted this position.

C. Duty to Protect a Client's Property

The duty to protect a client's property is closely related to the duty to retain confidences discussed above. The Model Code's commentary on this rule makes this point, saying that the two duties "are closely related."[130] As such, this section will not spend a great deal of time discussing this rule in depth. Overall, the failure to implement appropriate IT security safeguards would likely run afoul of this rule as well.

The rule requiring lawyers to protect their clients' property is found in section 3.5-2 of the Model Code, and reads:

A lawyer must:

a) care for a client's property as a careful and prudent owner would when dealing with like property; and
b) observe all relevant rules and law about the preservation of a client's property entrusted to a lawyer.[131]

The Code defines property rather broadly, stating that property includes:

a client's money, securities as defined in [provincial legislation], original documents such as wills, title deeds, minute books, licences, certificates and the like, and all other papers such as *client's correspondence, files, reports, invoices and other such documents*, as well as personal property including precious and semi-precious metals, jewellery and the like.[132]

---

130 Model Code, supra note 88, s 3.5-2[2] states: "These duties are closely related to those regarding confidential information. A lawyer is responsible for maintaining the safety and confidentiality of the files of the client in the possession of the lawyer and should take all reasonable steps to ensure the privacy and safekeeping of a client's confidential information. A lawyer should keep the client's papers and other property out of sight as well as out of reach of those not entitled to see them."

131 Model Code, supra note 88, s 3.5-2.

132 *Ibid*, s 3.5-1 [emphasis added].

With this definition in mind, it becomes clear that all manner of digital documents, produced during the ordinary course of work on a file, would clearly fall under the scope of this rule. As such, lawyers owe their clients a duty to care for electronic files as if they were a "careful and prudent owner," a standard that, based on the arguments advanced in the previous chapter, would clearly require some form of IT security planning.

D. Conclusion

The Model Code of Professional Conduct does not explicitly discuss cybersecurity and IT best practices. However, it can be logically inferred that the Model Code's duties of competence, confidentiality and to protect clients' property require lawyers to protect their clients' interests by having a basic understanding of the risks inherent in the technology they use and attempting to mitigate those risks. As was demonstrated above, a number of prominent legal organizations in Canada have issued guidance to that effect. While these ethical obligations are of course central to our profession, they are not the only source of normative guidance that compels lawyers to consider the cybersecurity implications of their practice. Privacy statutes, at both the federal and provincial levels, impose a number of obligations upon lawyers regarding the handling of information, and it is to these statutes that we now turn.

III. PRIVACY LEGISLATION IN CANADA

Lawyers and law firms, by virtue of the types of data that they come to possess during the course of ordinary practice, are likely to fall under the purview of various federal and provincial/territorial statutes concerning privacy. These statutes may impose duties upon, and give rise to liabilities for, practicing lawyers with regard to their handling of data and their cybersecurity practices, and as such, must be taken into account when the cybersecurity needs of a law practice are being considered. This section will look at a few of the key statutes that govern this area of law, with special attention paid to instances where legal obligations may arise for practising lawyers. The most comprehensive of these statutes is the federal *Personal Information Protection and Electronic Documents Act*[133] (*PIPEDA*).

---

[133] Personal Information Protection and Electronic Documents Act, SC 2000, c 5

A. Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA came into effect in 2001 and has been updated frequently since.[134] This work will not discuss the *PIPEDA* regime in its entirety, but rather, it will endeavour to provide a brief overview of the Act's scope, requirements and remedial structures. This information will be provided so the reader can appreciate both the likelihood that ordinary legal work may fall under the scope of the Act and the potential consequences of failing to comply with this regime.

One of the remarkable features of *PIPEDA* is the scope of the Act itself, specifically Part 1. By using the federal trade and commerce power,[135] this legislation regulates not only federal works and undertakings, but also undertakings that occur wholly within provinces without legislation deemed to be "substantially similar" to *PIPEDA*.[136]

The Act itself states that Part 1 of *PIPEDA* is applicable to: Every organization in respect of personal information that:

a) the organization collects, uses or discloses in the course of commercial activities; or
b) is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in

---

[PIPEDA].

134 PIPEDA was amended as recently as 2015, with the enactment of the Digital Privacy Act, SC 2015, c 32 [Digital Privacy Act].

135 Constitution Act, 1867 (UK), 30 & 31 Vict, c 3, s 91(2), reprinted in RSC 1985, Appendix II, No 5; Barbara McIsaac, Rick Shields & Kris Klein, The Law of Privacy in Canada (Toronto, ON: Carswell, 2012) at 1.3.3 argue that this "more controversial general branch of the trade and commerce power... allows the federal government to regulate matters affecting the country as a whole."

136 PIPEDA, supra note 133, s 26(2)(b) states: "(2) The Governor in Council may, by order ... (b) if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province." The specific jurisdictions which have "substantially similar" legislation will be discussed below.

> connection with the operation of a federal work, undertaking or business.[137]

There are, of course, limitations on *PIPEDA*'s scope, and one of them is clear from the passage quoted above. Personal information (defined below) held by an employer about an employee in a purely provincial organization would not fall within the jurisdiction of the Act. Additionally, the statute enumerates additional groups outside of its jurisdiction, including government institutions governed by the federal *Privacy Act*, an individual who collects or uses information exclusively for a personal or domestic purpose and an organization who collects information for exclusively journalistic, artistic or literary purposes.[138]

In their text concerning privacy law in Canada, McIsaac, Shields & Klein summarize the scope of *PIPEDA* as such:

> *PIPEDA* applies to the following:
>
> - The collection, use and disclosure of personal information by federal works and undertakings (e.g., banks, airlines, railways, telecommunications companies) and by local works and undertakings in provinces that do not have substantially similar legislation;
> - The collection, use and disclosure of personal information by federal works and undertakings about employees.[139]
>
> The purpose of *PIPEDA*, as stated in the Act, is:
>
> to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[140]

Notably, the term "personal information" is key to the interpretation and functioning of the Act and personal information is

---

137 *Ibid*, s 4(1)(a) & (b).

138 *Ibid*, s 4(2)(a-c).

139 *McIsaac, Shields & Klein, supra* note 135 at 1.3.3. Note: employee-employer information not governed by federal works and undertakings is excluded from *PIPEDA*'s scope.

140 *PIPEDA, supra* note 133, s 3.

defined broadly as "information about an identifiable individual."[141] It is beyond the scope of this work to provide a thorough accounting of the jurisprudence regarding exactly what constitutes personal information, both within the scope of *PIPEDA*, and in other federal legislation such as the *Privacy Act*;[142] instead this section will reference three sources to further define this term. First, in 2011 the Ontario Court of Appeal considered the meaning of personal information within the scope of *PIPEDA* and commented that the definition provided by *PIPEDA* was "*a very elastic definition*, and should be interpreted in that fashion to give effect to the purpose of the Act."[143] Second, returning again to McIsaac, Shields and Klein's text, after having consulted the jurisprudence concerning the term, the authors defined personal information as such:

> The key element in the definition of personal information is the concept of identifiability. To constitute personal information, a data element or compilation of data elements must be attributable to a specific individual.[144]

Third, the Office of the Privacy Commissioner of Canada, in a guide produced to assist organizations with meeting their obligations under *PIPEDA*, defined personal information as including:

> Any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:
>
> - Age, name, ID numbers, income, ethnic origin, or blood type;
> - Opinions, evaluations, comments, social status, or disciplinary actions; and
> - Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).[145]

---

141 *Ibid*, ats 2.

142 *McIsaac, Shields & Klein, supra* note 135 at 4.1.

143 *Citi Cards Canada Inc v Pleasance Eyeglasses*, 2011 ONCA 3 at para 22 [emphasis added].

144 *McIsaac, Shields & Klein, supra* note 135 at 4.1.1.

145 For what is not covered by *PIPEDA*, see "Summary of privacy laws in Canada" (1 January 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-incanada/02_05_d_15/#heading-0-0-2-2-2> [perma.cc/GL77-ZSY2].

It is apparent that the definition of personal information under the *PIPEDA* legislative regime is expansive, and for our purposes, it is plain to see that any number of documents, produced during the ordinary course of a legal practice, would clearly fall within the scope of personal information and would be subject to the obligations imposed by *PIPEDA*. It is to these obligations that we now turn.

When considering the legal obligations imposed upon legal practitioners by the *PIPEDA* regime, there are two provisions that warrant the most attention. The first is section 5(1) of the Act, which requires organizations to "comply with the obligations set out in Schedule 1"[146], to which we shall return shortly. The second is the more general provision found in section 5(3) of the Act, which imposes an obligation upon organizations that handle personal information to act appropriately; this section reads: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[147] The Supreme Court of Canada said this provision is "a guiding principle that underpins the interpretation of the various provisions of *PIPEDA*."[148] In an earlier decision considering this part of the *Act,* the Ontario Court of Appeal held that "Subsection 5(3) further confirms reasonableness as the touchstone of permissible disclosure of personal information under the Act."[149] Accordingly, compliance with *PIPEDA* generally requires organizations to consider their actions through the lens of a reasonableness standard. The legal test for compliance with the reasonableness standard found in section 5(3) of *PIPEDA* is a four-part test, perhaps best summarized by Ontario Superior Court Justice Perell as:

a) Is the collection, use or disclosure of personal information necessary to meet a specific need?;
b) Is the collection, use or disclosure of personal information likely to be effective in meeting that need?;
c) Is the loss of privacy proportional to the benefit gained?; and
d) Is there a less privacy-invasive way of achieving the same end?[150]

---

146 *PIPEDA*, *supra* note 133, s 5(1).

147 *Ibid*, *s* 5(3).

148 *R v Spencer*, 2014 SCC 34 at para 63.

149 *R v Ward*, 2012 ONCA 660 at para 42.

150 *Mountain Province Diamonds Inc v De Beers Canada Inc*, 2014 ONSC 2026 at para 47;

In summary, section 5(3) of *PIPEDA* is a key provision in understanding the legal obligations imposed by *PIPEDA*. Compliance with section 5(3) of the Act, due to its reliance upon the reasonableness standard, is highly contextual and consequently, there exists a multi-factored analytical framework for determining compliance with this provision of the Act.

While section 5(3) imposes a general requirement upon organizations to act reasonably with regard to the collection, use and disclosure of personal information, the Act also includes specific obligations with regard to how personal information is to be handled. As mentioned above, section 5(1) of the Act requires organizations to comply with the obligations set out in Schedule 1 of the Act.[151] This schedule consists of ten general principles, and a number of specific obligations to ensure compliance with those principles.[152] Table 1 briefly introduces some of the key sections that are of relevance for our purposes. This is far from an authoritative discussion of Schedule 1 of the Act itself, but rather is a general overview of some of the more pertinent principles. However, one final item should be noted before we proceed to the principles themselves. The Act makes clear that the use of the word "should" in any of the principles below does not impose a legal obligation upon the organization holding personal information, but rather serves as a recommendation.[153]

Table 1: Key principles within Schedule 1 of PIPEDA.

Principle	Section	Text of the Provision	Commentary
Accountability	4.1	An organization is responsible for personal information	

Perell J synthesized this test from two earlier decisions, the first being a Federal Court decision *Eastmond v Canadian Pacific Railway*, 2004 FC 852 at para 13 where Lemieux J imported the legal test used by the Privacy Commissioner in that case's previous hearing. This structure was also accepted by the Federal Court of Appeal, in *Turner v Telus Communications Inc* Eyeglasses, 2007 CAF 21 at para 15 when Décary JA endorsed and quoted from a lower court decision which used this analytical framework.

151 Additionally, *PIPEDA*, *supra* note 133, s 5(2) is a recommendation, not an obligation; Schedule 1 of the Act is titled "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96."

152 These principles are Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure, and Retention, Accuracy, Safeguards, Openness, Individual Access, & Challenging Compliance.

153 *PIPEDA*, *supra* note 133, s 11(1) still allows complaints to be brought against people for this.

		under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.	
	4.1.3	An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.	
	4.1.4	Organizations shall implement policies and practices to give effect to the following principles: (a) implementing procedures to protect personal information; (b) establishing procedures to receive and respond to complaints and inquiries; (c) training staff and communicating to staff information about the organization's policies and practices; and	

		(d) producing information to explain the organization's policies and procedures.	
Consent	4.3	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.	Section 6 of *PIPEDA* imposes additional criteria with regards to what constitutes knowledge and consent. Section 6.1 states that the consent of a person is only valid "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." Subsections 7(1) – (3) of the Act also provide a number of situations wherein organizations may collect, use and/or disclose information without knowledge and consent.
	4.3.2	The principle requires "knowledge and consent." Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be	

		used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.	
Limiting Collection	4.4	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.	
	4.4.1	Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (discussed below).	
Limiting Use, Disclosure, and Retention	4.5	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the	Sections 7(4) and (5) of the Act provide that disclosure of personal information may be permitted for purposes other than for which it was collected if

		individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.	it was collected under the circumstances set out in 7(2) of the act or circumstances exist such as those enumerated in section 7(3)(a) – (h.1).
	4.5.3	Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.	As mentioned above, section 5(2) of *PIPEDA* indicates that "should" does not establish a legal duty, but rather serves as a recommendation. As such, there is not a strict legal obligation to destroy personal information after it is no longer required. However, organizations should keep in mind the general duty to act reasonably, as set out in section 5(3).
Safeguards	4.7	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.	
	4.7.1	The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.	
	4.7.2	The nature of the safeguards will vary	

		depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection	
Openness	4.8	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.	

In addition to the obligations articulated by the ten principles set out in the Schedule I of the Act and the general duty to act reasonably set out in section 5(3) of the Act, upcoming changes to the *PIPEDA* regime will impose additional legal duties upon persons and organizations who handle personal information. Most notable are a series of provisions that, while not yet in effect, will impose affirmative reporting duties upon organizations that suffer data breaches.

The *Digital Privacy Act*[154] will introduce a number of reporting obligations into the *PIPEDA* statutory regime. This Act received royal ascent in June 2015, but the key provisions to which we will be referring will not come into effect until an order-in-council is made.[155] Section 10 of the *Digital Privacy Act* introduces a new division into *PIPEDA*, to be called "Division 1.1 Breaches of Security Safeguards."[156] This new division will impose a number of legal obligations upon organizations that hold personal information. In particular, they will be required to report breaches of security where personal

154 *Digital Privacy Act*, *supra* note 134.

155 *Ibid*, s 27.

156 *Ibid*, s 10.

information is at risk to both the Privacy Commissioner and the individual affected. The forthcoming section 10.1(1) of *PIPEDA* will require organizations to report to the Privacy Commissioner where there is "any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual."[157]

The language of the forthcoming subsection (3), which requires notification of the affected individual, employs the same language as subsection (1), except that the language is specific in its impact on the affected individual and it imposes a pre-condition that any notification must not contravene other laws.[158] The obligations to report under these yet to be enacted changes will only require reporting of breaches when there exists a "real risk of significant harm to an individual" and the legislation will provide some statutory guidance with regard to what constitutes a real risk of significant harm. Section 10.1(7) of the Act will inform its reader that the concept of "significant harm" is a potentially broad category.

For the purposes of that section, significant harm includes:

bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.[159]

Additionally, section 10.1(8) of the Act will also enumerate factors to be taken into account when assessing the real risk of significant harm, specifically:

a) the sensitivity of the personal information involved in the breach;
b) the probability that the personal information has been, is being or will be misused; and

---

157 The first of these obligations, found in s 10.1(1), requires a report be given to the Privacy Commissioner after "any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual."

158 The organization is also required by s 10.1(3) to notify an individual "of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual," except where informing the person would be in contravention of the law.

159 *Digital Privacy Act*, *supra* note 134, s 10.1(7).

c) any other prescribed factor.[160]

Once an organization is compelled to report its data breach, both the report to the Privacy Commissioner and the notification of the individual must occur "as soon as feasible after the organization determines that the breach has occurred."[161] Additionally, the Act will require that any notification to the affected individual contain "sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm" as well as any other prescribed information.[162] Moreover, such notifications must be made directly to the individual and shall be "conspicuous."[163] Furthermore, under section 10.2(1) of the Act, the organization that has notified an individual of a breach is also required to inform other organizations or government institutions of the breach "if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm."[164] Finally, *PIPEDA* will require that records be kept of all breaches concerning personal information under an organization's control.[165] In summary, these amendments to *PIPEDA* will impose positive reporting obligations upon organizations that suffer data losses, prescribing who is to be notified, when they are to be notified and what said notification must contain. These provisions are rather extensive and practicing lawyers in possession of personal information and under the jurisdiction of *PIPEDA* need be aware of this, or they may face the remedial provisions of the Act.

The final part of the *PIPEDA* legislative regime to be discussed are the remedial provisions. The federal Privacy Commissioner is responsible for investigating and recommending resolutions for breaches of this legislation. Section 11(1) of the Act establishes that an individual may file complaints with the Privacy Commissioner against organizations that breached any of the obligations imposed by *PIPEDA*, or for not following any

---

160 *Ibid*, s 10.1(8).

161 *Ibid*, ss 10.1(2) & (6) for report and notification.

162 *Ibid*, s 10.1(4).

163 *Ibid*, s 10.1(5).

164 *Ibid*, s 10.2(1).

165 *Ibid*, s 10.3.

recommendations set out in Schedule 1. Section 11(2) empowers the Commissioner to initiate an investigation themselves if there are reasonable grounds to investigate a matter.[166] Upon the filing of a complaint, the Privacy Commissioner is required to conduct an investigation, unless the Commissioner believes that the complainant has yet to exhaust available grievance or review procedures,[167] there is another, more appropriate legal remedy available to the complainant,[168] there was an unreasonable delay in the filing of the complaint,[169] or if the commissioner is of the opinion that the alleged violation would be a violation of certain other specific federal acts.[170] Upon commencing an investigation, the Privacy Commissioner is empowered by section 12.1 of the Act to compel witness testimony,[171] administer oaths,[172] receive or admit evidence, including evidence which would normally be excluded by a court of law,[173] and, subject to certain restrictions, enter any premises during the course of the investigation and obtain and examine copies of documents found in the premises.[174] The Privacy Commissioner is also entitled to attempt to resolve disputes by dispute resolution mechanisms.[175]

---

166 *PIPEDA*, *supra* note 133, s 11(2).

167 *Ibid*, s 12(1)(a).

168 *Ibid*, s 12(1)(b).

169 *Ibid*, s 12(1)(c).

170 *Ibid*, s 12(2) includes "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act."

171 *Ibid*, s 12.1(1)(a).

172 *Ibid*, s 12.1(1)(b).

173 *Ibid*, s 12.1(1)(c).

174 *Ibid*, ss 12.1(1)(d)-(f).

175 *Ibid*, s 12.1(2).

Upon the conclusion of a Privacy Commissioner's investigation,[176] and assuming a violation has been found,[177] the Commissioner shall file a report and send copies to both the complainant and the organization[178] detailing their findings and recommendations.[179] Complainants, including the Privacy Commissioner when they take on that role, have a statutory recourse allowing for a review in Federal Court on any matter with respect to the complaint or a matter found in the Commissioner's report,[180] as does the Privacy Commissioner with regard to complaints they did not initiate.[181] While not specifically permitted by the Act, the Federal Court has also held that organizations can initiate judicial review of the Privacy Commissioner's findings.[182] The Act empowers the Court with the authority to dispense remedies for violations of this Act, including ordering organizations into compliance with the Act,[183] ordering organizations to publicize their actions taken or proposed so as to come into compliance,[184] and damages to the complainant, including damages for "any humiliation the complainant has suffered."[185] In addition to the power to initiate investigations and then apply to Federal Court for a hearing on its findings, the Privacy Commissioner also has a number of other remedial or preventative powers. As a means of avoiding a court hearing,[186] the Privacy Commissioner has the authority to enter into compliance agreements with organizations that have, are likely to, or are about to commit an act or omission which would run contrary to the

---

176 No less than 12 months after complaint; see *Ibid*, s 13(1).

177 *Ibid*, s 12.2(1) details those situations where the commissioner may discontinue their investigation; *Ibid*, s 14 allows for a complainant to proceed to federal court seeking to overturn.

178 *Ibid*, s 13(3).

179 *Ibid*, s 13(1)(a).

180 *Ibid*, ss 14(1) & 14(2).

181 *Ibid*, s 15.

182 *Englander v Telus Communications Inc*, 2004 FCA 387 at para 51.

183 *PIPEDA*, *supra* note 133, s 16(a).

184 *Ibid*, s 16(b).

185 *Ibid*, s 16(c).

186 *Ibid*, s 17.1(3)-(4).

Act.[187] The Privacy Commissioner also has the authority, given by Division 3 of the Act, to conduct audits of organizations to ensure compliance if there are reasonable grounds to believe that provisions or recommendations are not being followed.[188] The powers granted to the Privacy Commissioner during an audit are identical to those granted during an investigation.[189]

B. Additional Privacy Statutes

In addition to *PIPEDA*, there are a number of other statutes, both at the federal and provincial/territorial level, that may impose obligations and liabilities on lawyers related to their practices' handling of data and related cybersecurity. Appendix I provides an overview of the relevant legislation in each jurisdiction. This section will briefly overview the recurring legislative themes and structures found throughout the country's privacy laws.

At the federal level, there are acts other than *PIPEDA* with potential privacy implications for lawyers' practices, including the federal *Privacy Act*,[190] which imposes restrictions on how personal information is to be handled by federal government organizations. Lawyers working for or with the federal Crown will need to be aware of these requirements. Additionally, at the federal level, anti-spam legislation[191] imposes strict rules regarding how certain types of electronic information can be used and imposes severe penalties for non-compliance.[192]

---

187 *Ibid*, s 17.1.

188 *Ibid*, s 18.

189 *Ibid*, s 18(1).

190 *Privacy Act*, RSC 1985, c P-21.

191 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23 [*Act to Promote the Efficiency and Adaptability of the Canadian Economy*].

192 *Ibid*, s 51 states if "the court is satisfied" that one or more persons have contravened the Act, then the court has statutory authority to not only provide compensatory damages for losses, damages or expenses suffered by the applicant, but also additional fines, the maximum of which are not to exceed $1,000,000 for each day the contravention

As mentioned at the beginning of this section, *PIPEDA* continues to operate within provinces that do not have "substantially similar" legislation. At the time of writing,[193] three provinces – Alberta, British Columbia and Quebec – have privacy statutes in place deemed to be "substantially similar" to *PIPEDA*. There are some general differences between these provincial Acts and *PIPEDA* (e.g. the provincial acts also apply to employer-employee relationships), as well as differences between the Acts themselves (e.g. the Alberta statute requires data losses to be reported to the province's Privacy Commissioner, who may require notification be given to an affected individual, while the British Columbia Act has no such reporting requirement in the Act or its regulations). Lawyers practicing in these provinces should be familiar with the scope of these pieces of legislation as they have the ability to strongly impact a legal practice.

Most provincial and territorial jurisdictions also possess two additional privacy related statutes that may impact legal practitioners. First, most provinces[194] have a statute governing the collection, use, storage and disclosure of personal health information.[195] These Acts often have a stated purpose of balancing the privacy rights of individuals, the need to secure sensitive data and the need to run an effective health care system. As such, there exists a great deal of overlap in terms of the duties imposed upon the providers of health care in these Acts, and the obligations imposed upon organizations more generally by *PIPEDA*. To that effect, the Acts from Ontario, Newfoundland and Labrador, New Brunswick and Nova Scotia have been deemed substantially similar to *PIPEDA* with regard to their handling of personal health information. Lawyers working for health care providers, or dealing with personal health information, should be aware of these statutes.

The second class of legislation found in most jurisdictions throughout the country are akin to the federal Privacy Act and impose restrictions on how personal information is collected, secured, used and

---

occurred.

193 "Provincial legislation deemed substantially similar to PIPEDA" (29 May 2017), online: *Office of the Privacy Commissioner of Canada* https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp> [perma.cc/PZ4T-MRLL]. [Provincial Legislation similar to PIPEDA]

194 Not PEI.

195 See Appendix I.

disclosed by governmental bodies. These pieces of legislation often also provide individuals with a right to access government information, including both general information and personal information specific to them as individuals, while also providing a statutory mechanism by which such requests can be processed and a number of restrictions, both mandatory and discretionary, are imposed on what can be released. Lawyers working with or for provincial Crowns should be aware of these restrictions.

Finally, there are a number of miscellaneous acts across the country that may impact lawyers and the data management of their practices. Some jurisdictions have acts that create torts for breach of privacy[196] which could impose liability on those lawyers who suffer data breaches.[197] There are also acts that govern the collection of personal information for specific purposes, such as employment or credit,[198] that unaware lawyers could run afoul of during their practice.

C. Conclusion

This section has provided the reader with a brief overview of how our nation's various privacy statutes may impose additional obligations and restrictions upon legal practices with regard to their cybersecurity practices. As has been seen, under the federal *PIPEDA* regime, or the provincial regimes deemed to be "substantially similar," lawyers are subject to a number of affirmative obligations to protect the personal information that they accumulate over the course of practice. The forthcoming changes to *PIPEDA*, specifically its notification requirements, will impose even more substantial obligations upon practitioners of the law. Furthermore, at the federal, provincial and territorial levels, there exists a number of Acts that may impact legal practitioners depending upon their practice areas. As such, the overlap of privacy laws and cybersecurity must be carefully considered by legal practitioners.

Notably, the website of the Privacy Commissioner of Canada contains useful guidelines regarding data privacy, various research papers on

---

196 *The Privacy Act*, CCSM, c P125 [MB Privacy Act].

197 The MB Privacy Act, for example, doesn't require that the breach be wilful, suggesting that negligent actions could bring about liabilities. This is a theoretical argument.

198 *MB Privacy Act*, *supra* note 196.

specific privacy topics,[199] and recommendations regarding data handling best practices resulting from business investigations.[200] These resources should be a useful starting point to assist lawyers in satisfying their professional duties, especially their duty of confidentiality and duty to protect a client's property, as well as their obligations under various pieces of privacy legislation.

---

199 "Explore privacy research" (last modified 14 December 2018), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/> [perma.cc/J95G-3QQ4].

200 "Investigations into businesses" (last modified 17 December 2019), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/> [perma.cc/WAQ5-NU9W].

CHAPTER III: Risk Management and Best Practices

I. Introduction

The last two chapters have presented the reader with evidence of cybersecurity threats and explained why lawyers need to care about these threats. This chapter deals with risk management and best practices for legal practitioners. Lack of cybersecurity investment can lead to serious losses for individuals, companies and government agencies.

A breach in client confidentiality due to a failure to proactively employ cybersecurity methods may be grounds for a negligence suit. Lawyers can benefit from consulting best practice guidelines developed by professional associations and standards organizations, for instance, the British Columbia Law Society report on cloud computing.[201] Other professional tips are available on a number of topics, including strategies to limit the quantity and redundancy of data that many law firms hold.[202]

The focus of this chapter is to provide the reader with a general framework regarding how one should think about cybersecurity in a law firm. A non-exhaustive list of specific practice tips for all areas of IT is included.

In short, this chapter will help the reader address the problems introduced in chapter I and maintain compliance with obligations discussed in chapter II.

---

201 Gavin Hume, Bruce LeRose, Peter Lloyd and Stacy Kuiack, "Report of the Cloud Computing Working Group" (27 January 2012), online (pdf): *The Law Society of British Columbia* <https://www.lawsociety.bc.ca/Website/media/Shared/docs/publications/reports/CloudComputing_2012.pdf> [perma.cc/A5Z6-67JX].

202 Randolph A. Kahn, "Why Destruction of Information Is So Difficult and So Essential: The Case for Defensible Disposal" (15 June 2018), online: *Business Law Today* <https://businesslawtoday.org/2018/06/destruction-information-difficult-essential-case-defensible-disposal/> [perma.cc/7376-T6KM].

II. RISK MANAGEMENT

A. General Framework: What is Risk Management?

There is no such thing as perfect security. "No security system is guaranteed to be impenetrable."[203] We must disabuse ourselves of that notion immediately. Even if there was, a perfect security system would not likely be desirable. What if one loses a password? An impenetrable security system might make it impossible to regain access to information if the password is lost. This paradox reiterates the need to balance convenience and security. Fundamentally, security systems must enable lawyers to carry out their obligations to clients by accessing information while prohibiting terrorists or hackers with said access.

Risk management can help lawyers strike the right balance between security and efficiently operating a business. Risk management has been defined as:

The discipline of identifying, monitoring and limiting risks. In some cases, the acceptable risk may be near zero. Risks can come from accidents, natural causes and disasters as well as deliberate attacks from an adversary. In businesses, risk management entails organized activity to manage uncertainty and threats and involves people following procedures and using tools in order to ensure conformance with risk-management policies. Risk management is also used in the public sector to identify and mitigate risk to critical infrastructure. Some traditional risk management programs are focused on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, ergonomics, death and lawsuits).[204]

Identifying, assessing and limiting IT risks has become central to law firms.[205] Some organizations guide businesses to reduce risks by providing standards for cybersecurity. The International Standards Organization (ISO) has created an internationally recognized guidance standard that provides a

---

203 *ABA Handbook*, *supra* note 5 at 113.

204 Sousa Emilio & Jordão Benigno, *Risk Management* (New York: Nova Science Publishers, Inc, 2010) at vii.

205 Robert S. Kaplan & Anette Mikes, "Managing Risks: A New Framework" (1 June 2012), online: *Harvard Business Review* <https://hbr.org/2012/06/managing-risks-a-new-framework> [perma.cc/NHW9-LRCQ].

framework of methods and processes to identify, assess and minimize IT risks in any organization.[206]

There are a number of ways of thinking about risk management; we conceptualize it as having two stages: 1) identification of risk and 2) response to risk. These two steps must be balanced together to enable efficient risk management.

B. Identification of Risk

To prevent and manage risk one must first be able to identify the risk. A third-party professional may be able to help identify specific risk within your organisation. In general, cybersecurity risks may be categorized into technical vulnerabilities and human vulnerabilities.

Technical vulnerabilities: These are vulnerabilities inherent within hardware components that make up a computer network and the vulnerabilities of software running on said networks. In order to properly carry out a legal risk assessment, which includes assessing the risk of reputational damage and financial loss, legal professionals may have to collaborate with a third party that can give accurate insight into any existing technical vulnerabilities.

Human vulnerability: A largely underestimated factor in identification of risk is the human factor, not the technological factor. This is at times counter-intuitive, as people tend to think about cybersecurity as more of a technical issue, forgetting that it also involves human resource management. In fact, the exploitation of human weakness through creative spear phishing attacks has increased over the years and has become a primary cybersecurity risk.[207] The modes of cyberattacks should be made familiar to all staff by training efforts in attempt to reduce the chances of a cyberbreach caused by human vulnerabilities.

Another human component to cybersecurity issues are insider threats. Breaches in cybersecurity caused by insider threats can be malicious or negligent or simply made by mistake. Motivation for staff to steal data is varied. For example, financial gain in the form of theft of trade secrets or

---

206 "35.030 - IT Security," online: *International Organization for Standardization* <https://www.iso.org/ics/35.030/x/> [perma.cc/3HQS-WAYE].

207 David Asselstine, "Cyber-Risk. A Breach May be Inevitable," Plans & Trusts (March/April 2018).

intellectual property, or revenge for personal reasons for perceived wrongs committed against the employee or partner.[208] Protecting the organization against external threats does not address the potential data breaches caused by insider malfeasance regardless of whether the conduct was intentional, malicious, ignorant or accidental.[209] For more information on how to reduce insider threats, see the Carnegie Mellon University best practices guide.[210]

A general protocol for a risk assessment should include:

1. Evaluate the likelihood and impact of potential risks to sensitive and confidential information;
2. Implement appropriate security measures to address the risks identified in the risk analysis;
3. Document the chosen security measures, and where required, the rationale for adopting those measures;
4. Maintain continuous, reasonable and appropriate security protections.[211]

More specifically, a cybersecurity action plan should address the following vulnerabilities:

1. Email scams
2. Browser and surfing dangers
3. Malware infections
4. Weak and overly used passwords
5. Operating system vulnerabilities
6. Vulnerable networks
7. Weak system configuration
8. Lost or compromised devices/data
9. Confidential information on discarded equipment
10. Remote access and public computer
11. Unsecured mobile devices
12. Public Wi-Fi and weak wireless and Bluetooth settings
13. Cloud storage and computing

---

208 ABA *Handbook*, *supra* note 5 at 20.

209 *Ibid* at 21.

210 George Silowash et al, "Common sense guide to mitigating insider threats 4th edition" (December 2012), online (pdf): *Carnegie Mellon University* <http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf > [perma.cc/W2VQ-WCLQ].

211 ABA *Handbook*, *supra* note 5 at 30.

14. Insider threats
15. Policies relating to personal versus firm owned computers
16. Data backup[212]

C. Response to Risk

Once risks are identified, suitable protocols may be designed to avoid events that are expected to cause loss. In situations where the complete avoidance of risk is not possible, methods should be employed to lessen the chances that a damaging event occurs – a strategy called risk reduction.[213] It would be wise for firms to also explore risk sharing options, which dilutes the effect of damaging events. In the event that engaging with technology has manifested into a scenario causing loss (i.e. a cyberbreach has occurred), one may at least take strides to mitigate the expected loss of said event. Thus, an intelligent cyberbreach reaction plan may be worth investing in. More details on these overarching concepts are provided below. The keen reader should contemplate how to apply the principles set out below to their specific practice in order to avoid a catastrophic disaster in favour for an incremental failure if a cyberbreach should occur.[214]

Risk Avoidance

The risk associated with technology could be avoided by refraining from the use of technology. However, it would be difficult for a lawyer to honour ethical obligations to be efficient and effective in providing legal services if they were to avoid communicating using technology. Paradoxically, this leaves the legal professional with the option of carrying out business efficiently by using potentially dangerous technology or inefficiently by avoiding said technological dangers. In order to best serve clients, lawyers

---

212 Kelly Friedman et al, Cybersecurity: Best Practices for Protecting Your Law Firm or Legal Practice, Webinar on Information Technology & Intellectual Property Law (Toronto: Ontario Bar Association, 2015) at 13-14; "" (last modified 18 July 2017), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/02_05_d_70_pw/> [perma.cc/QA2T-ZYBQ].

213 Douglas W. Hubbard, The Failure of Risk Management: Why It's Broken and How to Fix It (Hoboken: John Wiley & Sons, 2009) at page 27.

214 Michel Crouhy, Dan Galai & Robert Mark, The Essentials of Risk Management, 2nd ed (New York: McGraw-Hill, 2014) at page 3.

should embrace the use of technology while employing methods to avoid risk of a cyberbreach. Proficient use of technology in combination with risk avoidance strategies could help satisfy a lawyer's duties of confidence, competence and quality of service while maintaining compliance with rules of professional regulatory bodies and statutes.

Good file management and knowledge of when files can be disposed of may help in avoiding a cyberbreach. For example, a lawyer is required to retain documents for the law society,[215] the Canada Revenue Agency,[216] and under privacy laws. However, holding records longer then required unnecessarily exposes a lawyer to a cybersecurity breach, which can easily be avoided by disposing records in a timely manner.

Risk Prevention and Mitigation

Understandably, it is not always possible to avoid risk. However, firms can implement measures to reduce the risk of a security breach, some of which include: diligent use of encryption, strengthening the security of programs installed on office computers, storing digital documents securely, implementing policies to restrict certain uses of technologies, educating personnel about information security, and strengthening overall IT risk management practices.[217]

Due to human vulnerabilities, the success of a firm's cyberbreach risk prevention and mitigation strategy will be highly dependent on its staff. To this extent, staff training should be a priority for law firms. Lawyers should also keep up to date on imminent cyber threats, especially those relating to the specific industries they serve. In this regard, the Canadian Centre for Cyber Security, which issues alerts on certain imminent cyberthreats,[218] is a useful resource for lawyers to become familiar with.

---

215 Law Society of Manitoba, Rules of the Law Society of Manitoba, Winnipeg: LSMB, 2002, s 5-54(1) states that "A member must: (a) keep the books, records and accounts referred to in this division for at least ten years; and (b) on the completion and closing of a client's file, place on the file a copy of the individual client trust ledger."

216 Income Tax Information Circular, IC05-1R1 (2010) at s 8.

217 "The Risk IT Framework Excerpt" (2009) at 28, online (pdf): *ISACA* <http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf> [perma.cc/L8CA-WT8R].

218 "Alerts & Advisories" (last accessed 11 March 2020), online: *Canadian Centre for Cyber Security* <https://www.cyber.gc.ca/en/alerts-advisories> [perma.cc/ZQ9L-PB6G].

Ultimately, technology rapidly changes. It is best practice to keep pace with the newest security technology and to train staff accordingly.

Clear and organized risk reduction protocols are an easy way for management to reduce the chances of a disaster. In fact, some agencies have developed their own protocols on how professionals should handle information. For example, the Canada Revenue Agency states that all information stored in rewritable media must be backed up to avoid loss, damage, or alteration, and stored in a hazard free environment.[219] Hence, a comprehensive risk reduction procedure from relevant external agencies along with in-house procedures should be compiled and implemented as the standard practice within law firms.

Documents management policies are used to improve the efficiency of how a firm manages documents and a documents retention policy establish how a company manages data from a compliance perspective.[220] An organization may wish to implement a cybersecurity policy within, or alongside, a general documents management policy or document retention policy. Doing so will clarify to employees and clients how the firm expects data to be dealt with in the course of business, which should help prevent data breaches. Notably, the CRA provides policies on electronic substitutes for documents, which provides a useful starting point for firms interested in implementing a document retention policy.[221]

---

219 Income Tax Information Circular, *supra* note 216 at s 15 states: "Records that are retained by copying or backing up the data to another medium must be done so in accordance with the media manufacturers' suggested procedures with particular attention given to the suggested shelf life of the medium. Information recorded on rewritable media such as computer hard disks must be backed up on tape or other suitable medium to avoid accidental loss, deletion, or erasure of the recorded information. The media containing the recorded information must be stored in an environment free from hazards that could affect the media, such as magnetic fields, direct light, excessive moisture, and temperature extremes."

220 "What's the Difference Between Document and Records Management?" (last accessed 11 March 2020), online: *Laserfiche* <https://www.laserfiche.com/ecmblog/whats-the-difference-between-document-and-records-management/> [perma.cc/U3AV-JKR5]; "Document Management Policy: 10 Step Development Process" (29 October 2019), online: *LBMC* <https://www.lbmc.com/blog/document-management-policy-development/> [perma.cc/P4YS-59UU].

221 "Acceptable Format, Imaging Paper Documents, and Backing up Electronic Files" (last modified 24 February 2020), online: *Government of Canada* <https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/keeping-records/acceptable-format-imaging-paper-documents-backing-electronic-files.html>

Although a document management policy and a document retention policy can help mitigate the risk of electronic records being hacked, the maintenance of documents in electronic format, especially where the original paper-and-ink format has been destroyed, may create legal risk. A brief discussion on this topic follows.

***i.* Electronic Records**

Some statutes provide specific language regarding the expectations of electronic records that are subject to the statute. For example, Part 2 of *The Electronic Commerce and Information Act*[222] provides that, where a "designated law" of Manitoba provides that information or a document be in a particular format (e.g., "written"), that requirement may be satisfied by an electronic format that is "functionally equivalent" to a paper-and-ink format. Part 2 of the *Electronic Commerce Act* goes on to set out a "functional equivalence" standard for electronic documents, by providing that an electronic version of a document satisfies a legal requirement that the document must be "in writing,"[223] a legal requirement to provide an "original" version of a document,[224] and a legal requirement to "retain" a document,[225] when certain conditions are met.

As noted above, Part 2 of the *Electronic Commerce Act* only applies to "designated laws." The regulation accompanying the *Electronic Commerce Act* lists only a very small number of statutes, relating to issues such as registration of businesses.[226]

Although the inapplicability of Part 2 of the *Electronic Commerce Act* to a specific statute is not fatal to one's ability to manage records, designation under Part 2 of the *Electronic Commerce Act* would bolster the certainty of the view that one can rely on electronic documents (including electronic copies of paper-and-ink documents that are later destroyed). To the extent that there

---

[perma.cc/U25L-6EPX].

222 *The Electronic Commerce and Information Act* (Manitoba), CCSM c E55 [Electronic Commerce Act].

223 *Ibid*, s 12(1).

224 *Ibid*, s 14.

225 *Ibid*, s 15(1).

226 Electronic Documents Under Designated Laws Regulation, Man. Reg. 152/2011 at Schedule 1.

is a conflict regarding document retention requirements found in a specific act and the *Electronic Commerce Act*, the specific act will prevail.

Legislation such as *The Pension Benefits Act*[227] of Manitoba (and its accompanying regulations) provides that the requirement to retain records subject to the act may be satisfied by the retention of an electronic record under certain conditions.[228] Remember to exercise caution about the effect of electronic record requirements in specific legislation because multiple statutes may apply to any given matter, and each statute may have differing requirements on how it can be shown that the electronic version is accurate along with different minimum retention periods.

It is important to also consider the various Evidence Acts that may be applicable once litigation commences. The Canada Standards Council document on the use of electronic documents for evidentiary purposes states by way of introduction that:

"An organization must always be ready to produce its records as evidence in legal proceedings. To ensure their reliability, integrity and authenticity, organizations should consider the application of standards. To enhance the admissibility and the weight (probative value) of electronic records as evidence in legal proceedings, organizations should apply the principles and procedures outlined in this standard."[229]

Under the common law, courts have tended to accept electronic records into evidence only where there is satisfactory evidence regarding the authenticity, reliability and trustworthiness of the records.[230] However, both *The Manitoba Evidence Act*[231] and the *Canada Evidence Act*[232] provide for the

---

227 *The Pension Benefits Act*, CCSM c P32.

228 *Pension Benefits Regulation*, Man. Reg. 39/2010, s 3.38(2).

229 Canada Standards Council, "Electronic Records as Documentary Evidence", CAN/CGSB-72.34-2005 at p viii; A newer version of this document has been published in 2017: Canada Standards Council, "Electronic Records as Documentary Evidence", CAN/CGSB-72.34-2017.

230 Sopinka, Lederman & Bryant, *The Law of Evidence*, 2nd ed. (Markham, Ont: Butterworths, 1999) at §6.173, 6.174 and 18.24, cited in Bradley J Freedman, "Electronic Contracts Under Canadian Law – a Practical Guide" (2000) 28:1 Man LJ 1 at page 56.

231 *The Manitoba Evidence Act*, CCSM c E150, ss 51.1-51.8.

232 *Canada Evidence Act*, RSC 1985, c C-5, ss 31.1-31.8.

authentication of electronic documents. The effect of these provisions is that:[233]

- A person who wishes to introduce an electronic record into evidence must first prove the record is authentic.
- The "best evidence rule" (which requires that original documents that can be readily obtained must be used as evidence, rather than copies) is satisfied, if the electronic record has been produced and stored pursuant to a comprehensive document retention policy.
- The integrity of an electronic records system is proven by indicating that:
    - at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system; or
    - the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or
    - the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Thus, to the extent that one wishes to rely on the provisions of these Evidence Acts (and those with similar language) concerning authentication of electronic documents, it would seem prudent to put a comprehensive and documented policy in place. This comprehensive policy (the content of which would be guided by legal and best practices standards) could then be cited whenever the need arises.

Whether or not an electronic document is authentic is only half of the equation. To be used in a court proceeding, a document must also be admissible. Documentary evidence (whether pen-and-ink or electronic) is *prima facie* inadmissible because of the hearsay evidence rule: if the person who created the document is not present to testify, the court is being asked

---

[233] See, generally, Freedman, *supra* note 230 at page 55.

to consider an out-of-court statement that has been tendered to prove the truth of its contents.

However, the common law and the Manitoba and Canada Evidence Acts have created a number of exceptions to the application of the hearsay rule to documentary evidence. Individuals planning to rely on electronic documentation in the place of paper-and-ink originals should take steps to ensure that electronic documentation will be admissible in future court proceedings.[234] Indeed, Manitoba and Canada Evidence Acts provide that:

- For the purpose of determining whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice regarding how electronic records are to be recorded or stored, having regard to the type of business or endeavor that used, recorded or stored the electronic record and the nature and purpose of the electronic record.[235]

Taken literally, these provisions may not apply to an electronic copy of a paper-and-ink original document. However, an Alberta provincial court judge specifically admitted certain electronically imaged copies of original documents that had been destroyed[236] based on the *Alberta Evidence Act*[237] (which contains similar language to the Manitoba and Canada Evidence Acts) partly because the standards for admission as an electronic document under CAN/CGSB 7234-2005[238] were satisfied.

Unfortunately, it is not absolutely clear, under the precise wording of these statutes, whether these statutory provisions would apply to all types of electronic records of otherwise applicable government and business records. In New Brunswick, by contrast, the Legislature[239] has provided an absolutely explicit blessing of the admissibility of electronic images of documents, in lieu of pen-and-ink originals.[240]

---

234 Detailed recommendations on how to do this discussed in Electronic Records as Documentary Evidence (2017) *supra* note 229.

235 *The Manitoba Evidence Act*, *supra* note 231 s 51.6; *Canada Evidence Act*, *supra* note 232 s 31.5.

236 *R v Oler*, 2014 ABPC 130 at para 4.

237 *Alberta Evidence Act*, RSA 2000, c C-18, ss 41.1-41.8.

238 Electronic Records as Documentary Evidence (2005), *supra* note 229.

239 *Evidence Act*, RSNB 1973, c E-11, ss 47.2(1) and (2).

240 See, generally, Ken Chasse, "Electronic Records as Documentary Evidence" (2007), 6

There can be no doubt, whatever the legal technicalities, that the underlying logic and policy of the Manitoba and Canada Evidence Acts is entirely favourable to the admissibility of electronic copies of paper-and-ink documents. The statutes acknowledge that government and business records are prima facie reliable and admissible, notwithstanding the hearsay rule. The statutes also refer to tests for establishing the reliability of electronic documents. If it can be shown, via the "system integrity" route:

- that an electronic document is a reliable copy of a paper-and-ink original; and
- that the original document is itself admissible as a business or government record,

then, the policy behind these statutes clearly requires that the electronic document should be admissible.

Even if a court was to find that the statutory evidence rules must be read in a narrow and literal way (and thus, would not directly allow for the admission of electronic images of paper-and-ink documents), a court could still find the electronic versions are admissible under the common law.

The courts have established that statutory evidence rules supplement the common law, but do not replace it.[241] At common law, evidence can be admitted notwithstanding the hearsay rule (and the absence of a recognized exception to the rule), if the evidence is necessary and reliable.[242] A demonstrably authentic copy of a paper-and-ink business or government record would appear to satisfy these requirements.

Although the current state of the law, destroying paper-and-ink records in favour of electronic records may create a legal risk, however, said risk can be mitigated by abiding by electronic records keeping best practices,[243] relevant evidence acts, and with industry standards. Thorough document management and document retention policies should address the requirements necessary to legally maintain records (including the admissibility of the documents in court) as well as cybersecurity mitigation matters.

Canadian Journal of Law and Technology 141.

241 *R v Starr*, [2000] 2 SCR 144 at para 3.

242 *Ibid.*, at para 213.

243 Electronic Records as Documentary Evidence (2017) *supra* note 229.

Risk Sharing

Perhaps the most overlooked aspect of a risk management plan is risk sharing, which involves the transfer of risk from the lawyer to an individual or a pool of insurance holders. This can be done in a number of ways:

1. **Insurance.** Insurance can reduce financial losses from a data breach; however, lawyers should be conscious of the difficulty in indemnifying reputational damage. In Ontario as of 2014, LAWPRO offers coverage up to $250,000 for losses related to cybercrime.[244] Lawyers should be mindful of any exclusions for cyber-related coverage.[245] Insurance coverage for the loss due to phishing schemes have been denied because of exclusions in insurance policies.[246]
2. **Informed consent of client / retainer**. Retainers partially aim to protect the solicitor-client relationship as well as to shield the lawyer from liability. Ensuring the client is protected by taking proper precautions, and that the client is informed of the risks associated with technology use are important aspects of retainers. In the event of a cyberbreach, a proper retainer agreement may salvage the client-lawyer relationship.

Retainer agreements between a lawyer and a client may stipulate that the client assumes a reasonable risk to disclosure of confidential information while using information technologies to communicate with the lawyer and third-party service providers.[247] Informed consent to risk has its own

---

244 Friedman, *supra* note 212 at 56.

245 Tana Christianson, "Your Professional Liability Insurance and Cyber Coverage" (October 2012), online (pdf): *Law Society of Manitoba* <www.lawsociety.mb.ca/publications/technology-articles/TECH_Oct2012.pdf>.

246 Martin P.J. Kratz, "Cybersecurity—Loss Due to Social Engineering Attack Covered Under Insurance Policy" (3 August 2018), online (blog): *Bennett Jones* <https://www.bennettjones.com/en/Blogs-Section/Cyber-Security-Loss-due-to-Social-Engineering-Attack-Covered-Under-Insurance-Policy> [perma.cc/E6UQ-RKYC]; *Dentons Canada LLP v Trisura Guarantee Insurance Company*, 2018 ONSC 7311 [*Dentons*]; *The Brick Warehouse LP v Chubb Insurance Company of Canada*, 2017 ABQB 413.

247 "General Retainer Agreement" (July 2015), online (pdf): *Gardiner Miller Arnold LLP* <https://www.gmalaw.ca/wp-content/uploads/2015/07/General_Retainer_Agreement.pdf> [perma.cc/2U9M-ZUG5].

paradoxes: the more explicit a lawyer is about what purposes data is being used for and the modes of communication used, the more likely it is that a hacker can employ a targeted attack. For example, if the agreement establishes that the communication between lawyer and client will be on cell phones, then hackers would know to target phones.

A possible clause to include in a retainer agreement may be the following:

The client recognizes the risks of communicating with the lawyer via Internet and cell phones. No technology is perfect and absolutely secure. The client acknowledges this risk and releases the lawyer from any liability should those services be compromised, and the information be accessed by unauthorized parties, altered or corrupted in any way.

Such a clause may not release the lawyer completely from privacy law obligations and professional duties, but it may be a partial defence and shield for some torts, specifically negligence, breach of contract and breach of fiduciary duty.

Under privacy legislation, it is possible to get informed consent to a reasonable risk. However, asking a client to endure an unreasonable risk (e.g. I will be dealing with you by way of ordinary internet unless you tell me otherwise) will not shield the lawyer from cyberbreach liabilities under ethical responsibilities and privacy law.

Reacting to a Cyberbreach

A reasonable cybersecurity risk reduction plan should be developed by management leadership in collaboration with technical staff. Proper documentation of the methods employed will help with proving due diligence in protecting client's information. In a cybersecurity breach does occur, mitigation of damages is the only avenue left. Thus, it is important to have an incident response plan in place.[248] Some useful procedures to include in an incident response plan are:

- for your records, keep note to on how the cyberbreach happened to the best of your knowledge,
- send notifications to implicated parties and the authorities,
- wipe lost or stolen devices remotely, and
- revoke remote-access credentials.

---

248 Friedman *supra* note 212 at 55.

III. BEST PRACTICES

A. General

Computer security requires a combination of human resource management, safe computer practices and up to date technology. The foundation to an effective cybersecurity plan is good organisation. No plan will have only one course of action, but rather multiple steps and strategies to minimize risks.

IT security is everyone's responsibility. While it is important to have professionals who you can trust to assist with this work (perhaps even in-house, depending on a cost analysis), it is important to remember that this is not just the IT professional's problem or concern. Every staff member needs to be aware of IT security. Management should adopt a leadership role in IT security. Ideally, there will be a management structure in place to support IT security projects. All new hires should be trained as per the cybersecurity policy and sign a document that outlines their responsibilities. Hiring an IT security professional or contracting out IT security services that work on an as needed basis are good options, depending on the size of the law firm.

Encryption should be widely adopted but beware of its limitations. Encryption refers to the process of encoding data to ensure the confidentiality of the information. It also allows for verification of the origin of the message (authentication), integrity of the message and non-repudiation as the sender of the communication cannot deny sending it.[249] Encryption uses algorithms to convert data into undecipherable text that require a specific key (password) to make it readable again.[250] Although it is not impossible to crack encryption, it is still highly advisable to encrypt files, including communications, as it adds another layer of security that hackers

---

249 Margaret Rouse et al, "Encryption" (November 2014), online: *TechTarget* <http://searchsecurity.techtarget.com/definition/encryption> [perma.cc/Y6QE-QNVF].

250 Tuomas Rantalainen, "How does Encryption Work? (and Why it's So Important)" (1 September 2016), online (blog): *F-Secure* <http://safeandsavvy.f-secure.com/2016/09/01/how-does-encryption-work-and-why-its-so-important/> [perma.cc/8GVR-RYPA]; Charles Arthur, "How Internet Encryption Works." (5 September 2013), online: *The Guardian* <https://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works> [perma.cc/7FKG-PTFH].

would need to surpass in order to get your data. For most of what is going to be discussed below, be it email, computer use, phone use, tablet use, or thumb drives, encryption is a keyway of ensuring that data is protected. However, encryption does have its own risks. In particular, data may become unreadable if the encryption key is lost.

Other general best practices include ongoing staff training on cybersecurity, using up to date cybersecurity software, and hiring cyber consultants to audit and make recommendations on currently used protocols.

B. Bring Your Own Device (BYOD)

Staff should be aware of whether devices used for personal and work purposes are personally owned or owned by the firm and enabled to provide personal functionality. If the latter is true, staff should ensure users of devices keep up to date with security updates. It may be more difficult for a firm to force compliance with particular cybersecurity practices on personally owned devices. Whether a device is owned by a firm or not, personal use of devices can increase the risk of a cybersecurity breach.

One way to improve the security of client data on devices enabled with personal use is to employ Mobile Device Management (MDM) strategies. MDM provides a centralized way to manage mobile devices (such as phones, laptops, and tablets) remotely, including the ability to lock or erase a lost device remotely and check its geographical location.[251] It is essential that firms retain the ability to secure, control and remotely erase firm data on employee-owned devices in the event of a security breach.[252] Moreover, a firm's software and data that is managed on external servers can offer additional security if the firms data is not stored in the local memory of the employee's personal device.[253] To reduce the risk of a cyberbreach caused by a lost or stolen password, firms should employ multi-factor

---

251 *Ibid.*

252 Paul Martine, "How to Successfully Implement A 'Bring Your Own Computer' Program in Your Office" (8 April 2011), online: *Business Insider* <http://www.businessinsider.com/top-tips-for-successfully-introducing-byo-2011-4> [perma.cc/WV4U-CVSM].

253 "Best Practices to Make BYOD, CYOD and COPE Secure and Simple" (2017), online (pdf): *Citrix* <https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/byod-best-practices.pdf> [perma.cc/RWN7-SV3L].

authentication strategies to allow employees access to firm data from any remote device.[254]

In the end, a policy is necessary that clearly demarcates responsibilities and expectations. Specifically, firms should be aware of the strategies they employ to protect client data. BYOD policy templates are available and may be a good starting point for developing a solicitor-client specific program.[255]

C. Cell Phones / Tablets (Including BYOD)

Cell phones, and to some degree tablets such as iPads, are becoming a more crucial component of how business is conducted.[256] Ultimately, a firm will be faced with similar issues to BYOD computer policies for mobile devices. It is key to find an acceptable balance of cost/convenience versus control/security. Most importantly, cell phones need to be encrypted as a preventative measure. This is a default feature of most modern cell phone operating systems. For example, Android cell phones and tablets come with a feature to encrypt them.[257] Apple devices also have encryption features enabled by default so that IT specialists do not need to perform custom configurations.[258] However, this encryption does not guarantee absolute cyber-security. Vendors sell tools which can decrypt some forms of encryption. Often, only having a password to encrypt the device may not be enough. Nevertheless, access passwords most definitely should be used as a minimum level security measure.

---

254 James L. Pray, "Targeted Cyber Attacks Are Rapidly Increasing in 2019" (22 May 2019), online: *Best Lawyers* <https://www.bestlawyers.com/article/targeted-cyber-attacks-increasing/2460> [perma.cc/XP6R-VMKP].

255 Megan Berry, "BYOD Policy Template" (12 July 2012), online: *IT Manager Daily* <http://www.itmanagerdaily.com/byod-policy-template/> [perma.cc/2VH9-UFH9].

256 *ABA Handbook*, *supra* note 5 at 18-19.

257 Robert Triggs, "How to encrypt your Android device" (17 January 2017), online: *Android Authority* <http://www.androidauthority.com/how-to-encrypt-android-device-326700/> [perma.cc/5HHU-U2DA].

258 "iOS Security" (January 2018), online (pdf): Apple <https://www.apple.com/business/docs/iOS_Security_Guide.pdf> [perma.cc/9YD9-X625].

On phones that are owned by firms, MDM software is strongly suggested.[259] A company can control a device using MDM software, enabling added protection to the remote wiping capacity offered by android and iOS systems.[260]

The use of MDM can also be complemented with acceptable use policies for both corporate and personal owned devices. Acceptable use policy templates for mobile devices are available and may be tailored for solicitor-client specific purposes.[261]

D. Office Networks – Wi-Fi

Computer networks enable communication between devices. Wi-Fi technology is a popular method of enabling wireless networking. Reliance on Wi-Fi presents a potential security issue, as it creates opportunities for hackers to access sensitive data such as passwords for logging into corporate networks and online banking sites.[262] Firms should ensure that devices employ the most up to date Wi-Fi protected access (WPA) security protocols.[263] WPA security protocols ensure that only authorized users have access to the wireless network.[264] Firms wanting to allow clients and guests

---

259 Paul Ferrill, "The Best Mobile Device Management (MDM) Solutions for 2017" (20 June 2017), online: *PC Magazine* <https://www.pcmag.com/article2/0,2817,2500510,00.asp> [perma.cc/M2C3-WWDE].

260 Adam Stein, "How does mobile device management (MDM) work?" (13 February 2012), online: *Network World* <http://www.networkworld.com/article/2185771/tech-primers/how-does-mobile-device-management-mdm-work-.html> [perma.cc/957Z-RETK].

261 "Sample Corporate Mobile Device Acceptable Use and Security Policy." (2017), online (pdf): *Wise Gate IT* <http://wisegateit.com/resources/downloads/wisegate-sample-byod-policy.pdf?_ga=1.166862838.993227471.1475359178>; "Bring Your Own Device (BYOD) and Acceptable Use" (2012), online (pdf): *The Horton Group* <https://www.thehortongroup.com/sites/default/files/pdf/1012201348157320.pdf> [perma.cc/Q2K2-5BMR].

262 *ABA Handbook*, *supra* note 5 at 25.

263 "Wireless fundamentals: Encryption and authentication" (3 February 2015), online: *Meraki Documentation* <https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wireless_fundamentals%3A_Encryption_and_authentication> [perma.cc/T8ZS-CB7G].

264 "Discover Wi-Fi Security," online: *Wi-Fi Alliance* <http://www.wi-fi.org/discover-wi-fi/security> [perma.cc/2MGV-GLFB].

with Internet access should consider having two wireless networks.[265] A public Wi-Fi network separate from the network used by staff could enable guest access to the Internet while ensuring greater security of company data.

E. Public Wi-Fi

Public Wi-Fi is inherently risky, especially when there is no encryption/password requirement (for example, at some restaurants and cafes). It is highly advisable not to use public Wi-Fi for any device carrying confidential information.[266] One possible way to address security concerns in the use of a public Wi-Fi is by way of Virtual Private Networks (VPN).[267] VPNs act as another form of encryption, re-routing all Internet traffic to an encrypted private network while using the public Wi-Fi.[268] However, one must be wary of free VPNs. It is advisable to read terms of service regarding encryption, access to data, and confidentiality.

F. Cloud Computing and Data Storage

In general, 'the cloud' refers to a pool of external servers on which computations may be carried out and which data may be stored on.[269] The benefits of cloud computing include greater protection from data loss since data is redundantly stored on multiple servers and convenient access and sharing options since users can log into the cloud from multiple devices. Despite the advantages of cloud computing, privacy and security concerns continue to be a critical issue.[270]

---

265 ABA *Handbook*, *supra* note 5 at 119.

266 *Ibid*.

267 *Ibid*.

268 Jon G, "What is a VPN? Virtual Private Network explained" (27 October 2016), online (blog): My-Private-Network <https://www.my-private-network.co.uk/what-is-a-vpn-virtual-private-network-explained/> [perma.cc/6YAB-ZKWY].

269 Wayne Jansen and Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing" (December 2011) at 4, online (pdf): National Institute of Standards and Technology <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf> [perma.cc/K7K3-FBYX].

270 *Ibid* at 62.

The Law Society of British Columbia Cloud Computing Report discusses lawyer-specific issues from a law society compliance perspective.[271] It warns that a data breach of cloud storage can compromise large amounts of confidential client information, therefore, lawyers need to take reasonable steps to secure data.[272] Ensuring due diligence in establishing proper safeguards when contracting for cloud services is essential.[273] Since law societies regulate lawyers, and not third party technology providers, they do not have the statutory authority to compel cloud service providers to give access to lawyers' business records absent a court order.[274] Therefore, when choosing a cloud service provider, attention to security is a paramount issue.[275]

In order to comply with Law Society recordkeeping obligations, lawyers should pay special attention to the terms of the contract surrounding custody and control of data. Namely, what the third party is able to do with data stored on their servers, what their responsibilities are regarding the data, and how the data is integrated into other record keeping systems.[276] A lawyer can use a third-party cloud provider for the storage or processing of records if the lawyer retains custody of the data.[277] Moreover, as lawyers need to comply with record retention obligations, assurances from the cloud service providers must be made regarding the production of data in a comprehensible form at the request of the lawyer or the law society.[278]

It may be advantageous for a firm to use Canadian cloud services due to familiarity with the legal regime and less likelihood of having objections or complaints that the data is subject to the overriding laws of another sovereign nation.

---

271 Gavin Hume et al, "Report of the Cloud Computing Working Group" (15 July 2011), online (pdf): The Law Society of British Columbia <https://www.lawsociety.bc.ca/Website/media/Shared/docs/publications/reports/CloudComputing.pdf> [perma.cc/Z858-2292].

272 *Ibid* at 14.

273 *Ibid* at 7.

274 *Ibid* at 10.

275 *Ibid* at 13.

276 *Ibid* at 14.

277 *Ibid* at 15.

278 *Ibid* at 16.

G. Printers, Scanners, and other Network Devices

Auxiliary devices that use wireless Internet may represent a point of vulnerability and are often overlooked.[279] They operate like small computers with their own data storage, operating system and direct wireless network connection.[280] For example, a confidential client document scanned and sent to another department in the law firm is stored in the machine and can be hacked more easily than a computer directly. Some basic steps to protect your auxiliary devices involve:[281]

- Control access to printer and scanner and their functions at the group, individual, and activity level.
- Ensure data is secure at every stage of a workflow involving an auxiliary device – from the data path along the network to the device itself. This may involve hiring security specialists and training staff.
- Use all available tools to protect sensitive documents from loss or theft.
- Always include printers and scanners in standard network security measures and policies.
- Keep software updated on auxiliary device.
- Consider choosing a device with integrated security software that only lets authorized files run and alerts users of possible security threats.[282]
- If renting equipment from a supplier (e.g. Ricoh), be aware of what the contract says regarding data breaches originating on the equipment. Are the breaches indemnified? Who is responsible for ensuring updated security?
- Consider having printers and scanners disconnected from the Internet.

---

279 Eric Savitz, "The Hidden IT Security Threat: Multifunction Printers" (13 February 2013), online: *Forbes* <http://www.forbes.com/sites/ciocentral/2013/02/07/the-hidden-it-security-threat-multifunction-printers/> [perma.cc/S8AW-L7L9].

280 Eric Geier, "Your Printer Could Be a Security Sore Spot" (25 April 2012), online: *PC World* <http://www.pcworld.com/article/254518/your_printer_could_be_a_security_sore_spot.html> [perma.cc/3UAA-E9SF].

281 Savitz, *supra* note 279.

282 *Ibid.*

H. Thumb Drives and Hard Drives

Although convenient due to their small size and portability, external storage devices are more likely to be lost or stolen than laptops and computers.[283] Thus, encryption of USB drives and external hard drives is an important security measure to implement to prevent data theft.[284]

Malware can be transmitted to computers via data storage devices; hence it is good practice to only allow approved devices to be connected to a firm's network.[285]

Old hard drives are a potential security risk, despite the fact that they may have been wiped. The FBI Computer Forensics Evidence Unit has shown that it is possible to recover deleted files from a hard drive that has supposedly been wiped clean.[286] For the same reason, broken hardware should be disposed of properly to ensure that data cannot be retrieved from the devices. One potential remedy is to physically destroy data storage devices.[287] However, before any destruction of data remember that the Law Societies have mandated certain record retention requirements.

I. Email Policies

Email policies establish guidelines and minimum requirements regarding the acceptable use of the law firm's email. Like physical devices, email can be managed in a number of different ways. E-mails can be managed on site using a dedicated server or through a third-party management system. Firms should be aware of the indemnification provisions regarding third party email service providers. E-mails contain sensitive information should

---

283 Ondrej Krehel, "12 Security Best Practices for USB Drives" (6 February 2012), online (blog): *Cyber Scout* <http://cyberscout.com/education/blog/12-security-best-practices-for-usb-drives> [perma.cc/RR9D-HVER].

284 *Ibid* at 16 & 18.

285 Bruce Brown, "Malware Alert – Don't Put in that USB Stick You Found on the Street" (5 August 2016), online: *Digital Trends* <https://www.digitaltrends.com/computing/usb-sticks-carry-malware/> [perma.cc/X8L3-VKPK].

286 Michael Noblett, Mark Pollitt and Lawrence Presley, "Recovering and Examining Computer Forensic Evidence" (October 2000), online: *FBI* <https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm> [perma.cc/2AZS-CS42].

287 Ian Sutherland & Gareth Davies, "Hard Disk Storage: Data Leakage" in Joseph Demergis, ed, *Proceedings of the 9th Conference on Information Warfare and Security* (Thessaloniki: University of Macedonia, 2010) at 287.

be encrypted. The Law Society of British Columbia has a sample email and Internet use policy that may be of assistance.[288]

It is important to share a firms e-mail policies with clients. Include an overview of your email policy and obligations in retainer letters.[289] Another best practice to include in an email policy is to add an option to opt out of communication via email at the end of the email signature. For example: *"If you do not wish to receive future email correspondence from the sender please use the reply function above to respond, indicating this preference."*

Email Policies: Phishing Scams

Many cyber-attacks are attempted through phishing schemes, which are methods used to gain information on a fraudulent basis. Many phishing schemes are employed through electronic spam. Spam is an unsolicited electronic message used to make money and can be delivered using a variety of media, including emails and instant messages. Fraudulent e-mails designed to obtain sensitive information cost American businesses over $500 million a year.[290]

Spam can generally be categorized into unsolicited advertisements or cyber-attacks. Spam advertisements may be offering legitimate services but often sell knock-off products.[291] Spam may also be designed as a cyber-attack

---

288 David Bilinsky, "Sample Internet and Email Use Policy" (January 2002), online (pdf): *Law Society of British Columbia* <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/InternetPolicy.pdf>.

289 "Pomer & Boccia Email Policy," online: *Pomer & Boccia* <http://www.pomerandboccia.com/legal/email_policy.htm> [perma.cc/7LKX-UCG2]; David Amyot, "Service Terms and Policies," online: McTague Law Firm LLP <https://www.mctaguelaw.com/service-terms-and-policies/>; "Information Security Policy Templates," online: *SANS* <https://www.sans.org/security-resources/policies/general#email-policy> [perma.cc/QBH8-PSKU].

290 Lee Mathews, "Phishing Scams Cost American Businesses Half A Billion Dollars A Year" (5 May 2017), online: *Forbes* <https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#39d74d4f3fa1> [perma.cc/5LGJ-BVE2].

291 "Types of spam," online: *AO Kaspersky Lab* <https://encyclopedia.kaspersky.com/knowledge/types-of-spam/> [perma.cc/C9MF-HUKX].

of which many techniques exist.[292] Phishing scams are designed to fraudulently induce the consumers into divulging information relating to a legitimate service. For example, spammers may attempt to obtain passwords from their victims by falsely claiming that the security of their victims account has been compromised, requiring them to divulge personal information to the spammers.[293] Another spam cyber-attack is the advance fee scam. These scams usually promise a consumer something too good to be true for a small fee in advance. For example, spammers may post advertisements offering a space for rent at an outstanding rate in exchange for a deposit.[294] The deposit is then simply stolen.

As was recently demonstrated, phishing schemes can be arranged with such detail as to trick lawyers into thinking they are the client.[295] In this respect, it may be wise to implement a policy requiring that all wire transfers (over a certain threshold) and change in bank information be confirmed verbally or in-person by the client.[296]

The U.S. has a federal anti-spam legislation called the *CAN-SPAM Act* enacted in 2003 with criminal penalties that have put some violators in jail.[297] In 2014 *Canada's Anti-Spam Legislation* (CASL, formerly bill C-28) came

---

292 Roger A. Grimes, "The 5 types of cyber attack you're most likely to face" (21 August 2017), online: *SCO Online* <https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html> [perma.cc/2QDJ-LVQA].

293 Robert Hackett, "Beware of These Top 10 Phishing Emails. Would You Fall for Them?" (13 July 2017), online: *Fortune* <http://fortune.com/2017/07/13/email-security-phishing/> [perma.cc/5VYD-QWF5].

294 Lew Sichelman, "Rental scams can target either landlords or tenants" (25 March 2012), online: *Los Angeles Times* <http://articles.latimes.com/2012/mar/25/business/la-fi-lew-20120325> [perma.cc/K7S9-AJE4]; "Craigslist Scams" online: *Fraud Guide* <https://web.archive.org/web/20120705075209/http://www.fraudguides.com/internet-craigslist-scams.asp> [perma.cc/S5N2-H6KT].

295 McKiernan, *supra* note 72; *Dentons*, *supra* note 246.

296 Pray, *supra* note 254.

297 Tracy McVeigh, "Porn spammers jailed for five years" (14 October 2007), online: *The Guardian* <https://www.theguardian.com/technology/2007/oct/14/internet.crime> [perma.cc/3NL9-C7ZZ]; "15 U.S. Code Chapter 103 - Controlling the Assault of Non-Solicited Pornography and Marketing," online: *Cornell Law School* <https://www.law.cornell.edu/uscode/text/15/chapter-103> [perma.cc/3VWM-3G46].

into force.[298] CASL regulates commercial electronic advertising and provide a more secure Internet by penalizing cyber-attackers.[299] *CASL* has been used to grant a warrant to take down a Toronto based server that was the source of malware threatening computer security.[300] Critics claim that *CASL* may be too harsh on business marketers who, under the act, require strict consent to deliver electronic advertisements to consumers.[301] Nevertheless, *CASL* is a logical step forward to mitigate losses due to cyberthreats in an ever growing technological era.

Most Internet service providers have an acceptable use policy that contractually prohibits a user from engaging in the distribution of a large array of spam.[302] Despite the contractual obligations of Internet users and statutes that impose penalties, spam and phishing scams continue to be a major problem. Cybercriminals have a plethora of methods to assist in keeping their identity anonymous on the Internet, which enables easier distribution of spam.[303] Moreover, in 2011, computer science researchers discovered that a small number of foreign banks facilitate payment to

---

298 *An Act to promote the efficiency and adaptability of the Canadian economy*, *supra* note 191.

299 "Bill C-28: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities," online (pdf): *Parliament of Canada* <https://www.parl.ca/DocumentViewer/en/40-3/bill/C-28/royal-assent> [perma.cc/GHW6-T7WG].

300 "CRTC serves its first-ever warrant under CASL in botnet takedown" (3 December 2015), online: *Government of Canada* <https://www.canada.ca/en/radio-television-telecommunications/news/2015/12/crtc-serves-its-first-ever-warrant-under-casl-in-botnet-takedown.html> [perma.cc/YEK5-QYR3].

301 "Canada's Anti-Spam Legislation (CASL)" (30 July 2018), online: *Canadian Chamber of Commerce* <http://www.chamber.ca/resources/casl/> [perma.cc/EM4L-S5KA].

302 "Acceptable Usage Policy (AUP) – Internet Services" (30 July 2018), online: *Frontier Networks* <http://www.frontiernetworks.ca/aup/> [perma.cc/JH4S-U8PX].

303 Roger A. Grimes & Preston Gralla, "17 steps to being completely anonymous online" (1 January 2018), online: *SCO* <https://www.csoonline.com/article/2975193/data-protection/9-steps-completely-anonymous-online.html> [perma.cc/N69L-77X3].

spammers.[304] Notably, the researchers claim that these small number of foreign banks may be an effective target to intervene spam schemes.[305]

Rather than making criminal sanctions even stronger, it may be more feasible to target bottlenecks such as the handful of foreign banks that cybercriminals rely upon to receive payment for their scams. However, given the availability of decentralized currency such as Bitcoin and others, this might be a futile attempt.

As noted above, phishing schemes succeed because of human error in combination with technical limitations in detecting such scams. Indeed, many phishing schemes target human vulnerabilities such as the need to act due to urgency, fear or anxiety.[306] Psychology researchers have shown that e-mail recipients are more likely to respond to phishing attempts when scammers invoke emotions relating to failure or express shared interest.[307] We recommend that business owners rigorously train their staff to identify, avoid and report phishing scams. This in combination with a reliable spam filter will lessen the risk that a business suffers from a phishing scam. Understandably, in this age of sophisticated socially engineered scams, training staff to avoid attacks may be a difficult task. Thus, an emerging quality that firms may desire in new hires is basic proficiency technology including the ability to recognize, avoid and report complex phishing scams.

Ultimately, spam and cybercrime are complex issues and will likely require future legal practitioners and other experts to develop novel strategies to combat this multi-billion-dollar issue.

J. Internet Use - Personal Browsing

It is perhaps unavoidable in the modern workplace that people will use the Internet at work for personal use (e.g. checking personal email, perhaps online shopping). The key is to set realistic limits on personal

---

304 Kirill Levchenko et al, "Click Trajectories: End-to-End Analysis of the Spam Value Chain," online (pdf): *UCSD* <https://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf> [perma.cc/QPT3-A2AV].

305 Rik Farrow, "Interview with Stefan Savage on the Spam Payment Trail" (August 2011), online (pdf): *UCSD* <http://cseweb.ucsd.edu/~savage/papers/LoginInterview11.pdf> [perma.cc/CC2F-NBC5].

306 Asselstine, *supra* note 207.

307 Prashanth Rajivan & Cleotilde Gonzalez, "Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks" (2018) 9 Front Psychol Article 135.

Internet use at work. Generally speaking, as with everything else, you need a policy in place which lays out the expectations for partners and staff.[308]

K. Social Media Policies

Social media sites enable wide exposure of content, and therefore, may pose issues to corporation hoping to keep information private. Something could be said by an employee or partner about the firm on social media, which can have damaging consequences for the reputation and image of the firm, as well as the confidentiality of clients' information. A strong social media policy can help mitigate these risks.

The Law Society of British Columbia developed a model policy for social media and social networking to help guide lawyers in their online behaviour.[309] Social media blurs the lines between personal and professional lives. The model policy reminds lawyers that they are responsible for their online activity when using the firm's email address and when publishing content from the firm's equipment.[310] The model policy sets clear guidelines regarding online identity, creating and managing content, leaving comments, and confidentiality and privacy of clients' information.[311] Similarly, the Law Society of Ontario drafted an online activity and social media policy. It applies to online behaviours of lawyers, paralegals, staff and third-party contractors.[312]

Some law firms have developed their own online and social media policy. For example, Jaffe's social media policy attempts to compel lawyers

---

308 "Counsel to the Internet Client: Practical Advice, Strategy and Litigation" (Faculty of Law, Harvard University) online: <https://cyber.harvard.edu/seminar/internet-client/> [perma.cc/J9H4-WZC7], see weekly readings: Week 7 (10/22) "Model Law Firm Policy Regarding the Use of the Internet."

309 "Model Policy. Social Media and Social Networking," online: *Law Society of British Columbia* <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/policy_social-media.pdf> [perma.cc/UQH5-K9D4].

310 *Ibid* at 1-2.

311 *Ibid*.

312 "Sample Online Activity and Social Media Policy" (September 2010), online (pdf): *Law Society of Ontario* <https://lawsocietyontario.azureedge.net/media/lso/media/legacy/pdf/o/online-activity-social-media-policy.pdf> [perma.cc/TJN5-WFP4].

and law firms to use social media effectively and responsibly.[313] The American Bar Association has also created guidelines for law firms when drafting a social media policy for their lawyers and staff.[314]

L. Electronic Records Management

As noted above, in order to mitigate cybersecurity risks and improve the legal compliance (including admissibility) of electronic records, document management and document retention policies should be comprehensive and comply with industry standards. Indeed section 51.6 of *The Manitoba Evidence Act* (and similar legislation) expressly allows a party entering electronic evidence to cite the "standard" it relied upon.

A variety of national and international organizations have issued "best practices" recommending the imaging of paper-and-ink documents. One of these organizations is the International Standards Organization. "Information and Documentation – Records Management – General", and ISO/TR 15489-2, "Information and Documentation – Records Management – Guidelines" are relevant. The CRA[315] and Canada Standards Council[316] have also published invaluable guides on keeping electronic records. Note that there may be specific standards that certain industry expects to be followed.

---

313 "Social Media Policy Template" (August 2016), online: *Jaffe* <http://www.jaffepr.com/policy-templates/social-media-policy-template> [perma.cc/T9NT-VNB7].

314 "How to Create a Law Firm Social Media Policy" (January/February 2012), online: *American Bar Association* <https://www.americanbar.org/publications/law_practice_magazine/2012/january_february/how-to-create-a-law-firm-social-media-policy.html> [perma.cc/SD2Z-HK84].

315 Canada Revenue Agency, Information Circular IC05-1R10, "Electronic Record Keeping" (June 2010) online: < https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/ic05-1/electronic-record-keeping.html> [perma.cc/D4PC-4EAA] and the complementary document Canada Revenue Agency, Information Circular IC78-10R5, "Books and Records Retention/Destruction" (June 2010) online: < https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/ic78-10/books-records-retention-destruction.html> [perma.cc/2MAU-XAMC].

316 Electronic Records as Documentary Evidence (2017), *supra* note 229.

M. Conclusion

The recommendations presented here along with the general concepts of risk managements are meant to guide the reader in formulating their own firm specific cybersecurity management protocol. One must balance convenience with security when choosing the right strategies while always keeping professional obligations in mind. Although this task presents paradoxes at times, it is best to plan ahead in order to avoid irrational strategies formulated mid-crisis. Some lucky ones will never suffer the damages caused by a cyberbreach. However, considering the increasing likelihood of a cyberattack, a very good cybersecurity management plan is necessary and will enable incremental, calculated failure with a reasonable recovery time, whereas lack of such a plan may be bound for catastrophic failure. Although this may be an intimidating thought, readers should feel encouraged that technology and resources are available to assist in the creation of a custom cybersecurity management plan that is right for you.

APPENDIX I: Privacy Legislation Summaries

In this appendix, readers will find a brief summary of various federal, provincial and territorial privacy statutes. It functions as a companion to chapter II, in that it includes a discussion of all of the various privacy statutes discussed in text. These summaries are not comprehensive, but rather seek to provide the reader with a very general understanding of the scope of these Acts and direct the reader to key provisions, which may be applicable to the cybersecurity of legal practices.

I. TABLE 1: FEDERAL ACTS

Act	Commentary
An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying Out Commercial Activities, and to Amend the Canadian Radio-Television and	This Act has relevance for our purposes as it overrules certain features of PIPEDA, which were discussed in the section concerning privacy legislation and provides a private cause of action with regards to certain actions prohibited by PIPEDA.[317] The Act seeks to regulate the use of electronic messages in commercial settings[318] and is perhaps most remarkable for its strict regulation of, and strong penalties relating to, unsolicited electronic marketing (i.e. spam). Section 47 of the Act creates a private right of action for a person who has been affected by a corporation's breach of the anti-spam provisions found in sections 6-9. Section 47 also allows an action to be

317 *An Act to promote the efficiency and adaptability of the Canadian economy supra* note 191 s 2 states: "In the event of a conflict between a provision of this Act and a provision of Part 1 of [PIPEDA], the provision of this Act operates despite the provision of that Part, to the extent of the conflict."

318 *Ibid* at s 3.

Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act	commenced when section 5 of PIPEDA is breached as described in sections 7.1(2) or (3) of PIPEDA. Recall that section 5 of PIPEDA specifies that the obligations set out in the Model Code, Schedule 1, are to be complied with, and also contains the "reasonableness" provisions. Sections 7.1(2) and (3) of PIPEDA, which were not previously discussed in this work, establish certain exceptions to the Act's consent requirements as laid out in section 7 of the Act. Section 7.1(2) specifies that these exceptions do not apply when an electronic address,319 including an email address, is collected by a computer program specifically designed or marketed primarily for the use of generating or searching and collecting such addresses. In short, the act does not provide the protections afforded by section 7.1 when organizations use computer software primarily designed to collect electronic addresses. Section 7.1(3) of the act specifies that the exceptions to the consent requirements do not apply when personal information is collected when a computer system is accessed in contravention of an Act of Parliament.320 Returning to the private action found in this Act, this work will not fully discuss the rules of procedure as laid out in sections 48-50. However, a brief discussion of the potential remedies available to litigants is provided. Under section 51 of the Act, if "the court is satisfied" that one or more persons have contravened the Act, then the court has statutory authority to not only provide compensatory damages for losses, damages or expenses suffered by the applicant, but also impose additional fines, the maximum of which are not to exceed $1,000,000 for each day the contravention occurred.321
Privacy Act	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, the federal Privacy Act will

319 PIPEDA *supra* note 133 at s 7.1(1) defines an electronic address as "an address used in connection with (a) an electronic mail account; (b) an instant messaging account; or (c) any similar account."

320 *Ibid* at s 7.1(3).

321 An Act to promote the efficiency and adaptability of the Canadian *supra* note 191, s 51(1)(b)(vi).

	only be touched on briefly as its scope is limited relative to PIPEDA.[322] The Privacy Act applies only to the personal information[323] held by "government institutions," a complete list of which is found in schedule 1 of that Act. The Privacy Act, which is also the originating legislation of the Privacy Commissioner's Office, imposes obligations on the collection,[324] use,[325] storage,[326] disclosure[327] and disposal[328] of personal information by the Crown or its agents. Lawyers working for and with the federal Crown should be aware of these more specialized obligations, including the right to access this information.[329]

II. TABLE 2: PROVINCIAL AND TERRITORIAL LEGISLATION: ALBERTA

Title	Commentary
Personal Information Protection Act[330]	This Act has been deemed "substantially similar" to *PIPEDA* and as such, pursuant to *PIPEDA* Regulations, organizations subject to this Act, "other than a federal work, undertaking or business,"[331] are exempt from the provisions found in Part 1 of *PIPEDA*. As with *PIPEDA*, the stated purpose of this Act is to govern the collection, use and disclosure of

322 Importantly, Privacy Act, *supra* note 190, s 53 allows governor in council to appoint a Privacy Commissioner.

323 Note, the definition of personal information is more detailed in the Privacy Act than in PIPEDA.

324 Privacy Act, *supra* note 190 s 4 & 5.

325 *Ibid* s 7.

326 *Ibid* ss 10 & 11 through personal information banks as well personal information index.

327 *Ibid* s 8.

328 *Ibid* s 6(3).

329 *Ibid*, ss 13-18.

330 *Personal Information Protection Act*, SA 2003, c P-6.5.

331 SOR/2004-219, s 1.

	personal information by organizations, seeking to balance the privacy interests of individuals and the reasonable needs of organizations.[332] Unsurprisingly, the definition of "personal information" is the same in this Act as it is in *PIPEDA*, being "information about an identifiable individual."[333] Also like *PIPEDA*, the Act imposes obligations upon organizations with regards to the personal information they control,[334] including consent requirements,[335] and limitations on the collection,[336] usage[337] and disclosure[338] of personal information. The Act also requires that organizations act in a reasonable manner in complying with the Act[339] and that the collection, use and disclosure of personal information must also be reasonable. The Act also imposes obligations upon the holders of personal information to protect said

332 *Personal Information Protection Act*, *supra* note 330 s 3: Purpose of AB Act is "to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable."

333 *Ibid*, s 1(1)(K) - although it lacks the French term used in PIPEDA.

334 *Ibid*, s 5(1): "An organization is responsible for personal information that is in its custody or under its control."

335 *Ibid* s 7(1): "Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,

(a) collect that information unless the individual consents to the collection of that information,

(b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,

(c) use that information unless the individual consents to the use of that information, or

(d) disclose that information unless the individual consents to the disclosure of that information."

336 *Ibid*, s 11(1) states that an "organization may collect personal information only for purposes that are reasonable," which differs from PIPEDA at s 4 of Schedule 1.

337 *Ibid*, s 16(1) – again reasonableness.

338 *Ibid*, s 19(1) – again reasonableness.

339 *Ibid*, s 5(5)

	information "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction,"[340] and to report any loss or unauthorized access of this information to the privacy commissioner where there exists a "real risk of significant harm."[341] The privacy commissioner may then require the organization to inform the affected individuals.[342] Despite the Act's similarities to *PIPEDA*, there are two differences which need to be briefly mentioned. First, the Act applies to employment relationships within Alberta, and as such, there are specific provisions which deal with the collection, usage and disclosure of personal information by trade unions and employers.[343] As such, the Act also provides protection for employees who comply with this legislation in good faith[344] and/or report any potential contraventions of the Act to the privacy commissioner.[345] Under the Act's remedial scheme, certain breaches of the Act's provisions are offenses under the act[346] and can result in fines of up to $10,000 for an individual and $100,000 for and organization.[347] As with the federal Act, claims for damages can also be brought against an organization that breached its obligations under the Act.[348] However, the Act provides legal protection for an organization against

340 *Ibid*, s 34

341 *Ibid*, s 34.1.

342 *Ibid*, s 37.1; Note that reporting is not mandatory.

343 *Ibid*, ss 14.1 & 15 (collection); *Ibid* at ss 17.1 & 18 (usage); *Ibid* at ss 20.1 & 21 (disclosure).

344 *Ibid*, ss 58(b) & (c).

345 *Ibid*, s 58(a).

346 *Ibid*, s 59(1).

347 *Ibid*, ss 59(2) (a) & (b).

348 *Ibid*, s 60(1).

	any claim of damages resulting from "the disclosure of or failure to disclose, in good faith, all or part of a record or personal information under this Act, or any consequences of that disclosure or failure to disclose."[349]
Freedom of Information and Protection of Privacy Act[350]	Belonging to a class of legislation found across all jurisdictions that governs the use of information held by the government, Alberta's *Freedom of Information and Protection of Privacy Act* governs "records" held by public bodies in the province.[351] The Act provides a statutory mechanism for requesting information held by the government and legislates when disclosure of information during a freedom of information request by a public body is not permissible.[352] Additionally, the Act imposes obligations related to the collection,[353] protection,[354] use,[355] and disclosure[356] of "personal information" as defined in the Act. Lawyers working on behalf of, or with, the Crown in Alberta should be aware of these requirements.
Health Information Act[357]	The *Health Information Act*, which has similar counterparts in most common-law provinces, governs the use of "health information" by healthcare providers. "Health information" is defined in the Act as "diagnostic, treatment and care information"[358] or "registration information."[359] The Act aims to protect

349 *Ibid*, s 57(a). See also *Ibid* at s 57(b).

350 *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25.

351 See *Ibid*, ss 4(1)(a)-(u) for a long list of exceptions.

352 *Ibid*, s 16(1) (business interests); *Ibid* at s 17(1) (personal privacy); *Ibid* at s 18 (public safety); *Ibid* at s 19 (employee/hiring evaluations); There are many more exceptions to disclosure.

353 *Ibid*, ss 33-35, 37.

354 *Ibid*, s 38.

355 *Ibid*, s 39.

356 *Ibid*, s 40.

357 *Health Information Act*, RSA 2000, c H-5.

358 *Ibid*, s 1(1)(k)(i).

359 *Ibid*, s 1(1)(k)(ii); See also Alta Reg 70/2001, s 3 which details what registration

	the privacy of individuals' health information[360] by providing rules relating to the collection, use and disclosure of health information[361] by healthcare providers while ensuring that this information can also be shared so as to provide health services and manage the health system.[362] The Act also provides a remedial structure for enforcing the obligations in this Act.[363] The Act imposes a duty upon healthcare providers, referred to as Custodians in the Act, to "take reasonable steps" to protect the confidentiality of health information and the privacy of individuals, including health information stored or used in a jurisdiction outside of Alberta.[364] Legal practitioners whose work intersects with the provision of health services should be aware of the duties and obligations imposed by this Act.

III. TABLE 3: PROVINCIAL AND TERRITORIAL LEGISLATION: BRITISH COLUMBIA

Personal Information Protection Act[365]	This Act has been deemed to be "substantially similar" to *PIPEDA* and as such, pursuant to *PIPEDA* Regulations, organizations subject to this Act, "other than a federal work, undertaking or business"[366], are exempt from the provisions found in Part 1 of *PIPEDA*. There is considerable overlap between *PIPEDA* and this Act. As with *PIPEDA*, the stated

information is.

360 *Health Information Act*, *supra* note 357, s 2(a)

361 *Ibid*, s 2(c); Collection is governed by ss 18-24; Use is governed by ss 25-30; Disclosure is governed by ss 31-56, including Division 3 – research purposes; See also *Ibid* at s 57.

362 *Ibid*, s 2(b).

363 *Ibid*, s 2(f); The Act's remedial structure is centred around a Commissioner, whose powers are detailed in Part 7 of the Act.

364 *Ibid*, s 60(1).

365 *Personal Information Protection Act*, SBC 2003, c 63.

366 SOR/2004-220, s 1.

	purpose of this Act is to govern the collection, use and disclosure of personal information by organizations, seeking to balance the privacy interests of individuals and the reasonable needs of organizations.[367] Consequently, the Act imposes a general duty upon organizations to act reasonably in their compliance with the Act.[368] The definition of "personal information" is nearly the same in this Act as it is in *PIPEDA*, being "information about an identifiable individual."[369] However, the BC Act's definition of "personal information" specifically includes "employee personal information."[370] Like *PIPEDA*, the Act imposes obligations upon organizations with regards to the personal information they control,[371] including consent

367 Personal Information Protection Act, *supra* note 365, s 2 states: "The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

368 *Ibid*, s 4(1) states: "In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances."

369 *Ibid*, s 1.

370 *Ibid*: "'employee personal information' means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment;"

371 *Ibid*, s 4(2): "An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization."

	requirements,[372] and limitations on the collection,[373] usage[374] and disclosure[375] of personal information.

372 *Ibid*, s 6(1) states that an organization shall not (a) collect, (b) use or (c) disclose personal information except for where (2)(a) consent of the individual is given or (b) the Act authorizes collection without consent, or (c) the Act deems that consent has been given. Additionally, ss 7-9 govern specific issues surrounding consent, such as requirements before consent can be given, implied consent and the withdrawal of consent.

373 *Ibid*, ss 10-13; s 10(1) details the information which organizations must disclose to individuals before they can collect their information, including the purpose of the collection. Failure to provide this information would appear to nullify any consent given by the individual per s 7(1)(a). s 10(2) deals with inter-organizational transfers of personal information without the consent of the individual, imposing an obligation upon the organization requesting the transfer to demonstrate that the collection is in compliance with the act. s 11 imposes a general duty of reasonableness upon the collection of personal information (that in which "a reasonable person would consider appropriate in the circumstances") and requires the information to only be collected in furtherance of the objective disclosed under s 10. s 12 details the instances where consent is not required to collect personal information. There are several provisions under s 12 which are of interest, including (a) where the collection is in the interest of the individual but consent cannot be obtained "in a timely way"; (b) the collection is necessary for medical treatment of the individual and the individual is unable to consent; (h) the collection is required or authorized by law; and (k) the information was collected for the purposes of providing legal services to a third party, and the information is necessary to provide those services. s 13 outlines specific instances where employers may be exempt from the consent requirement upon collection of information.

374 *Ibid*, ss 14-16; s 14, structurally similar to s 11, imposes a general duty to use the personal information "only for purposes that a reasonable person would consider appropriate in the circumstances" and meets other requirements set out in the act. s 15 details the instances wherein personal information can be used without consent. Although there is some overlap with the exceptions provided for collection under s 12, there are differences (e.g. as mentioned in the note above, s 12(b) allows for personal information to be collected when the collection is necessary for medical treatment an individual is unable to consent, while s 15(a) allows of the use of personal information when it is necessary for medical treatment and the individual does not have the legal capacity to give consent. Additionally, and perhaps most importantly, there is no equivalent of s 12(k), discussed above which allows for the collection of information for the purpose of providing legal services per s 15).

375 *Ibid*, ss 17-22; s 17, structurally similar to ss 11 and 14, imposes a general duty to disclosure personal information "only for purposes that a reasonable person would consider are appropriate in the circumstances" and meets other requirements set out in the act. Similarly to ss 12 & 15, s 18 provides a list of exceptions whereby an organization can disclose personal information without consent (s 18(1)(a) is similar to ss 15(a) & 12(a) as discussed above). For our purposes, s 18 provides exceptions for information compelled by warrants, court orders or subpoenas (s 18(1)(i)), disclosure to law

	The *Act* also imposes obligations upon the holders of personal information to protect personal information in their custody "by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks"[376]. This Act, however, does not appear to have the affirmative reporting duties as present in its Alberta counterpart or soon to be found in *PIPEDA*, but rather the Act appears to mirror the current schema found in PIPEDA. The Act is enforced by a Commissioner[377] who has the authority to conduct investigations and audits regarding compliance with the Act,[378] as well as initiate reviews following complaints regarding non-compliance with the Act.[379] The Act also creates a number of offences related to non-compliance with its core provisions,[380] which can result in fines of up to $10,000 for an

enforcement agencies concerning an offence to assist in an investigation (s 18(1)(j)). The Act also allows for disclosure of personal information without consent of the individual wherein "the disclosure is to a lawyer who is representing the organization" (s 18(1)(m)). s 19 details the obligations concerning disclosing employee personal information. s 20 concerns the transfer of personal information as a result of the sale of an organization or its assets. Finally, ss 21 & 22 deal with disclosure of personal information for research and archival purposes.

376 *Ibid*, s 34.

377 *Ibid*, s 1, "commissioner" means the commissioner appointed under s 37(1) or 39(1) of the Freedom of Information and Protection of Privacy Act.

378 *Ibid*, s 36 details the general powers of the commissioner. S 36(1) states: "(a) whether a complaint is received or not, initiate investigations and audits to ensure compliance with any provision of this Act, if the commissioner is satisfied there are reasonable grounds to believe that an organization is not complying with this Act;" s 38 provides the commissioner with powers to conduct investigations, audits and inquiries, similar to those powers found in PIPEDA.

379 *Ibid, s* 36(2) governs how the commissioner may investigate complaints made regarding non-compliance with the Act. S 46 of the Act allows the Commissioner to initiate a review after receiving a complaint. Under s 46 a complaint must have asked for access to information, or a correction to said information and may ask the commissioner to review the organizations failure to comply with specific provisions of the Act regarding this.

380 *Ibid, s* 56(1).

	individual and $100,000 for an organization.[381] As with the federal Act, claims for damages can also be brought against an organization that breached its obligations under the Act.[382] Finally, as mentioned above, this Act specifically concerns employee personal information, and as such, there are two specific whistleblower protection provisions in the Act which provide protection against retaliation for working within the scheme of the Act to report non-compliance.[383]
Freedom of Information and Protection of Privacy Act[384]	Belonging to a class of legislation found across all jurisdictions that governs the use of information held by the government, British Columbia's *Freedom of Information and Protection of Privacy Act* governs "records" held by public bodies in the province.[385] The Act provides a statutory mechanism for requesting information held by the government,[386] and provides a series of exceptions whereby a head of a public body may refuse to disclose information,[387] and instances where the head of the public body is obligated not to

381 *Ibid*, s 56(2).

382 *Ibid*, s 57. However, there exists a limitation that such actions under ss 57(1) & (2) only allow for a claim against organizations for "damages for actual harm" that was suffered as a result of the conduct. There is no definition of "actual harm" in the act.

383 *Ibid*, s 54 (employee provisions); *Ibid*, s 55 (general non-retaliation).

384 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.

385 *Ibid*, s 1, record means, "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records." The Act includes a list of exceptions to which it does not apply, found at ss 3(1)(a)-(k).

386 *Ibid*, s 4 provides a person with a right to request information from a public body including personal information, and s 6 imposes a duty upon the head of public bodies to assist applicants in their requests for information. s 5 details the mechanism by which this is to occur. s 7 provides the legislated timeline for responses, while s 8 concerns what must come in a response.

387 *Ibid*, ss 13-20 (Division 2); E.g. s 13 concerns policy advice/recommendations, s 14 concerns information subject to solicitor-client privilege, s 15 harmful to law enforcement.

	disclose information.[388] Additionally, the Act imposes obligations related to the collection,[389] protection,[390] use,[391] and disclosure[392] of "personal information" as defined in schedule 1 of the Act. Lawyers working on behalf of, or with, the Crown in British Columbia should be aware of these requirements.
E-Health (Personal Health Information Access and Protection of Privacy) Act[393]	The *E-Health (Personal Health Information Access and Protection of Privacy) Act*, which has similar counterparts in most common-law provinces, governs databases, called health information banks, maintained by provincial healthcare bodies, which contain "personal health information." "Personal health information" is defined in the Act as "recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual."[394] The Act creates a government mechanism (a designation order by the minister) which allows the minister to designate the purposes for which personal health information can be collected into health information banks[395] and how that information can be used[396] or disclosed,[397] while proscribing any non-designated use of the health banks and their information.[398] Legal practitioners

388 *Ibid*, s 12 (cabinet or local public body confidences); *Ibid*, s 21 (harmful to business interests of a third party); *Ibid*, s 22 (harmful to personal privacy); *Ibid*, s 22.1 (relating to abortion services).

389 *Ibid*, ss 26-27.

390 *Ibid*, ss 30 & 30.1.

391 *Ibid*, s 32.

392 *Ibid*, ss 33-36.

393 *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c 38.

394 *Ibid*, s 1.

395 *Ibid*, ss 3 & 4.

396 *Ibid*, s 4 (use).

397 *Ibid*, s 5.

398 *Ibid*, s 21 states: "(1) Personal health information must not be collected into a health information bank or used in a health information bank for any purpose or in any manner other than in accordance with the designation order in respect of the health information

	who practice in this field need to be aware of the obligations imposed by this statute.
Privacy Act[399]	This Act makes it an actionable tort for "a person, wilfully and without a claim of right, to violate the privacy of another."[400] While this Act may not have direct relevance to the cybersecurity interests of law practices, the haphazard use of technology could potentially violate the privacy of another, exposing oneself to litigation.

IV. TABLE 4: PROVINCIAL AND TERRITORIAL LEGISLATION: MANITOBA

The Freedom of Information and Protection of Privacy Act[401]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Manitoba's *Freedom of Information and Protection of Privacy Act* governs "records" held by public bodies in the province.[402] The Act provides a statutory mechanism for requesting information held by government bodies,[403] and provides a series of

bank. (2) Personal health information contained in a health information bank must not be disclosed for any purpose or in any manner other than (a) in accordance with the designation order in respect of the health information bank, or (b) as permitted under this Act."

399 *Privacy Act*, RSBC 1996, c 373.

400 *Ibid*, s 1(1) [emphasis added]. It should be noted that this Act requires the violation of privacy to be "wilful."

401 The Freedom of Information and Protection of Privacy Act, SM 1997, c 50, CCSM c F175.

402 *Ibid*, s 1(1), record is defined as "a record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records." A list of the records exempted from this act's scope can be found in s 4.

403 *Ibid*, Part 2 and specifically ss 7-16 amount to a statutory mechanism whereby persons can request records from the government. These sections prescribe a means by which a person can request records, imposes an obligation upon the head of a public body to "make every reasonable effort" to assist such an application (s 9) and outlines the

	exceptions whereby a head of a public body *may* refuse to disclose information,[404] as well as instances where the head of the public body is obligated not to disclose information.[405] The Act compels the head of a public body to refuse to disclose personal information[406] if doing so would amount to an "unreasonable invasion of a third party's privacy."[407] The Act further defines what would be "unreasonable"[408] in that context, exceptions to this obligation,[409] as well as a notice requirement in the event that personal information is disclosed.[410] Additionally, the Act imposes obligations related to the collection,[411] protection,[412] and use[413] of "personal information." Lawyers working on behalf of, or with, the Crown in Manitoba should be aware of these requirements.
Privacy Act[414]	This Act creates a tort, allowing a person to bring a claim for damages against a person "who substantially, unreasonably, and without claim of right, violates the privacy of another person."[415]

procedure and form by which such requests must be answered (including timelines).

404 This includes, but is not limited to: s 23 (advice to a public body), s 24 (harmful to individual or public safety), s 27 (solicitor client privilege).

405 This includes, but is not limited to: s 17 (disclosure harmful to a third party's privacy), s 18 (business interests, with an exception in the case of public interest at s 18(4)).

406 *Ibid*, s 1(1), personal information means recorded information about an identifiable individual. The section contains many examples.

407 *Ibid*, s 17(1).

408 *Ibid*, ss 17(2) & 17(3).

409 *Ibid*, s 17(4).

410 *Ibid*, s 33(1).

411 *Ibid*, ss 36-37.

412 *Ibid*, s 41.

413 *Ibid*, ss 42-48 (Division 3 of Part 2).

414 Privacy Act, RSM 1987, c P125, CCSM c P125.

415 *Ibid*, s 2(1). Note, unlike some other provincially created statutory torts concerning the

	While this Act may not have direct relevance to the cybersecurity interests of law practices, the haphazard use of technology could potentially violate the privacy of another, exposing lawyers to potential litigation, especially considering that this tort does not require the violation to be brought about "wilfully" (as other provincial Acts do).
The Personal Health Information Act[416]	*The Personal Health Information Act*, which has similar counterparts in most common-law provinces, governs the use of "personal health information"[417] by trustees[418] in the healthcare system. The Act has several aims, including governing the collection,[419] use,[420] retention,[421] and disclosure[422] of personal health information, while attempting to balance the competing interests of an individual's privacy and the need for health

invasion of privacy (such as BC), this Act does not require the violation to be wilful. *Ibid*, s 3 gives specific examples of breaches of privacy.

416 *The Personal Health Information Act*, SM 1997, c 51, CCSM c P33.5.

417 *Ibid*, s 1, personal health information means "recorded information about an identifiable individual that relates to (a) the individual's health, or health care history, including genetic information about the individual, (b) the provision of health care to the individual, or (c) payment for health care provided to the individual, and includes (d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and (e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;"

418 *Ibid*, s 1, trustee means "a health professional, health care facility, public body, or health services agency that collects or maintains personal health information."

419 *Ibid*, ss 13-15.

420 *Ibid*, s 19.1 concerns the consent requirements when using or disclosing personal health information. s 20(1) imposes a general duty upon trustees to not use or disclose personal health information in a manner not authorized in the Act. s 21 concerns specific restrictions on the use of this information.

421 *Ibid*, s 17.

422 *Ibid*, s 19.1 concerns the consent requirements when using or disclosing personal health information. s 20(1) imposes a general duty upon trustees to not use or disclose personal health information in a manner not authorized in the Act. s 22 concerns the manner in which personal health information can be disclosed, including instances where consent is not required.

	practitioners to access said information in order to provide effective healthcare. The Act also provides individuals with the right and a mechanism to access their personal health information.[423] The Act also imposes a general obligation upon trustees of personal health information to protect said information.[424]
The Personal Investigations Act[425]	*The Personal Investigations Act* governs the collection of information for the purposes of a personal investigation.[426] The Act proscribes personal investigations without the consent of the subject[427] and specifically outlaws the presence of certain forms of information[428] in any personal report.[429] The Act also forbids the sharing of information gained in the course of a personal investigation except under specific enumerated circumstances,[430] outside of which is an offence under the Act.[431]

423 *Ibid*, s 5(1); *Ibid*, ss 5-10 govern the process; *Ibid*, s 11 provides reasons why a trustee can refuse to disclose.

424 *Ibid, s* 18(1) states: "In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information." s 18(2) imposes specific procedures to be followed by the Trustee.

425 *The Personal Investigations Act*, RSM 1987, c P34, CCSM c P34.

426 *Ibid*, s 1, personal identification means "any inquiry by any person to obtain factual or investigative information from any source other than the subject with a view to entering into or amending an agreement with the subject for credit, insurance, employment or tenancy, whether the information is transmitted immediately in a personal report or compiled in a personal file."

427 *Ibid*, s 3(1)(a); *Ibid, s* 3(1)(b) there exists an exception for government agencies conducting investigations related to the granting of denial of a "benefit," although this still requires written notice be given.

428 *Ibid*, s 4.

429 *Ibid*, s 1, personal report means "any report, whether written or oral, of information obtained from others in the course of making a personal investigation."

430 *Ibid*, s 5.

431 *Ibid*, s 19 outlines the penalties for failing to comply with the Act.

The Personal Information Protection and Identity Theft Prevention Act[432]	This law received royal assent in 2013 but has yet to come into force.[433] This Act would appear to be similar in scope and subject matter to the federal *PIPEDA*,[434] governing the collection, use and disclosure of personal information[435] by organizations, seeking to balance the privacy rights of individuals against the needs of organizations.[436] Should this Act be proclaimed, there are two specific subsections of this Act that are relevant. First, section 4(5) of the Act specifically excludes any documents protected by legal privilege[437] and specifically does not "limit or affect the collection, use or disclosure of information that is the subject of trust conditions or undertakings by which a lawyer is subject."[438] Second, this Act also contains mandatory breach notification requirements. Section 34(2) of the Act will impose upon organizations an obligation to notify an individual "as soon as reasonably practicable and in the prescribed manner," if their personal information has been "stolen, lost or accessed in an unauthorized manner."[439] The Act also provides a statutory cause of action, allowing for an individual to seek

---

432 *Bill 211, The Personal Information Protection and Identity Theft Prevention Act*, 2nd Sess, 40th Leg, Manitoba, 2013.

433 *Ibid*, *s* 45 specifies that the Act comes "into force on a day to be fixed by proclamation" which, at the time this was written has yet to happen.

434 Provincial Legislation similar to PIPEDA, *supra* note 193.

435 Bill 211 *supra* note 432, s1, personal information means "information about an identifiable individual."

436 *Ibid*, *s* 3, states that the purpose of the act is "to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable."

437 *Ibid*, *s* 4(5)(a).

438 *Ibid*, *s* 4(5)(c).

439 *Ibid*, *s* 34(2); *Ibid*, s 34(3) states exceptions to this rule.

	damages from an organization for either a loss of their personal information, or the organization's failure to notify them as required by the Act.[440]

V. TABLE 5: PROVINCIAL AND TERRITORIAL LEGISLATION: NEW BRUNSWICK

Right to Information and Protection of Privacy Act[441]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, New Brunswick's *Right to Information and Protection of Privacy Act* concerns "records"[442] and personal information[443] held by public bodies[444] in the province. The Act confers a right upon persons to access certain types of information (concerning the public business of a public body[445] or themselves[446]) and provides a statutory mechanism for requesting this information.[447] The Act also provides a series of

440 *Ibid*, s 34(4).

441 Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6.

442 *Ibid*, s 1, records mean "a record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records." s 4 of the Act specifically enumerates the records which are excluded from this Act.

443 *Ibid*, s 1, personal information means "recorded information about an identifiable individual," with a number of examples.

444 *Ibid*, s 1, public bodies means "(i) a department, secretariat or office of the Province of New Brunswick, including but not limited to those portions of the public service specified in Part I of the First Schedule of the Public Service Labour Relations Act, (ii) a government body, board, Crown corporation or commission listed under Part IV of the First Schedule of the Public Service Labour Relations Act, (iii) a government body, (iv) the office of a Minister of the Crown, or (v) a local public body." The definition specifically excludes the office of a member of the Legislative Assembly, the office of an officer of the Legislative Assembly and the NB Courts from the scope of this term.

445 *Ibid*, s 7(2).

446 *Ibid*.

447 *Ibid*, ss 8-16 govern this, including a statutory duty imposed upon the head of a public

	mandatory[448] and discretionary[449] exceptions whereby a head of a public body shall not disclose requested information. Additionally, the Act imposes obligations related to the collection,[450] use and disclosure[451] of personal information. Lawyers working on behalf of, or with, the Crown in New Brunswick should be aware of these restrictions.
Personal Health Information Privacy and Access Act[452]	New Brunswick's *Personal Health Information Privacy and Access Act* has been deemed "substantially similar" to Part 1 of *PIPEDA*, and as such, any personal health information custodian[453] to which this Act applies is exempt from *PIPEDA* with regards to their collection, use and disclosure of personal health information.[454] The Act, which

body to make every reasonable effort to assist applicants (s 9).

448 *Ibid*, Division B (ss 17-22); Amongst this enumerated list is where the disclosure of this information would be an unreasonable invasion of a third party's privacy (s 21(1)); s 21(2) enumerates a series of situations which would be considered unreasonable. s 34 further imposes an obligation for the head of a public body give notice to a third party if they are considering disclosing information which "might" fall under the criteria of s 21(1) or s 22's third party interest.

449 *Ibid*, Division C (ss 23-33), including legal privilege at s 27(1).

450 *Ibid*, ss 37-38.

451 *Ibid*, s 43 imposes a general duty upon public bodies to not use of disclose Personal information except for where authorized by the statute and that the information released be confined to a minimum amount of information necessary. s 44 enumerates the situations where a public body may use of personal information. s 46 specifically enumerates situations where a public body may disclose personal information. s 47 outlines a general statutory mechanism by which personal information can be used or disclosed in situations not previously enumerated in the Act.

452 Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05. [NB Personal Health Information Act]

453 *Ibid*, s 1, custodian means "an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and management of the health care system or delivering a government program or service." This definition includes a number of enumerated examples.

454 Personal Health Information Custodians in New Brunswick Exemption Order, SOR/2011-265;

	has similar counterparts in most common-law provinces, governs the collection,[455] use,[456] and disclosure[457] of personal health information.[458] The Act also provides individuals with the right and a mechanism to access their personal health information.[459] The Act also imposes a general obligation upon custodians of personal health information to protect said information,[460] as well as affirmative duties to notify individuals and the Commissioner when said information is lost, stolen, improperly disposed of or disclosed.[461] Lawyers whose practice involves personal health information, while not being subject to the Act, will still likely need to be aware of its requirements and restrictions.

VI. TABLE 6: PROVINCIAL AND TERRITORIAL LEGISLATION: NEWFOUNDLAND AND LABRADOR

Personal Health Information Act[462]	Newfoundland and Labrador's *Personal Health Information Act* has been deemed "substantially similar" to Part 1 of PIPEDA, and as such, any

Ibid, s 1, personal health information means "identifying information about an individual in oral or recorded form" with 7 specific limiting conditions on that initial broad definition (a-g).

455 NB Personal Health Information Act, supra note 454 at Part 4, Division A, ss 27-31.

456 *Ibid* at Part 4 Division B, ss 32-34.

457 *Ibid* at Part 4, Division C, ss35-47.

458 A central feature of this Act is its consent requirements found in Part 3 (ss 17-26) for the collection, use and disclosure of personal health information.

459 *Ibid* at Part 2, ss 7-14.

460 *Ibid*, s 50(1) states: "in accordance with any requirements prescribed by the regulations, a custodian shall protect personal health information by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information."

461 *Ibid*, s 49(1)(c); *Ibid*, s 49(2) provides situations where the notification requirements of s 49(1)(c) does not apply.

462 Personal Health Information Act, SNL 2008, c P-7.01.

	personal health information custodian[463] to which this Act applies is exempt from *PIPEDA* with regards to their collection, use and disclosure of personal health information.[464] The Act, which has similar counterparts in most common-law provinces, governs the collection,[465] use,[466] and disclosure[467] of personal health information. The Act also provides individuals with the right and a mechanism to access their personal health information.[468] The Act also imposes a general obligation upon custodians of personal health information to protect said information,[469] as well as affirmative duties to notify individuals when said information is lost, stolen, improperly disposed of or disclosed.[470]

463 *Ibid*, s 4.

464 Personal Health Information Custodians in Newfoundland and Labrador Exemption Order, SI/2012-72; *Ibid*, s 5.

465 *Personal Health Information Act, supra* note 467 at Part IV, specifically ss 29-32; See also ss 23-28.

466 *Ibid* at Part IV, specifically ss 33-35; See also *Ibid,* ss 23-28.

467 *Ibid* at Part IV, specifically ss 36-50; See also *Ibid* at ss 23-28.

468 *Ibid, s* 52; *Ibid*, ss 53-64 set out the mechanism for access and correcting personal health information as well as the duties imposed upon custodians related to this mechanism.

469 *Ibid, s* 13(1) establishes an obligation on custodians to establish and implement "information policies and procedures to facilitate the implementation of, and ensure compliance with, this Act and the regulations respecting the manner of collection, storage, transfer, copying, modification, use and disposition of personal information whether within or outside the province." s 13(2) imposes further obligations, including (a) which requires that any procedures defined in s 13(1) protect the confidentiality of personal health information, and the privacy of the individual. s 13(3) of the Act requires that the policies and procedures referenced in s 13(1) also "shall include appropriate measures to address the risks associated with the storage of personal health information." s 15(1) also imposes a general obligation for custodians to "take steps that are reasonable" so as to (a) protect personal health information from loss, theft and unauthorized use or disclosure, or (b) to prevent unauthorized copying or modification.

470 *Ibid, s* 15(3) sets out this requirement, while s 15(7) provides exceptions where such notice is not required. Additionally, s 15(4) requires a custodian to inform the commissioner if there has been a "material breach," as defined in the regulations.

	Lawyers whose practice involves handling personal health information, while not being subject to the Act, will likely still need to be aware of its requirements and restrictions.
Access to Information and Protection of Privacy Act, 2015[471]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Newfoundland and Labrador's *Access to Information and Protection of Privacy Act, 2015* concerns "records"[472] and personal information[473] held by public bodies[474] in the province.[475] The Act confers a right upon a person to access records held by a public body, including personal information pertaining to that person,[476] and provides a statutory mechanism for requesting this information.[477] The Act also provides a series of mandatory[478] and discretionary[479] exceptions

471 *Access to Information and Protection of Privacy Act*, 2015, SNL 2015, c A-1.2.

472 *Ibid*, s 2(y), records mean "a record of information in any form, and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium;"

473 *Ibid*, s 2(u), personal information means "recorded information about an identifiable individual." The Act then lists a number of examples.

474 A list of "public bodies" is enumerated in s 2(x) of the Act and those designated in the Act's regulations or Schedule B.

475 *Ibid*, s 5 specifically enumerates those records which are not to be protected by this Act.

476 *Ibid*, s 8(1) defines the right, while ss 8(2) & (3) provide some initial restrictions.

477 *Ibid*, ss 11-26 outline this mechanism. Divisions 3 & 4, ss 42-60 detail the appeal mechanism for such requests.

478 *Ibid*, ss 33(2), 34(2), 39-41. S 40 imposes a duty upon the head of a public body to refuse to disclose personal information "where the disclosure would be an unreasonable invasion of a third party's personal privacy," and the remaining sections of s 40 provides guidance for what could be considered unreasonable for the purposes of the section.

479 *Ibid*, ss 28-32, 34(1), 35(1), 36-38. Additionally, s 9 provides an exception where the head of a public body is not entitled to utilize their discretionary exceptions specifically enumerated in s 9(2) to not release information if "it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception."

	whereby a head of a public body shall not disclose requested information. Additionally, the Act imposes obligations related to the collection,[480] protection,[481] use[482] and disclosure[483] of personal information. Lawyers working on behalf of, or with, the Crown in Newfoundland & Labrador should be aware of these restrictions.
Privacy Act[484]	This Act makes it an actionable tort for "a person, wilfully and without a claim of right, to violate the privacy of an individual."[485] The Act also enumerates a specific set of situations or actions which, when they occur without consent, can be said to be proof of a violation of privacy.[486] While this Act may not have a direct relevance to the cybersecurity interests of law practices, the haphazard use of technology could potentially violate the privacy of another, exposing lawyers to litigation.

VII. TABLE 7: PROVINCIAL AND TERRITORIAL LEGISLATION: NOVA SCOTIA

Freedom of Information and	Belonging to a class of legislation found across all jurisdictions which governs the use of

480 *Ibid*, ss 61-62.

481 *Ibid*, s 64 imposes a duty upon the head of a public body to "take steps that are reasonable in the circumstances to ensure that (a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure."

482 *Ibid*, ss 66-67.

483 *Ibid*, ss 68-72.

484 *Privacy Act*, RSNL 1990, c P-22.

485 *Ibid*, s 3(1); *Ibid*, s 3(2) states: "The nature and degree of privacy to which an individual is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of an individual, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties."

486 *Ibid*, s 4.

Protection of Privacy Act[487]	information held by the government, Nova Scotia's *Freedom of Information and Protection of Privacy Act* concerns "records"[488] and personal information[489] held by public bodies[490] in the province.[491] The Act confers a right upon a person to access records held by a public body,[492] and provides a statutory mechanism for requesting this information.[493] The Act also provides a series of mandatory[494] and discretionary[495] exceptions whereby a head of a public body shall not disclose requested information. Additionally, the Act imposes obligations related to the collection,[496] protection,[497] use[498] and disclosure[499] of personal information. Lawyers

487 *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5.

488 *Ibid*, s 3(k), records "includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records."

489 *Ibid*, s 3(i), personal information means "recorded information about an identifiable individual" The Act then lists a number of enumerated examples.

490 *Ibid*, s 3(j), public bodies includes bodies designated by order in council and enumerated in the Act's Schedule.

491 *Ibid*, s 4(1) stipulates that the Act applies to all records in the custody or control of a public body, while s 4(2) provides a list of enumerated exceptions.

492 *Ibid*, s 5(1) provides this right, with s 2 specifying limitations.

493 *Ibid*, ss 6-11, 22-23 provides the statutory mechanism by which access must be given.

494 *Ibid*, ss 20-21.

495 *Ibid*, ss 12-19.

496 *Ibid*, s 24.

497 *Ibid*, s 24(3) states: "The head of the public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

498 *Ibid*, ss 26 & 28.

499 *Ibid*, ss 27, 29-31.

	working on behalf of, or with, the Crown in Nova Scotia should be aware of these restrictions.
Personal Information International Disclosure Protection Act[500]	This Act requires that a public body or service provider[501] ensure that any personal information[502] in their custody be stored and accessed only in Canada;[503] the Act then prescribes a number of situations where this restriction can be avoided.[504] The Act also imposes restrictions on the disclosure of personal information outside of Canada,[505] as well as requirements for how public bodies and providers are to deal with foreign demands for disclosure.[506]
Privacy Review Officer Act[507]	This Act creates a Privacy Review Officer, akin to the privacy commissioners in other jurisdictions, and enumerates their powers.[508]
Personal Health Information Act[509]	The *Personal Health Information Act*, which has similar counterparts in most common-law provinces, governs the use of "personal health information"[510] by custodians[511] of the healthcare

500 *Personal Information International Disclosure Protection Act*, SNS 2006, c 3, s 43.

501 *Ibid*, s 2(g), service provider means "a person who (i) is retained under a contract to perform services for a public body, and (ii) in the course of performance of the services, uses, discloses, manages, stores or accesses personal information in the custody or under the control of a public body."

502 *Ibid*, s 2(2) states: "words and expressions have the same meaning as in the Freedom of Information and Protection of Privacy Act."

503 *Ibid*, s 5(1).

504 *Ibid*, ss 5(1)(a)-(4).

505 *Ibid*, s 9; *Ibid* at s 9(1) only allows information to be disclosed as permitted in the Act; *Ibid* at ss 9(2)-(4) gives examples of when information may be disclosed outside of Canada.

506 *Ibid*, s 6.

507 Privacy Review Officer Act, SNS 2008, c 42, s 1.

508 *Ibid*, ss 5-6.

509 Personal Health Information Act, SNS 2010, c 41.

510 *Ibid*, s 3(r).

511 *Ibid*, s 3(f).

	system. The Act has several aims, including governing the collection,[512] use,[513] retention,[514] and disclosure[515] of personal health information, while attempting to balance the competing interests of an individual's privacy and the need for health practitioners to access said information in order to provide effective healthcare.[516] The Act also provides individuals with the right[517] and a mechanism to access their personal health information.[518] The Act also imposes obligations upon custodians of personal health information to protect said information,[519] and to notify individuals when there is a breach of said information.[520] Lawyers whose practice involves personal health information, while not being subject to the Act, will

512 *Ibid*, ss 30-32; Also subject to consent requirements set out in ss 11-29.

513 *Ibid*, ss 33-34. Also subject to consent requirements set out in ss 11-29, but with exceptions enumerated in s 35(1).

514 *Ibid*, s 47.

515 *Ibid*, ss 36-37. Also subject to consent requirements set out in ss 11-29, but with exceptions enumerated in ss 38-44.

516 *Ibid*, s 2 states: "The purpose of this Act is to govern the collection, use, disclosure, retention, disposal and destruction of personal health information in a manner that recognizes both the right of individuals to protect their personal health information and the need of custodians to collect, use and disclose personal health information to provide, support and manage health care."

517 *Ibid*, s 71.

518 *Ibid*, ss 75-84; *Ibid* at ss 85-90 outline the process for requesting corrections; *Ibid*, ss 91-103 outline the appeals process.

519 *Ibid*, ss 61-66 impose a number of obligations upon custodians with regards to protecting the information in their custody. Amongst them are s 61, a duty to protect the confidentiality of health information and the privacy of the individuals who are subject of that information and s 62 which impose duties regarding information practices which are (b) reasonable and (c) ensure that PHI is protected against (i) theft or loss and (ii) unauthorized access, use or disclosure.

520 *Ibid*, s 69 details a general duty to notify individuals whose personal health information has been stolen, lost or subject to authorized access if there is a "potential for harm or embarrassment to the individual." s 70 details instances where there is no need to notify.

	still likely need to be aware of its requirements and restrictions.

VIII. TABLE 8: PROVINCIAL AND TERRITORIAL LEGISLATION: ONTARIO

Freedom of Information and Protection of Privacy Act[521]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Ontario's Freedom of Information and Protection of Privacy Act concerns "records"[522] and personal information[523] held by institutions[524] in the province. The Act confers a right upon a person to access records held by a public body[525], and provides a statutory mechanism for requesting this information.[526] The Act also provides a series of mandatory[527] and discretionary[528] exceptions whereby a head of a public body shall not disclose requested information.

521 Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31.

522 *Ibid*, s 2, records means "any record of information however recorded, whether in printed form, on film, by electronic means or otherwise," and the Act enumerates a number of examples.

523 *Ibid*, s 2, personal information means "recorded information about an identifiable individual." The Act then lists a number of enumerated examples.

524 *Ibid*, s 2, institutions means Legislative Assembly, the ministries of the government of Ontario, a service provider, as defined in the Ministry of Government Services Act, a hospital, and also those bodies designated by the regulations; RRO 1990, Reg 460, s 1(1) expands this list of institutions to include more than 157 enumerated examples listed in Schedule 1 of the regulation.

525 *Freedom of Information and Protection of Privacy Act*, *supra* note 523, s 10.(1) grants the right, subject to exceptions.

526 *Ibid*, ss 11, 24-30, Part IV of the Act deals with appeals.

527 *Ibid*, ss 12(1), 17, 21.

528 *Ibid*, ss 13, 14-17, 18-20, 21.1-23.

	Additionally, the Act imposes obligations related to the collection,[529] storage,[530] use[531] and disclosure[532] of personal information. Lawyers working on behalf of, or with, the Crown in Ontario should be aware of these restrictions.
Municipal Freedom of Information and Protection of Privacy Act[533]	Similar in scope to the above-mentioned Freedom of Information and Protection of Privacy Act of Ontario, the Municipal Freedom of Information and Protection of Privacy Act concerns records and personal information[534] held by municipalities, enumerated municipal agencies and services,[535] and other bodies enumerated in the regulations.[536] As with the many of the previous Acts, this Act provides a right to, and a mechanism by which persons can, request information held by these institutions,[537] as well as imposing obligations regarding the collection,[538] use[539] and disclosure[540] of personal information by these municipal bodies.
Personal Health Information	Ontario's Personal Health Information Protection Act, 2004, has been deemed "substantially similar" to Part 1 of PIPEDA, and as such, any personal health information custodian to whom this Act applies is

529 *Ibid*, ss 38(2)-39.

530 *Ibid*, s 44 requires that all information be kept in personal information banks. RRO 1990, Reg 460, s 4(1) outlines a duty to be imposed.

531 Freedom of Information and Protection of Privacy Act, supra note 523, ss 41, 43.

532 *Ibid*, ss 41-43.

533 Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56.

534 *Ibid*, s 2.

535 *Ibid*, s 2(b).

536 *Municipal Freedom of Information and Protection of Privacy Act Regulations*, O Reg 372/91.

537 Municipal Freedom of Information and Protection of Privacy Act, supra note 535, ss 4.(1), 17-23.

538 *Ibid*, ss 28-29.

539 *Ibid*, ss 31 & 33.

540 *Ibid*, ss 32 & 33.

Protection Act, 2004[541]	exempt from PIPEDA with regards to their collection, use and disclosure of personal health information.[542] The Act, which has similar counterparts in most common-law provinces, governs the use of "personal health information"[543] by health information custodians.[544] The Act has several aims, including governing the collection,[545] use,[546] and disclosure[547] of personal health information, while attempting to balance the competing interests of an individual's privacy and the need for health practitioners to access said information in order to provide effective healthcare.[548] The Act also imposes obligations upon custodians of personal health information to protect said information,[549] and to notify individuals when there is a breach of said information.[550]

541 Personal Health Information Protection Act, 2004, SO 2004, c 3.

542 Health Information Custodians in the Province of Ontario Exemption Order, SOR/2005-399, s1.

543 Personal Health Information Protection Act, supra note 543 s 4, personal health information means identifying information about an individual if that information meets one of seven enumerated criteria ss 4(a)-(g).

544 *Ibid*, s 3.

545 *Ibid*, Part IV (specifically s 36); Subject to the Consent requirements of ss 18-29.

546 *Ibid*, Part IV (specifically s 37); Subject to the Consent requirements of ss 18-29.

547 *Ibid*. Part IV (specifically s 38-50); Subject to the Consent requirements of ss 18-29.

548 *Ibid*, s 1(a) states that the purpose of the Act is "to establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care".

549 *Ibid*, s 12(1) states: "shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal;" See also s 13.

550 *Ibid*, s 12(2) states: "if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall, (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure;" There exists an exception for researcher's whose data has been stolen

	Lawyers whose practice involves personal health information, while not being subject to the Act, will still likely need to be aware of its requirements and restrictions.

IX. TABLE 9: PROVINCIAL AND TERRITORIAL LEGISLATION: PRINCE EDWARD ISLAND

Freedom of Information and Protection of Privacy Act551	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Prince Edward Island's Freedom of Information and Protection of Privacy Act concerns "records"552 and personal information553 held by public bodies554 in the province. The Act confers a right upon a person to access records held by a public body,555 and provides a statutory mechanism for requesting this information.556 The Act also provides a series of mandatory and discretionary exceptions whereby a head of a public body shall not disclose requested information.557

if it was acquired with consent s 12(4).

551 *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01.

552 *Ibid*, s 1(l).

553 *Ibid*, s 1(i), personal information means "recorded information about an identifiable individual" and the Act provides a number of enumerated examples.

554 *Ibid*, s 1(k).

555 *Ibid*, s 6(1).

556 *Ibid*, ss 7-13.

557 *Ibid* at Division 2 (ss 14-27); *Ibid*, s 15(1) states: "shall refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy. "Additionally, there are government obligations to inform persons when their information has been disclosed.

	Additionally, the Act imposes obligations related to the collection,[558] storage,[559] use[560] and disclosure[561] of personal information. Lawyers working on behalf of, or with, the Crown in Prince Edward Island should be aware of these restrictions.

X. TABLE 10: PROVINCIAL AND TERRITORIAL LEGISLATION: QUEBEC

An Act respecting the Protection of Personal Information in the Private Sector[562]	This Act is deemed to be "substantially similar" to PIPEDA and as such, pursuant to PIPEDA Regulations, organizations subject to this Act, "other than a federal work, undertaking or business," are exempt from the provisions found in Part 1 of *PIPEDA*.[563] It is therefore not surprising that there is considerable overlap between *PIPEDA* and this Act. The stated purpose of this Act is to govern the collection, storage, use and communication of personal information by persons engaging in enterprises as defined by the Civil Code.[564]

558 *Ibid*, ss 31-32.

559 *Ibid*, s 35.

560 *Ibid*, ss 36 & 38.

561 *Ibid*, ss 37-40.

562 *An Act respecting the Protection of Personal Information in the Private Sector,* CQLR c P39.1.

563 *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.

564 An Act respecting the Protection of Personal Information in the Private Sector, *supra* note 564, s 1, states: "The object of this Act is to establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code [Respect of Reputation and Privacy] concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code." Enterprise, as defined in article 1525 of the Civil Code is "The carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service, constitutes the operation of an enterprise." Personal Information as defined in s 2 of the Act means "any information which relates to a natural person and allows that person to be identified."

	Like *PIPEDA*, the Act imposes obligations upon persons carrying on an enterprise with regards to the personal information they control, including consent requirements[565] and limitations on the collection,[566] usage[567] and communication[568] of personal information, including restrictions on the circumstances in which said personal information can be transferred outside of the province.[569] The Act also provides individuals with a right to review any personal information concerning them which is held by an enterprise.[570] The Act also imposes obligations upon the holders of personal information to protect personal information in their custody by taking "the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored."[571] In order to enforce these obligations, the Act contains a number of penal provisions, which impose fines upon individuals who fail to comply with the obligations set out in the Act.[572] Finally, the Act confers certain powers upon the *Commission d'accès à l'information*,[573] including oversight authority and investigative powers regarding compliance with the Act[574] and the ability to respond to requests and complaints regarding access to personal information held

565 *Ibid*, ss 14-15.

566 *Ibid* at Division II (ss 4-9).

567 *Ibid*, ss 12-13.

568 *Ibid*, ss 13, 18, 18.1 (an affirmative duty to communicate to prevent an act of violence), 18.2.

569 *Ibid*, s 17.

570 *Ibid*, Division IV (ss 27-41). This division includes a mechanism and a number of exceptions.

571 *Ibid*, s 10.

572 *Ibid*, ss 91-93.

573 *Ibid*, s 103.

574 *Ibid*, ss 81-87.

	by an enterprise; the Act provides an administrative process for such disputes, including rights of appeal to a judge of the Court of Québec.[575]
An Act to Establish a Legal Framework for Information Technology[576]	In their text on privacy legislation, McIsaac, Shields and Klein note that the aforementioned *Act respecting the Protection of Personal Information in the Private Sector* must be read alongside *An Act to Establish a Legal Framework for Information Technology*, due to the latter's provisions regarding the "confidentiality of information found in technology based documents."[577] The most obvious of these provisions would be section 25 of this Act, which imposes an obligation upon the persons who control technology-based documents containing confidential information to take "appropriate security measures."[578] The Act also places restrictions on the use of biometrics, which may be relevant to cybersecurity measures contemplated by law firms.
An Act respecting Access to Documents Held by Public Bodies and the Protection of	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Quebec's *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* concerns documents held by public bodies and professional orders[580] in the province. The Act confers a right upon a person to access records held by a public body,[581] including personal

575 *Ibid*, ss 42-69.

576 *An Act to Establish a Legal Framework for Information Technology*, CQLR, c C1.1.

577 Barbara McIsaac, Rick Shields & Kris Klein, *supra* note 135 at 4.5.1.

578 *An Act to Establish a Legal Framework for Information Technology*, supra note 578, s 25, states: "The person responsible for access to a technology-based document containing confidential information must take appropriate security measures to protect its confidentiality, such as controlling access to the document by means of a restricted view technique, or any technique that prevents unauthorized persons from accessing such information or from otherwise accessing the document or the components providing access to the document."

580 *Ibid*, ss 1 & 1.1; The Act enumerates which institutions are to be considered public bodies for the purposes of ss 3-7, including the Government (s 3), municipal bodies (s 5), school bodies (s 6), health and social service institutions (s 7), and a more general provision (s 4) concerning non-enumerated bodies.

581 *Ibid*, s 8.

Personal Information[579]	information concerning them held by the state,[582] and provides a statutory mechanism for requesting this information.[583] The Act also provides a series of mandatory and discretionary exceptions whereby a head of a public body shall not disclose requested information.[584] Additionally, the Act also imposes an obligation requiring that personal information be kept confidential, except in specific circumstances, such as where the information is public, or consent is given.[585] Furthermore, the Act imposes obligations related to the collection,[586] storage,[587] use[588] and disclosure[589] of personal information, including a general provision requiring a public body to take "the security measures necessary to ensure the protection" of said information.[590] Lawyers working on behalf of, or with, the Crown in Quebec should be aware of these restrictions.
Civil Code of Quebec	The Civil Code of Quebec has a number of privacy-related provisions which need to be addressed. Foremost amongst them is that under the Civil Code, a person has an unalienable right to the "respect of his name, reputation and privacy."[591] This right is expanded upon in later

579 An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, CQLR, c A2.1.

582 *Ibid*, Division IV (s 83).

583 *Ibid*, ss 10-17; *Ibid* at Division III (ss 42-52.1); See also *Ibid* at ss 84-85, 94-102.1.

584 *Ibid*, Division II (ss 18-24, 27, 28-41.3); See also ss 86-88.1.

585 *Ibid*, ss 53 & 55; s 54 defines personal information. s 57 defines which personal information is "public information."

586 *Ibid*, ss 64-65.

587 *Ibid*, Division III, concerning personal information files.

588 *Ibid*, s 65.1.

589 *Ibid*, ss 66-68.1.

590 *Ibid*, s 63.1 states: "A public body must take the security measures necessary to ensure the protection of the personal information collected, used, released, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored."

591 Civil Code of Quebec, SQ 1991, c 64, at Book 1, title 1, s 3.

	sections of the Code, which amongst other features, specifically proscribes violating the privacy of another individual without their consent, enumerates a number of examples of violations of privacy and imposes limitations upon the gathering of information about individuals.[592] These provisions are reflected in the *Act respecting the Protection of Personal Information in the Private Sector*, discussed above.

XI. TABLE 11: PROVINCIAL AND TERRITORIAL LEGISLATION: SASKATCHEWAN

Freedom of Information and Protection of Privacy Act[593]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Saskatchewan's *Freedom of Information and Protection of Privacy Act* concerns records[594] held by government institutions[595] in the province. The Act confers a right upon a person to access records held by a government institution,[596] and provides a statutory mechanism for requesting this information.[597] The Act also provides a series of mandatory and discretionary exceptions whereby a head of a government institution shall not disclose requested information.[598] Additionally, the Act imposes obligations related to the collection,[599] use[600] and disclosure[601] of personal

592 *Ibid* at Title 2, chapter 3, ss 35-41.

593 Freedom of Information and Protection of Privacy Act, SS 1990-91, c F-22.01.

594 *Ibid*, s 2.

595 *Ibid*, s 2(2).

596 *Ibid*, s 5.

597 *Ibid*, ss 6-12.

598 *Ibid*, ss 13-23; Additionally, the Act's regulations detail other instances wherein disclosure is permitted, ss 14-18; The Freedom of Information and Protection of Privacy Regulations, RRS c F-22.01 Reg 1.

599 *Ibid*, ss 25-26.

600 *Ibid*, s 28.

601 *Ibid*, s 29.

	information[602] by government institutions, and creates a summary offence for knowingly collecting, using or disclosing of personal information in contravention of the Act.[603] Lawyers working on behalf of, or with, the Crown in Saskatchewan should be aware of these restrictions.
The Health Information Protection Act[604]	The *Health Information Protection Act*, which has similar counterparts in most common-law provinces, governs the use of "personal health information"[605] by trustees[606] in the healthcare system. The Act has several aims, including governing the collection,[607] use,[608] and disclosure[609] of personal health information, while attempting to balance the competing interests of an individual's privacy and the need for health practitioners to access said information in order to provide effective healthcare.[610] The Act also provides individuals with the right and a mechanism to access their personal health information.[611] The Act also imposes obligations upon custodians of

602 *Ibid*, s 24(1) states: "personal information about an identifiable individual that is recorded in any form." This section of the Act also enumerates a number of specific examples of what constitutes personal information and provides a number of exceptions.

603 *Ibid*, s 68(1).

604 The Health Information Protection Act, SS 1999, c h-0.021.

605 *Ibid*, s 2(M).

606 *Ibid*, s 2(t).

607 *Ibid* at Part IV (specifically ss 23-25); Also subject to the consent requirements found in ss 5-7 of the Act.

608 *Ibid* at Part IV (specifically ss 23, 26, 29, 30); Also subject to the consent requirements found in ss 5-7 of the Act.

609 *Ibid* at Part IV (specifically ss 23, 27-30); Also subject to the consent requirements found in ss 5-7 of the Act; Additionally, s 10(1) requires that a trustee take "reasonable steps to ensure that the trustee is able to inform an individual about any disclosures... made without the individual's consent."

610 The introductory paragraph of the Act.

611 *Ibid*, s 12 gives a person the right to request access to any personal health information about themselves held by a trustee; *Ibid* at Part V (ss 31-40) outlines the statutory mechanism by which someone can access their personal health information; *Ibid* at Part VI concerns the appeals process for the processes outlined in Part V.

	personal health information to protect said information,[612] and to notify individuals when there is a breach of said information.[613] Lawyers whose practice involves personal health information, while not being strictly subject to the Act, will still likely need to be aware of its requirements and restrictions.
The Privacy Act[614]	This Act creates a tort actionable against a person who "wilfully and without claim of right" violates the privacy of another person.[615] The Act additionally enumerates a non-exhaustive list of examples of privacy violations,[616] as well as providing a number of defences against the tort.[617] While this Act may not have direct relevance to the cybersecurity interests of law practices, the haphazard use of technology could potentially violate the privacy of another, exposing lawyers to litigation.

XII. TABLE 12: PROVINCIAL AND TERRITORIAL LEGISLATION: NORTHWEST TERRITORIES

Access to Information and Protection of Privacy Act[618]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, the Northwest Territories' *Access to*

612 *Ibid* at Part III specifically details the duties imposed upon trustees with regards to protecting personal information; *Ibid*, s 16 imposes a duty upon trustees to ensure that personal health information is protected from damage (s 16(b)(i)), loss (s 16(b)(ii)), or unauthorized access (s 16(b)(iii)).

613 *Ibid*, s 10(1) requires that a trustee take all reasonable steps to ensure that it is able to inform an individual of any disclosures of their personal health information made without their consent.

614 The Privacy Act, RSS 1978, c P-24.

615 *Ibid*, s 2 states: "It is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person."

616 *Ibid*, s 3; *Ibid*, s 6 prescribes considerations to be used in determining if there has been a violation of privacy.

617 *Ibid*, s 4.

618 *Access to Information and Protection of Privacy Act*, SNWT 1994, c 20.

	Information and Protection of Privacy Act concerns records[619] held by public bodies[620] in the territory. The Act confers a right upon a person to access records held by a public body,[621] and provides a statutory mechanism for requesting this information.[622] The Act also provides a series of mandatory and discretionary exceptions whereby a head of a public body shall not disclose requested information.[623] Additionally, the Act imposes obligations related to the collection,[624] storage,[625] use[626] and disclosure[627] of personal information[628] by government institutions, and creates a summary offence for knowingly collecting, using or disclosing personal information in contravention of the Act.[629] Lawyers working on behalf of, or with, the Crown in the Northwest Territories should be aware of these restrictions.

619 *Ibid*, s 2; *Ibid*, s 3 specifically enumerates a number of records which are outside of the scope of this Act, including personal health information s (1)(b.1), or the personal notes made by someone acting in a judicial or quasi-judicial capacity s (1)(b) among other examples.

620 *Ibid*, s 2.

621 *Ibid*, s 5.

622 *Ibid* at Part I (ss 6-12).

623 *Ibid* at Part I, Division B; *Ibid*, ss 13-39 includes an appeals mechanism. Additionally, the Act imposes upon the head of a public body an obligation to provide notice to a third party whose privacy may be violated by a disclosure (s 26).

624 *Ibid*, ss 40-41.

625 *Ibid*, s 42 requires that the head of a public body protect personal information "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

626 *Ibid*, ss 43-45.

627 *Ibid*, s 47-49.

628 *Ibid*, s 2.

629 *Ibid*, s 59.

Health Information Act[630]	The *Health Information Act* belongs to the class of legislation found in most common-law jurisdictions in Canada which governs the use of "personal health information"[631] by health information custodians.[632]. The Act has several aims, including governing the collection,[633] use,[634] and disclosure[635] of personal health information, while attempting to balance the competing interests of protecting a person's personal health information and the need for healthcare practitioners to access said information in order to provide effective healthcare.[636] The Act also provides individuals with the right and a mechanism to access their personal health information.[637] The Act also imposes obligations upon custodians of personal health information to protect said information,[638] and to notify individuals when there is a breach of said information.[639] Lawyers whose practice involves personal

630 *Health Information Act*, SNWT 2014, c 2.

631 *Ibid*, s 1.

632 *Ibid*.

633 *Ibid*, ss 27-33; Also subject to the consent requirements set out in ss 14-24. Additionally, ss 67-83 concern the collection, use and disclosure of PHI for research purposes.

634 *Ibid*, ss 27-28, 34-37; Also subject to the consent requirements set out in ss 14-24. Additionally, ss 67-83 concern the collection, use and disclosure of PHI for research purposes.

635 *Ibid*, ss 27-28, 38-66, 84; Also subject to the consent requirements set out in ss 14-24. Additionally, ss 67-83 concern the collection, use and disclosure of PHI for research purposes.

636 *Ibid*, s 2 states: "The purpose of this Act is to govern the collection, use, disclosure and protection of personal health information in a manner that recognizes both the right of individuals to access and protect their personal health information and the need of health information custodians to collect, use and disclose personal health information to support, manage and provide health care."

637 *Ibid* at Part 5; s 94(1) confers the right.

638 *Ibid* at s 85-86; s 86(2) states: "The measures under subsection (1) must include measures to address risks to confidentiality and privacy associated with electronic health records that are based on nationally or territorially recognized information technology security standards and processes that are appropriate for the high level of sensitivity of personal health information."

639 *Ibid*, s 87 imposes a duty upon a custodian to notify an individual "as soon as reasonably

	health information, while not being strictly subject to the Act, will still likely need to be aware of its requirements and restrictions.

XIII. TABLE 13: PROVINCIAL AND TERRITORIAL LEGISLATION: NUNAVUT

Access to Information and Protection of Privacy Act[640]	On the day Nunavut ceased to be part of the Northwest Territories and became a separate territory,[641] the existing laws of the Northwest Territories were duplicated and became the laws of Nunavut.[642] The *Access to Information and Protection of Privacy Act* was a Nunavut statute created in this manner, and therefore it closely resembles its NWT counterpart. The Act confers a right upon a person to access records[643] held by a public body,[644] and provides a statutory mechanism for requesting this information.[645] The Act also provides a series of mandatory and discretionary exceptions whereby a head of a public body shall not disclose requested information.[646]

possible" if personal health information about that individuals has been (a) "used or disclosed other than as permitted by this Act; (b) lost or stolen; or (c) altered, destroyed or otherwise disposed of without authorization."

640 *Access to Information and Protection of Privacy Act*, *supra* note 620.

641 April 1, 1999.

642 *Nunavut Act*, SC 1993, c 28, s 29(1) states: "Subject to this Act, on the day that section 3 comes into force, the ordinances of the Northwest Territories and the laws made under them that have been made, and not repealed, before that day are duplicated to the extent that they can apply in relation to Nunavut, with any modifications that the circumstances require. The duplicates are deemed to be laws of the Legislature and the laws made under them."

643 Access to Information and Protection of Privacy Act, supra note 620, s 2.

644 *Ibid*, s 5 provides the right. Public body is defined in s 2.

645 *Ibid* at Part I, ss 6-12.1.

646 *Ibid* at Part I, Division B; See also *Ibid*, ss 13-39, including an appeals mechanism found in Division D; Additionally, the Act imposes upon the head of a public body an obligation to provide notice to a third party whose privacy may be violated by a disclosure (s 26).

	Additionally, the Act imposes obligations related to the collection,[647] storage,[648] use[649] and disclosure[650] of personal information[651] by government institutions, and creates a summary offence for knowingly collecting, using or disclosing personal information in contravention of the Act.[652] Lawyers working on behalf of, or with, the Crown in Nunavut should be aware of these restrictions.

XIV. TABLE 14: PROVINCIAL AND TERRITORIAL LEGISLATION: YUKON

Access to Information and Protection of Privacy Act[653]	Belonging to a class of legislation found across all jurisdictions which governs the use of information held by the government, Yukon's *Access to Information and Protection of Privacy Act* concerns records[654] held by public bodies[655] in the territory. The Act confers a right upon a person to access records held by a public body,[656] and provides a statutory mechanism for requesting this information.[657] The Act also provides a series of mandatory and discretionary exceptions whereby a head of a public body shall not disclose requested information.[658]

647 *Ibid*, ss 40-41.

648 *Ibid*, s 42 requires that that the head of a public body protection personal information "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

649 *Ibid*, ss 43-45.

650 *Ibid*, ss 47-49.

651 *Ibid*, s 2.

652 *Ibid*, s 59.

653 Access to Information and Protection of Privacy Act, RSY 2002, c1.

654 *Ibid*, s 3.

655 *Ibid*, s 3.

656 *Ibid*, s 5(1).

657 *Ibid* at Part 2, specifically ss 6-14, 26(1)-27.

658 *Ibid*, ss 15(1)-25(4), 28.

	Additionally, the Act imposes obligations related to the collection,[659] storage,[660] use[661] and disclosure[662] of personal information[663] by government institutions, and creates a summary offence for knowingly collecting, using or disclosing personal information in contravention of the Act.[664] Lawyers working on behalf of, or with, the Crown in Yukon should be aware of these restrictions.

659 *Ibid*, ss 29-30.

660 *Ibid*, ss 33-34, specifically s 33 reads: "The public body must protect personal information by making reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal."

661 *Ibid*, s 35.

662 *Ibid*, ss 36, 38, 39.

663 *Ibid*, s 3.

664 *Ibid*, s 67(1).

APPENDIX II: Link Index

This appendix contains a compilation of the various links that are cited throughout this manuscript with a brief description of what information can be found there.

*As noted, this manuscript was up to date to January 1st, 2020, websites marked with an asterix were not available to time of publication in 2021

Preface and Chapter 1	
2018 report of IT sector growth	https://www.comptia.org/resources/it-industry-trends-analysis
Former US President Obama's 2015 speech on cyberecurity	https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit
2011 CBC news article on law firm cyberattack	http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810
2015 Boston Business Journal commentary on Boston's law as targets of cyberattacks	http://www.bizjournals.com/boston/blog/techflash/2015/04/guest-commentary-boston-s-law-firms-are-targets.html?page=all
Cisco 2015 annual security report	https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf
Two Canadian Bar Association National Magazine articles highlighting the weak cybersecurity of law firms	http://www.nationalmagazine.ca/Articles/Sept-Oct-2013/On-guard.aspx and http://www.nationalmagazine.ca/Articles/Sept-Oct-

	2013/Renseignements-sous-surveillance.aspx
Overview of the Internet Engineering Task Force	http://www.ietf.org/old/2009/overview.html
2011 BBC News article on ACS:Law data breach	http://www.bbc.com/news/technology-13358896
2013 Financial Post article highlighting the increasing number of cyberattacks on small businesses	http://business.financialpost.com/fp-tech-desk/cyberattacks-symantec-report?__lsa=faf8-b093
2015 data loss statistics from the Open Security Foundation	https://blog.datalossdb.org/
2014 estimates of the cost of cybercrime by the Center for Strategic and International Studies	http://csis.org/files/attachments/140609_McAfee_PDF.pdf
2014 cybersecurity trends for 2014 by SmartDataCollective	https://www.smartdatacollective.com/look-cyber-security-trends-2014/
Top 11 cloud security threats for 2018 by CSO Online	https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html
2015 CBC news article on mobile phone spyware	http://www.cbc.ca/news/canada/spy-agencies-target-mobile-phones-app-stores-to-implant-spyware-1.3076546
2010 Huffington Post discussing cyberwar between America and China	http://www.huffingtonpost.com/nathan-gardels/cyberwar-with-china-forme_b_452639.html
Royal Canadian Mounted Police review 2014 cybercrime in Canada	http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada
2001 convention on cybercrime	https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
2001 convention on cybercrime signatories	https://www.coe.int/en/web/conventions/full-list/-

	/conventions/treaty/185/signatures
International Telecommunication Union 2010 cybercrime legislation resources	http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf
Public Safety Canada cyber-incident report form	https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-en.aspx
SANS Institute conversations about cybersecurity	https://www.sans.org/security-resources/cybersecurity-conversations
2013 Lexpert article on law firms as a primary cyber-target	https://www.lexpert.ca/article/law-firms-cyber-target-1/?p=&sitecode=
2013 LawPRO issue on cybercrime and law firms	https://www.practicepro.ca/wp-content/uploads/2017/09/2013-12-lawpro-magazine12-4-dec2013.pdf
Chapter 2	
Various 2016 New York Times articles on the 2016 presidential election cyberattack	http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html and http://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html?action=click&contentCollection=Politics&module=RelatedCoverage&region=Marginalia&pgtype=article and http://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html and

	http://www.nytimes.com/interactive/2016/05/27/us/politics/what-we-know-about-hillary-clintons-private-email-server.html and http://www.nytimes.com/2016/07/06/us/politics/hillary-clinton-fbi-email-comey.html?action=click&contentCollection=Politics&region=Footer&module=WhatsNext&version=WhatsNext&contentID=WhatsNext&moduleDetail=undefined&pgtype=Multimedia
Various articles on the 2014 Sony cyberattack	2014 article USA Today: http://www.usatoday.com/story/tech/2014/12/01/hack-attack-sony-pictures-north-korea-the-interview/19733463/ 2014 article by The Independent: http://www.independent.co.uk/life-style/gadgets-and-tech/news/sony-hack-us-to-officially-blame-north-korea-allege-china-could-have-helped-say-reports-9936438.html 2014 article by The Los Angeles Times: http://www.latimes.com/business/la-fi-mh-the-sony-hack-20141219-column.html 2014 article by The New York Times: http://www.nytimes.com/2015/02/06/business/amy-pascal-leaving-as-sony-studio-chief.html 2014 article by Variety Media:

	http://variety.com/2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack-1201367036/ 2016 article by Tech Times: http://www.techtimes.com/articles/171941/20160731/sony-sued-for-revenues-lost-when-film-was-released-online-in-hack.htm
The Federation of Law Societies of Canada's Model Code of Professional Conduct, amended 2017	https://flsc.ca/wp-content/uploads/2018/03/Model-Code-as-amended-March-2017-Final.pdf
Quebec's Code of Professional Conduct of Lawyers, updated 2020	http://legisquebec.gouv.qc.ca/en/pdf/cr/B-1,%20R.%203.1.pdf
Canadian Bar Association Codes of Professional Conduct	https://www.cba.org/Publications-Resources/Practice-Tools/Ethics-and-Professional-Responsibility-(1)/Codes-of-Professional-Conduct
American Bar Association Rule 1.1: Competence	http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html
American Bar Association Rule 1.1: Competence - comment	http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html
2011-2012 report to the Benchers from the Technology Committee of the Law Society of Manitoba*	http://www.lawsociety.mb.ca/publications/technology-articles/2011-2012_tech_committee_report.pdf
Guidelines on Ethics and the New Technology circulated by the Federation of Law Societies of Canada in 1999.*	https://www.nsbs.org/sites/default/files/ftp/tech_ethics_guidelines.pdf, http://www.lawsociety.mb.ca/lawyer-regulation/law-society-practice-notices/ethics_newtech.pdf/

Technology Practice Management Guideline by the Law Society of Ontario	http://www.lsuc.on.ca/For-Lawyers/Manage-Your-Practice/Technology/Technology-Practice-Management-Guideline/
Provinces legislation deemed substantially similar to PIPEDA	https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/
Chapter 3	
2012 Law Society of British Columbia Report of the Cloud Computing Working Group	https://www.lawsociety.bc.ca/Website/media/Shared/docs/publications/reports/CloudComputing_2012.pdf
2018 Business Law Today article on destruction of data	https://businesslawtoday.org/2018/06/destruction-information-difficult-essential-case-defensible-disposal/
2012 Harvard Business Review article on risk management framework	https://hbr.org/2012/06/managing-risks-a-new-framework
International Standardization Organization on IT security	https://www.iso.org/ics/35.030/x/
2012 Carnegie Mellon University guide to mitigating insider threats	http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf
2009 risk IT framework by the Information Systems Audit and Control Association*	http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf
Canadian Lawyers Insurance Association limitations on cyber-related losses, 2012 comment*	www.lawsociety.mb.ca/publications/technology-articles/TECH_Oct2012.pdf
Gardiner Miller Arnold LLP General Retainer Agreement	https://www.gmalaw.ca/wp-content/uploads/2015/07/General_Retainer_Agreement.pdf
Information on encryption	Definition of encryption:

	http://searchsecurity.techtarget.com/definition/encryption How encryption works, 2017 F-Secure article: http://safeandsavvy.f-secure.com/2016/09/01/how-does-encryption-work-and-why-its-so-important/ How encryption works, 2013 article from The Guardian: https://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works
2011 Business Insider Article on how to implement a bring your own computer policy	http://www.businessinsider.com/top-tips-for-successfully-introducing-byo-2011-4
2017 white paper by Citrix Systems Inc. on best practices for bring your own device, choose your own device and corporate-owned, personally enabled programs	https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/byod-best-practices.pdf
2012 IT Manager Daily article template for bring your own device policy	http://www.itmanagerdaily.com/byod-policy-template/
2017 Android Authority article on how to encrypt your Android device	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
2018 iOS 11 security guide, white paper by Apple, Inc.	https://www.apple.com/business/docs/iOS_Security_Guide.pdf
2017 PC Magazine article on the best mobile device management solutions	https://www.pcmag.com/article2/0,2817,2500510,00.asp
2012 Network World article on how mobile device management works	http://www.networkworld.com/article/2185771/tech-primers/how-does-mobile-device-management--mdm--work-.html

Sample corporate mobile device acceptable use policy by Wisegate LLC, 2017*	http://wisegateit.com/resources/downloads/wisegate-sample-byod-policy.pdf?_ga=1.166862838.993227471.1475359178
Bring your own device acceptable use policy by The Horton Group, 2012	https://www.thehortongroup.com/sites/default/files/pdf/1012201348157320.pdf
2015 article on wireless encryption and authentication by Cisco Meraki	https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wireless_fundamentals%3A_Encryption_and_authentication
Wi-Fi security by the Wi-Fi Alliance	http://www.wi-fi.org/discover-wi-fi/security
2016 article explaining virtual private network by My Private Network	https://www.my-private-network.co.uk/what-is-a-vpn-virtual-private-network-explained/
2011 guidelines on security and privacy in public cloud computing by the National Institute of Standards and Technology	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
2011 Law Society of British Columbia Report of the Cloud Computing Working Group	https://www.lawsociety.bc.ca/Website/media/Shared/docs/publications/reports/CloudComputing.pdf
Printers as a security threat	2013 Forbes article: http://www.forbes.com/sites/ciocentral/2013/02/07/the-hidden-it-security-threat-multifunction-printers/ 2012 PC World article: http://www.pcworld.com/article/254518/your_printer_could_be_a_security_sore_spot.html
2012 article on security best practices for USB drives by CyberScout	http://cyberscout.com/education/blog/12-security-best-practices-for-usb-drives

2016 Digital Trends article on USB drives as a security threat	https://www.digitaltrends.com/computing/usb-sticks-carry-malware/
2000 Forensic Science Communications article on recovering and examining computer forensic evidence by the Federal Bureau of Investigation	https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm
2002 sample internet and email use policy by the Law Society of British Columbia	https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/InternetPolicy.pdf
Email policy by Pomer & Boccia Professional Corporation	http://www.pomerandboccia.com/legal/email_policy.htm
Privacy policy by McTague Law Firm LLP	https://www.mctaguelaw.com/service-terms-and-policies/
Email policy template by the SANS Institute	https://www.sans.org/security-resources/policies/general#email-policy
2017 Forbes article on the cost of phishing scams on American businesses	https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#39d74d4f3fa1
Types of spam defined by Kaspersky	https://encyclopedia.kaspersky.com/knowledge/types-of-spam/
2017 CSO online article describing common cyberattacks	https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html
2017 Fortune Magazine article on top 10 phishing emails	http://fortune.com/2017/07/13/email-security-phishing/
2012 Los Angeles Times article on rental scams	http://articles.latimes.com/2012/mar/25/business/la-fi-lew-20120325
2012 Fraud Guides article on Craigslist scams	https://web.archive.org/web/20120705075209/http://www.fraudguides.com/internet-craigslist-scams.asp

2007 article in The Guardian on spammers being jailed	https://www.theguardian.com/technology/2007/oct/14/internet.crime
United States Code, 2006 Edition, Supplement 5, Title 15: commerce and trade, Chapter 103: controlling the assault of non-solicited pornography and marketing	https://www.law.cornell.edu/uscode/text/15/chapter-103
Bill C-28: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities.	https://www.parl.ca/DocumentViewer/en/40-3/bill/C-28/royal-assent
2018 Cision article on the Canadian Radio-television and Telecommunications Commission serving its first warrant under Canada's anti-spam law	http://www.newswire.ca/news-releases/crtc-serves-its-first-ever-warrant-under-casl-in-botnet-takedown-560496941.html
Canada's anti-spam Legislation	http://www.chamber.ca/resources/casl/
Frontier Networks Internet services acceptable usage policy, 2018	http://www.frontiernetworks.ca/aup/
2018 CSO online article on online anonymity	https://www.csoonline.com/article/2975193/data-protection/9-steps-completely-anonymous-online.html
2011 research article on the spam payment trail	https://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf
Interview with Stefan Savage on the spam payment trail, 2011	http://cseweb.ucsd.edu/~savage/papers/LoginInterview11.pdf
Model Internet use policy by Harvard University	https://cyber.harvard.edu/seminar/internet-client/readings/Week7/UsePolicy.doc
Model policy for social media and social networking by the Law Society of British Columbia	https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/policy_social-media.pdf

Online activity and social media policy sample from the Law Society of Upper Canada*	http://www.lsuc.on.ca/WorkArea/DownloadAsset.aspx?id=2147491875
Social media policy template by Jaffe, 2016*	http://www.jaffepr.com/policy-templates/social-media-policy-template
2012 Law Practice Magazine article on how to create a law firm social media policy*	https://www.americanbar.org/publications/law_practice_magazine/2012/january_february/how-to-create-a-law-firm-social-media-policy.html