itworldcanada.com

Understanding Canadian Cybersecurity Laws: Measuring up — Outlining existing federal cybersecurity legislation in Canada, the UK, Australia, and the US (Article 8)

Melissa Lukings and Arash Habibi Lashkari

50-64 minutes

Introduction

One year ago, with the dawn of a new decade ahead of us — the 2020s — many of us looked back at the end of 2019 and start of 2020 as a turning point; an opportunity for a fresh start. At that point in time, we had no idea of the dramatic social, educational, and occupational changes that this year would have in store for us all. While the new decade has not yet been the vibrant beacon of social and technological advancement that we may have hoped for, our global entry into 2020 has undoubtedly been a rollercoaster. From widespread mandatory isolation, necessarily remote workspaces and increased civilian interaction with public health authorities, to the necessarily rapid introduction of digital communication technologies to populations who had previously been able to avoid developing a dependance on digital technology as a primary form of social interaction. All of these factors, and more, have contributed to the massive inundation of public reliance on digital communication technology and its corresponding infrastructure in Canada.

Much of this increase in technological reliance has long been foreseen; anticipated by researchers, academics, and the especially tech-savvy folks among us. What was not anticipated,

however, was the sudden increase in the speed at which we have all had to adapt to these new realities. This past year in particular, has necessitated a review and revitalization of our existing Canadian privacy, data protection, cybersecurity, and cybercrime laws in keeping with the ongoing effort to expand, revise, or otherwise rewrite the relevant legislation to accommodate for our rapidly-evolving global, national, and localized cybersecurity concerns.

In our previous articles, we have explored the legal landscape of the current Canadian privacy and cybersecurity laws, including the relevant federal legislation: the *Privacy Act*, the *Access to Information Act*, the *Personal Information Protection and Electronic Documents Act*, the *Criminal Code of Canada*, and *Canada's Anti-Spam Legislation*; as well as the more newly recognized criminal provision for illegal distribution of intimate images the corresponding common law civil tort of "intrusion upon seclusion"; and outlining the challenges presented by the growing use of encrypted and anonymous dark networks, including Tor, which are often cross-jurisdictional. Those previous articles are included here:

In case you missed it

- Understanding Canadian cybersecurity laws: The foundations (Article 1)
- Understanding Canadian cybersecurity laws: Privacy and access to information, the Acts (Article 2)
- Understanding Canadian cybersecurity laws: Privacy protection in the modern marketplace — PIPEDA (Article 3)
- Understanding Canadian cybersecurity laws: Interpersonal privacy and cybercrime — Criminal Code of Canada (Article 4)
- **Understanding Canadian cybersecurity laws: 'Insert something clever here' — Canada's Anti-Spam Legislation (Article 5)**
- **Understanding Canadian cybersecurity laws: Peer-to-peer privacy protection — 'Intrusion Upon Seclusion' and the**

Protection of Intimate Images (Article 6)

- Understanding Canadian cybersecurity laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)

With 2020 being a year of rapid, unprecedented, large-scale global change, the many necessarily proposed alternations to our current cybersecurity-related laws have quickly shifted to the forefront of national security discussion. While the *Privacy Act,* the *Access to Information Act*, and *PIPEDA* have adequately covered our national personal privacy and granted provisions, and while the *Criminal Code of Canada* has done an adequate job of categorizing and detailing the legal provisions for criminal offences, there remains an increasingly ominous lack of comprehensive cybersecurity-specific legislation and cybercrime-specific *Criminal Code* provisions under our existing Canadian federal law. When so many features and daily facets of our lives are digitally connected to a larger network upon which our daily activities and interactions have become reliant, the idea that our national security and digital infrastructure may be at risk of exploitation or malicious interference is terrifying.

This past year, in the era of the global COVID-19 pandemic, has helped to effectively highlight many of the legislative gaps and other areas in need of improvement within our current national legislative scheme. One possible explanation for this gap is the reality that the speed of technological development increased far too quickly, when compared with the adaption of our federal legislation, to allow for the construction of adequately-tailored legal accommodations. Posited from an adjusted position, another explanation of the same result is that the legislation did not adapt quickly enough to keep up with the inevitable (and arguably foreseeable) advances in data technology and digital communication that we have seen and continue to see.

Fortunately, we are not alone. Indeed, many other countries are experiencing the same push to revise and re-evaluate legislative structures which had, until very recently, been adequately effective at regulating privacy relations and general data protection. In this

article, we will outline the relevant national privacy and cybersecurity-related laws currently in effect in the United Kingdom, Australia, and the United States, as fellow common law countries.

Common law countries

Countries that follow the common law legal system, including Canada, the United Kingdom, Australia, and the United States are considered to be “common law countries”. The basis for common law legal system relies upon a body of customary law; the body of unwritten laws based on legal precedents established by the courts in previous judicial decisions.

In addition to being common law countries, Canada, the United Kingdom, Australia, and the United States each have specific statutory provisions which apply to identity theft and fraud, copyright infringement, patents and intellectual property, commercial electronic messages, and general criminal provisions. We can start by reviewing the current laws in Canada before outing the laws in effect in the United Kingdom, Australia, and the United States, respectively.

Review of Current Cybersecurity Laws in Canada

In our past articles, we outlined the existing legislation related to cybersecurity and data privacy in Canada: the *Privacy Act*, the *Access to Information Act*, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, the *Criminal Code of Canada*, and *Canada’s Anti-Spam Legislation (CASL).* As a quick review, the relevant Canadian cybersecurity legislation is outlined below, as described in our previous articles in this series.

Regulating governmental relationships

The *Privacy Act* and the *Access to Information Act* were both implemented by the Canadian federal government in 1985 and have acted as a starting point for more recent legislation and privacy laws, including those pertaining to the cyber sector. These Acts work together to provide a legislative framework for personal data collection, use, retention, disclosure, and individual access

within the federal public sector.

***Privacy Act* (RSC 1985, c P-21)**

The *Privacy Act* regulates governmental bodies' access to the information of individuals. The *Privacy Act* is the legal framework governing personal information in the federal public sector. It explains how personal information must be protected in the relationships between individuals and the federal government.

***Access to Information Act* (RSC 1985, c A-1)**

The *Access to Information Act*, in contrast, serves to provide a method for individuals to access their own personal information as held by those governmental bodies. The fundamental key to the *Access to Information Act* is the "right of access". This legislation is overseen by the Information Commissioner of Canada.

Regulating businesses, organizations, and commercial enterprises

The commercial marketplace, including private businesses, corporations, and organizations, must abide by the provisions established in the *Personal Information Protection and Electronic Documents Act* and by the rules regulating the use of commercial electronic messages in *Canada's Anti-Spam Legislation.*

***Personal Information Protection and Electronic Documents Act* (SC 2000, c 5)**

The *Personal Information Protection and Electronic Documents Act*, otherwise known as *PIPEDA*, officially became law in 2000 as a means to help grow consumer trust in both electronic commerce and the digital economy.

The *PIPEDA* applies specifically to private-sector organizations; which are operating either fully or partially in Canada; and, that collect, use, or disclose personal information in the course of commercial activities. For the purposes of this legislation, the law defines a commercial activity as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial

character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

Private sector organizations that fit into this category are bound by the provisions of the *Personal Information Protection and Electronic Documents Act* to apply the provided privacy principles to protect consumer information exchanged during commercial activities. These provisions aim to protect the privacy of those individuals, specific subsets and targeted groups of individuals, or organizations from whom the personal information has been gathered.

Exemptions to *PIPEDA* arise when a province already has its own privacy legislation. Those provinces are currently: Alberta, British Columbia, and Quebec. *PIPEDA* provisions can also be applied specifically to personal health information collected or handled in the provinces of: Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia. These exemptions to *PIPEDA* apply only where the commercial activity actually took place within the relevant province.

***Canada's Anti-Spam Legislation* (SC 2010, c 23)**

Canada's Anti-Spam Legislation (CASL), is the federal law that addresses spam and other electronic threats. It established the rules for sending commercial electronic messages and the installation of computer programs. As defined in *CASL*, "spam" refers to unwanted or unsolicited commercial electronic messages received over the internet. As defined, a "commercial electronic message" is an electronically received message that encourages participation in a commercial activity, such as an email that contains a coupon or tells customers about a promotion or sale.

CASL aims to protect consumers and businesses from the misuse of digital technology, including spamming and other nonconsensual activities. It applies to all electronic messages sent by businesses and organizations in connection with a "commercial activity" — that is, electronic messages sent in hopes of encouraging engagement from the consumer, with the ultimate purpose being to make a profit. The key distinguishing feature of this legislation is the

requirement that Canadian (and global) organizations that send commercial electronic messages within, from, or to Canada must receive express consent from recipients prior to sending those messages.

This strategy goes much further than regulating the bulk, unsolicited email communications, which we know as spam. *Canada's Anti-Spam Legislation* creates an "express consent-based regime" that applies to almost all electronic messages which are sent for any commercial purpose. There are five full exemptions to the *CASL* requirements, a few specified categories of implied consent, and a partial exemption for third party referral messages.

The legislation has penalties for non-compliance with anti-spam provisions. When the *CASL* requirements are not followed, corporate directors, officers, and agents can be held liable for corporations, and corporations can be held liable for the actions of their employees. For corporations, fines can be up-to $100,000 for the first offence and $250,000 for repeat offences. For individuals, fines can be $10,000 for a first offence and $25,000 for subsequent offences. Penalties for violating the legislation can be as severe as $1 million for individuals and $10 million for businesses.

Regulating interpersonal relationships and criminal activities

Criminal law provisions in Canada are governed by federal legislation in the *Criminal Code of Canada* which outlines the relevant criminal offences, features required to make a criminal offence, the procedures, possible defences, and sentencing rules for the criminal courts. Civil courts are guided by tort law and presidential common law, rather than overarching federal legislation.

Criminal Code, RSC (1985) c C-46

The *Criminal Code of Canada* provides the Canadian criminal justice system with the applicable laws, offences, defences, procedures, and penalties for those who are charged and convicted

of a criminal offence. Malicious parties participating in cybercriminal activity can be divided into cyber-enabled crimes and cyber-supported crimes.

Cyber/computer-enabled activities with corresponding *Criminal Code* provisions include hacking, possession of "hacking tools," denial-of-service attacks, distributed denial of service attacks, botnets, malware, phishing, identity theft and identity fraud, and criminal copyright infringement.

Cyber/computer-supported activities can be thought of as traditional crimes which are committed through a cyber medium. For example, child trafficking is a criminal offence regardless of the medium over which the exchange is made or the forum used for the transaction. If a child trafficking offence is committed through the use of DarkNets, encrypted or anonymous networks, or otherwise supported by cyber technology, then the crime is a cyber-supported crime.

Protecting Canadians from Online Crime Act (SC 2014, c 31)

The *Protecting Canadians from Online Crime Act* came into force on March 10, 2015 and was intended to address the problem of cyberbullying after the high profile suicide deaths of Rehtaeh Parsons and Amanda Todd. This Act, among other things, amended the Criminal Code to create a new offence for the non-consensual distribution of intimate images. This is given under s. 162.1(1) where "everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or of an offence punishable on summary conviction.

The Common Law and Civil Tort Law

In January 2012, the case of *Jones v. Tsige (*2012 ONCA 32) became a landmark case in the Ontario Court of Appeal for recognizing the "new" privacy tort of "intrusion upon seclusion",

which allows victims of such privacy breaches to have the right to sue the privacy breacher in civil court for invasion of privacy. In this case, the Ontario Court of Appeal found that the Canadian common law was required to evolve in order to effectively respond to more modern privacy issues. This includes those which have arisen from technological changes and the constantly evolving need to reassess how personal information is collected, stored, protected, and made accessible in electronic form.

Jones v. Tsige involved a bank employee who accessed and reviewed another employee's personal bank accounts on 174 occasions over a four-year period. When the victim became aware of this, she sued the defendant. The victim claimed that by improperly accessing and reviewing her bank accounts the defendant committed the tort of invasion of privacy. In response, the defendant argued that Ontario does not recognize the invasion of privacy as a tort.

Following a thorough review of the case law and previous legal commentary related to the "invasion of privacy" tort, Ontario Court of Appeal Justice Sharpe concluded that "Ontario has already accepted the existence of a tort claim for appropriation of personality and, at the very least, remains open to the proposition that a tort action will lie for an intrusion upon seclusion."

The *Canadian Charter of Rights and Freedoms* protects the right to privacy under s. 8. Although the *Charter* cannot apply in a civil case, the Court considered the idea that the common law should evolve and develop consistently with *Charter* values to be most effective in our modern circumstances. Justice Sharpe noted that the existing case law establishes that personal privacy is worthy of constitutional protection and that it is integral to the relationship between individuals and the rest of society. He then combined this explicit *Charter* recognition with the idea that the common law should evolve and develop consistently with *Charter* values. In Justice Sharpe's view, there was already ample support to recognize a civil action for damages (aka: a lawsuit) for "intrusion upon seclusion" as a tort. He described it as follows:

"…the tort includes physical intrusions into private places as well as listening or looking, with or without mechanical aids, into the plaintiff's private affairs. Of particular relevance to this appeal, is the observation that other non-physical forms of investigation or examination into private concerns may be actionable. These include opening private and personal mail or examining a private bank account."

— ONCA Justice Sharpe

And just like that, the common law tort of "intrusion upon seclusion" was born.

This common law tort, in conjunction with the provisions given in the *Protecting Canadians from Online Crime Act*, the *Criminal Code of Canada*, *Canada's Anti-Spam Legislation (CASL),* the *Personal Information Protection and Electronic Documents Act (PIPEDA),* the *Access to Information Act,* and the *Privacy Act*, make up the majority of Canada's currently existing data privacy and cybersecurity-related federal legislation.

Cybersecurity laws in the United Kingdom

In the United Kingdom, as in Canada, there is no overarching comprehensive national cybersecurity law, although the European Union's *General Data Protection Regulation (GDPR),* in which the United Kingdom was a member party, came pretty close. For government, businesses, and other private-sector organizations, the UK's *General Data Protection Regulation* (UK-GDPR), the *Data Protection Act* (2018), and the *NIS Regulations* make up the bulk of the law relating to cybersecurity law and risk mitigation in the United Kingdom. For individuals and malicious parties, the UK's *Computer Misuse Act,* which was implemented back in 1990, continues to be a primary law at the forefront of interpersonal digital privacy, even 30 years later.

Regulating government, businesses, and organizations

Government, businesses, and organizations in the United Kingdom are subject to the *General Data Protection Regulation (GDPR),*

the *Data Protection Act 2018, and the NIS Regulations.* When the Brexit transition period concludes on December 31, 2020, the United Kingdom will have its own *UK General Data Protection Regulation (UK-GDPR)* which will work in conjunction with the current *Data Protection Act 2018.*

General Data Protection Regulations (GDPR) and Data Protection Act 2018

The collection, processing, use, and possession of personal data in the European Economic Area is governed by the *General Data Protection Regulation (GDPR)*. The *Data Protection Act 2018* is essentially the UK's implementation of the European Economic Area's *General Data Protection Regulation.* Both the *GDPR* and the *Data Protection Act* require that government, public entities, private-sector businesses, corporations, and organizations reduce the risk of personal data loss and privacy breaches by implementing strict security measures in an effort to safeguard all personal data collected, processed, used, or held by that entity.

These laws require that personal data must be securely kept and access to personal data is only permitted to third parties subject to sufficient guarantees regarding the security of the processing services.They also require the implementation of technical (e.g., firewalls, anti-virus programs, specific software, perimeter scanning tools) and organizational (e.g., policies and procedures regarding cybersecurity) protective measures to safeguard personal data and protect against unauthorized or unlawful access, use, loss, destruction and damage of any personal data. It is interesting to note that, according to these laws, enforcement action to address inadequate safeguards can be taken even in the absence of a reported cyber-attack or personal data breach.

Businesses which are subject to the *GDPR* and the *Data Protection Act* are required to implement appropriate
and proportionate measures to manage their risks. Failing to do so can result in enforcement action, including the imposition of significant fines of up to a maximum of the greater of £17.5 million or 4% of annual global turnover.

Network and Information Security Regulations 2018

The *Security of Network & Information Systems Regulations (NIS Regulations)* provide legal measures to boost the level of cybersecurity and physical resilience of network and information systems in the provision of essential, and digital, services. Whereas the *GDPR* is concerned with the security of personal data, the *NIS Regulations* are similarly concerned with the security of information systems.

The *NIS Regulations* establish a range of network and information security requirements and impose cybersecurity-related obligations which apply to operators of essential services and to digital service providers that offer services to individuals within the United Kingdom.

As with the obligations in the *GDPR* and *Data Protection Act 2018*, businesses subject to the obligations in the *NIS Regulations* have the freedom to determine which measures
are appropriate and proportionate to adequately manage the risks posed to network and information systems and to prevent or minimize the impact of incidents which could affect the security of the network and information systems.

The penalty for a business failing to meet the requirements of the *NIS Regulations* can result in enforcement action, including the imposition of significant fines. The *NIS Directive* allows member states to set their thresholds. In the UK, the maximum penalty is £17 million.

Regulating Interpersonal Relationships and Criminal Activities

Computer Misuse Act 1990

The UK's *Computer Misuse Act 1990* criminalizes individuals who attempt to access or modify data on a computer without authorization. This extends to include cyber-attacks, such as malware or ransomware attacks, which seek to disrupt services, obtain information illegally and/or extort individuals or businesses.

The *Computer Misuse Act 1990* was designed over 30 years ago with the intention of protecting telephone exchanges; when less than 0.5 per cent of the UK population used the internet and long before our current normalization of network reliance, digital communication, smartphones, and unlimited data plans.

The first offence in the *Computer Misuse Act* is achieving or attempting to achieve, access to a computer or the data it stores, by inducing a computer to perform any function with intent to secure access. The second and third offences are aggravated offences, requiring a specific intent to commit another offence and are intended to deter the more serious criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer.

The implications of this Act are that hackers who program their computers to search through password permutations could be liable under the first section, even if all of their attempts are rejected by the target computer. As well, using another person's login credentials without proper authority to access data or a program, or to alter, delete, copy or move a program or data, or to output a program or data to a screen or printer, or to impersonate that other person using email, online chat programs, web or other services, constitute the offence.

Although it has been amended two since its implementation, some groups in the UK have expressed concern that the *Computer Misuse Act* has been long superseded by technological progress and that it unintentionally inhibits the work of cyber-threat analysts, cybersecurity researchers, network security companies, and penetration testers, all of whom may be inadvertently caught by this Act. As the precondition to liability is that the hacker should be aware that the access attempted is unauthorized, then even if the initial access to a computer or data is authorized, a subsequent exploration (if there is a hierarchy of privileges in the system) may inadvertently lead to entry to parts of the system for which the required authorizations are lacking. Although unintentional, this would make out the commission of the offence.

Together, the UK's *Computer Misuse Act 1990*, the *NIS Regulations,* the *Data Protection Act* (2018), and the *General Data Protection Regulation (GDPR),* make up the bulk of the United Kingdom's cybersecurity and data privacy protection legislative scheme.

Cybersecurity laws in Australia

In Australia, the legislative powers are divided between the national government (called the Commonwealth) and the six States (New South Wales, Queensland, South Australia, Tasmania, Victoria and Western Australia) and three Territories (Australian Capital Territory, Northern Territory, and Norfolk Island) within the greater nation.

Regulating governmental, business, and organizational relationships

Within the Australian Commonwealth, cybersecurity laws for government and corporations are guided by the *Privacy Act 1988,* the *Privacy Amendment 2012,* and the *Privacy Regulation 2013.* The 13 *Australian Privacy Principles* included in the *Privacy Act* legislation are to be applied in guiding the development of privacy protocols in these organizations. The use of commercial electronic messages is regulated by the *Spam Act 2003*.

Privacy Act 1988 (Cth)

Australia's *Privacy Act 1988* is the foundational piece of Australian legislation that protects the handling of personal information, including the collection, use, storage and disclosure of personal information in the federal public sector and the private sector. The *Privacy Act* and the 13 Australian Privacy Principles apply to all organizations which carry out business in Australia which include actively collecting personal information

Other statutory provisions also affect privacy and separate privacy regimes apply to state and territory public sectors. This department assists the Attorney-General to administer the *Privacy Act*. The *Privacy Act* is supported by the *Privacy Amendment (Enhancing*

Privacy Protection) Act 2012, and the *Privacy Regulation 2013*.

The Notifiable Data Breaches scheme was implemented as part of the *Privacy Act* in February 2018. This scheme requires notification to all affected individuals and to the Office of the Australian Information Commissioner (OAIC) when a party who is subject to the *Privacy Act* experiences a data breach of personal information which poses a likely risk of serious harm to the affected individuals.

Australian Privacy Principles (APPs)

With the enacting of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* the *Privacy Act* outlines 13 *Australian Privacy Principles* (APPs) which apply to government agencies and to private sector organizations with an annual turnover of $3 million or more. The APPs are “principles-based” with the aim of protecting individual privacy while simultaneously not overburdening agencies and organizations with inflexible, and potentially expensive, prescriptivist rules.

The *Australian Privacy Principles* deal with all stages of the processing of personal information. They set out the standards for the collection, use, disclosure, quality and security of personal information, and they provide obligations concerning access to, and correction of, an individual’s own personal information for agencies and organizations which are subject to the *Privacy Act.*

This is overseen by the Office of the Australian Information Commissioner — the independent national regulator for privacy and freedom of information which promotes and upholds the right of individuals to access government-held information and have their personal information protected — within the Australian Government. The 13 *Australian Privacy Principles* are summarized on the OAIC website (www.oaic.gov.au) as:

Principle 1 — Open and transparent management of personal information

This ensures that APP entities manage personal information in an open and transparent way and includes having a clearly expressed and up to date APP privacy policy.

Principle 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Principle 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

Principle 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

Principle 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

Principle 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

Principle 7 — Direct marketing

An organization may only use or disclose personal information for direct marketing purposes if certain conditions are met.

Principle 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

Principle 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organization may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Principle 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

Principle 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorized access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

Principle 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

Principle 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

The OAIC is responsible for investigating breaches of the APPs and credit reporting provisions. The OAIC's has the power to accept enforceable undertakings, seek civil penalties in the case of serious or repeated breaches of privacy, and conduct assessments of privacy performances for both Australian Government agencies and businesses.

Australian Government Agencies Privacy Code 2017

The *Australian Government Agencies Privacy Code* was registered in October 2017 and went into effect on July 1, 2018. It applies to all Australian governmental agencies who are subject to the *Privacy Act 1988* (except for Ministers) and sets out the specific requirements and key practical steps that must be taken in order to comply with the *Australian Privacy Principles.*

In effect, the *Australian Government Agencies Privacy Code 2017* enhances existing privacy capability within agencies, builds greater transparency in information handling practices, and fosters a culture of respect for privacy and the value of personal information. It requires government agencies to move towards a “best practice” approach to privacy governance in order to help to create a consistent, high standard of personal information collection and management across all Australian government agencies.

Spam Act 2003 (Cth)

The *Spam Act 2003* was passed by the Australian Parliament in 2003 to regulate commercial e-mail and other types of commercial electronic messages. The *Act* restricts the prevalence of spam, particularly email spam and some types of phone spam, as well as the harvesting of email addresses.

Specifically, the *Spam Act 2003* provides that unsolicited commercial electronic messages must not be sent unless they are “designated commercial electronic messages”. As well, the messages must include information about the individual or organization who authorized the sending of the messages and must also contain a functional unsubscribe (or “opt-out”) option. In addition, address-harvesting software, or electronic address lists produced using address-harvesting software, must not be supplied, acquired or used.

The legal remedies given for breaches of the *Spam Act 2003* are predominantly civil penalties, punitive fines, and injunctions.

Regulating interpersonal relationships and criminal activities

Most of the criminal law provisions in Australia are created and administered by the six individual States (New South Wales, Queensland, South Australia, Tasmania, Victoria and Western Australia) and three Territories (Australian Capital Territory, Northern Territory, and Norfolk Island) of Australia. However, there is a body of criminal law, including the *Criminal Code Act 1995*, which is made and administered by the federal government.

Crimes Act 1914 (Cth)

Australia's historical equivalent to the *Criminal Code of Canada,* the *Crimes Act 1914* is one of the first recognizable compilations of federal criminal law since federation in 1901. The *Crimes Act 1914* deals with the most serious criminal offences against the Commonwealth. Historically, it was the most extensive legislative instrument addressing federal criminal offences, but is now being superseded with the passing of the *Criminal Code Act 1995 (Cth),* which is a compilation of all the federal offences in Australia.

Criminal Code Act 1995 (Cth)

Apart from the criminalization of specific activities, Australian law also presents a means to legally address wrongdoing in the civil law, which relates to non-criminal law including civil wrongs, contract law, property law and other areas that concern the rights and duties of individuals amongst themselves.

The Common Law and Civil Tort Law

As in Canadian civil tort law and, unless barred by an existing statute, individuals are entitled to sue other people, or the state, for the purpose of obtaining a civil legal remedy for a legally-recognized "tort" or wrongdoing. However, to sue someone in tort law, requires the pre-existence or creation of an applicable tort, through the common law, case law, or challenge in a court. At the time of writing, there is currently no federal or state legislation articulating a specific cause of action for breach of privacy in Australia law.

Although privacy protections exist in the *Privacy Act 1988* (Cth), those provisions do not apply to individuals who are not operating a business, businesses with an annual turnover of less than $3 million, media organizations, members of a parliament, contractors for political representatives, and individual volunteers for registered political parties. In 2014, the Australian Law Reform Commission formally recommended the creation of a tort for "serious invasions of privacy" to the federal government in their report on Serious Invasions of Privacy in the Digital Era.

Although there is no established common law tort to pursue civil causes of action in Australia, the *Criminal Code Act 1995 (Cth),* in conjunction with the provisions given in the *Spam Act 2003*, the *Australian Government Agencies Privacy Code 2017*, *Privacy Act 1988,* including the *Privacy Amendment 2012,* and the *Privacy Regulation 2013,* make up the majority of Australia's currently existing data privacy and cybersecurity-related federal legislation.

Cybersecurity laws in the United States

As we have seen in Canada, in the United Kingdom, and in Australia, there is no singular federal law or federal cybersecurity regulation that governs data privacy in the United States. Rather, there are few sector-specific federal cybersecurity regulations that focus on specific industries, including healthcare, financial institutions, and commercial marketing.

The *Privacy Act of 1974* continues to be the foundational legislation governing federal government use of personal information, however, this does not apply to businesses or organizations outside of government. The three main sector-specific cybersecurity regulations are: the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, the *Gramm–Leach–Bliley Act of 1999*, and the *Homeland Security Act of 2002*

which included the *Federal Information Security Management Act* (FISMA).

In essence, these regulations mandate the need for healthcare organizations, financial institutions and federal agencies to enact and enforce policies to protect their systems, ensure data privacy, and comply with all relevant privacy legislation with regard to the access to and collection, processing, use, and disclosure of personal or private information.

Regulating the federal government and governmental agencies

Privacy Act of 1974

The purpose of the *Privacy Act* is to balance the federal government's need to maintain information about individuals with the rights of those individuals to be protected against unwarranted invasions of their privacy arising from the collection, maintenance, use, and disclosure of personal information by a federal agency.

Only United States citizens and aliens admitted for permanent legal residence are permitted to obtain records under this statute. The *Privacy Act* does not apply to state or local governments unless such entities are involved in a computer matching program with the federal government, or to private companies or organizations unless these entities are under contract with the agency to maintain an agency-approved *Privacy Act* system of records.

Federal Information Security Management Act

The *Federal Information Security Management Act* (FISMA) applies to all agencies within the United States federal government. This has served to bring greater attention and awareness cybersecurity issues within the federal government while explicitly emphasized a "risk-based policy for cost-effective security". Since the law was originally enacted in 2002, the federal government expanded the *Federal Information Security Management Act* to include state agencies that administer federal programs, including Medicare/Medicaid, unemployment insurance, and student loans.

The *FISMA* requires each federal agency to create, distribute, and enact an agency-wide program to provide information security for the information and information systems that work to support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Regulating sector-specific industries: healthcare

Ensuring patient and maintaining doctor-patient confidentiality can promote more effective communication between physician and patient in an effort to enhance quality of individualized health care and treatment, to improve patient autonomy, and with the goal of preventing economic harm or embarrassment to the patient.

Health Insurance Portability and Accountability Act of 1996

The *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* is a US federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services issued the **Privacy Rule** and the **Security Rule** to implement the requirements of the *HIPAA*.

The **Privacy Rule** standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.

The **Security Rule** protects a subset of information covered by the **Privacy Rule**.

Regulating sector-specific industries: Banking and financial institutions

Financial institutions are among the most heavily regulated entities, at both the federal and state levels, and similarly are required to protect customer personal information against reasonably foreseeable threats to security.

Gramm–Leach–Bliley Act / Financial Services Modernization Act of 1999

The *Gramm–Leach–Bliley Act (GLBA)*, also known as the *Financial Services Modernization Act of 1999,* requires a wide range of financial institutions to adequately explain their information-sharing

practices to their customers and to safeguard sensitive personal data. Compliance with the *GLBA* is mandatory; there must be an adequate policy in place to protect the information from foreseeable threats in cybersecurity and integrity of data protection measures regardless of whether or not a financial institution discloses personal or private information.

The three major components overlaying the collection, disclosure, and protection of consumers' personal information in the *GLBA* include: the **Financial Privacy Rule**, the **Safeguards Rule**, and **Protection from Pretexting**.

The **Financial Privacy Rule** requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is initially established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how it is used, and how it is protected. The notice must identify the consumer's right to opt out of the information being shared with unaffiliated parties pursuant to the provisions set out in the *Fair Credit Reporting Act*.

The **Safeguards Rule** requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. The aim of the Safeguards Rule is to force financial institutions to reexamine their relationship with personal private data and to perform a thorough risk analysis on their current safeguard processes.

Protection from Pretexting is to protect against personal data breaches which occur through impersonation. This is, when someone tries to gain access to personal information without the proper authority to do so. This is related to identity theft and identity fraud. Pretexting includes requesting private information while impersonating the account holder either, by phone, by postal mail, by email, or by phishing. The *GLBA* encourages organizations to implement adequate safeguards against pretexting, such as the implementation of multi-factor authentication.

Regulating interpersonal relationships and criminal activities

Computer Fraud and Abuse Act (1986)

The *Computer Fraud and Abuse Act* is both a criminal law and a civil statute that creates a private (tort) right of action, allowing compensation and injunctive or other equitable relief to anyone harmed by a violation of this law. The *National Information Infrastructure Protection Act of 1996* later amended the C*omputer Fraud and Abuse Act,* modifying several sections and increasing the penalties for specific crimes.

The Common Law and Civil Tort Law

The United States has a few torts which developed out of the "invasion of privacy" cause of action in tort law. These include:

Public Disclosure of Private Facts

The dissemination of truthful private information which a reasonable person would find objectionable.

False Light

The publication of facts which place a person in a false light, even though the facts themselves may not be defamatory.

Appropriation

The unauthorized use of a person's name or likeness to obtain some benefits.

Intrusion of Solitude / Intrusion Upon Seclusion

The intentional intrusion, physically, electronically, or otherwise, upon the private space, solitude, or seclusion of a person, or the private affairs or concerns of a person.

The civil law in the United States recognizes invasion of privacy torts as **civil** wrongs and allows injured parties to recover for their losses by bringing a cause of action (suing) the other party to recover damages, such as financial compensation or an injunction to legally compel the other party to immediately cease an activity.

Together, the United States' *Computer Fraud and Abuse Act of 1986*, the *Gramm–Leach–Bliley Act (GLBA)* — aka the *Financial Services Modernization Act of 1999* — the *Health Insurance Portability and Accountability Act of 1996*, the *Federal Information Security Management Act,* and the *Privacy Act of 1974* make up the bulk of the United States' cybersecurity and data privacy protection legislative scheme.

Summary Tables

Type of Cybercrime	Canada	United Kingdom	Australia	United St
Applicable National Cybersecurity and Data Privacy Laws	*Canadian Charter of Rights and Freedoms* (1982) *Criminal Code of Canada* (1985) *Privacy Act* (1985) *Copyright Act* (1985) *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000) *Canada's*	*Criminal Law Act* (1967)*Theft Act* (1968) *Copyright, Designs and Patents Act* (1988) *Computer Misuse Act* (1990) *Communications Act* (2003) *Privacy and Electronic Communications Regulations* (PECR) (2003) *Fraud Act*	*Crimes Act* (1914) *Copyright Act* (1968) *Privacy Act* (1988) *Criminal Code Act* (1995) *Telecommunications Act* (1997) *Spam Act* (2003) *Cybercrime Legislation Amendment Act* (2012) *Privacy Amendment (Enhancing Privacy*	*Privacy A 1974Copy Act of 197 Electronic* *Communi* *Privacy A 1986* (EC *Computer and Abus of 1986* (CFAA) *Identity Th and Assu* *Deterrenc of 1998* *Gramm–L Bliley Act* (GLBA) a.k.a. *Financial Services*

	Anti-Spam Legislation (CASL) (2014) *Protecting Canadians from Online Crime Act* (2014)	(2006) *General Data Protection Regulation* (GDPR) (2018) *Data Protection Act* (2018) *NIS Regulations* (2018)	*Protection) Act* (2012) *Australian Government Agencies Privacy Code* (2017) *Security of Critical Infrastructure Act* (2018)	*Moderniz Act of 19* *Federal Informatic Security Managem Act of* 20((FISMA) *Controllin Assault of Non-Solic Pornogra And Mark Act* (CAN-SP (2003)
Hacking and/or Unauthorized Access	*Criminal Code of Canada* (1985) s. 184 s. 342.1 s. 380(1) s. 430	*Computer Misuse Act* (1990) *Terrorism Act* (2000)	*Criminal Code Act* (1995) s. 478.1	*Computer and Abus of 1986*ss *Electronic Communi Privacy A 1986* *Stored Communi Act of 19* s. 2702

DOS and DDOS Attacks	*Criminal Code of Canada*(1985) s. 430(1.1)	*Computer Misuse Act* (1990)	*Criminal Code Act* (1995) s. 477.3	*Computer and Abus of 1986* (C s. 1030(a)
Phishing	*Criminal Code of Canada* (1985) s. 380(1)	*Computer Misuse Act* (1990) *Fraud Act* (2006)	*Criminal Code Act* (1995)s. 134.2(1) s. 135.1(1) s. 135.1(3) s. 135.1(5)	*Computer and Abus of 1986* (CFAA) s.1030(a) s. 2702
Modification or Impairment of Data	*Criminal Code of Canada*(1985) s. 380(1)	*Computer Misuse Act* (1990)	*Criminal Code Act* (1995) s. 478.1 s. 478.2	*Computer and Abus of 1986* (C s.1030(a)
Interception of Data and/or Electronic Theft	*Criminal Code of Canada* (1985) s. 342.1	*Theft Act* (1968) *Computer Misuse Act* (1990) *Terrorism Act* (2000) *Fraud Act* (2006)	*Criminal Code Act* (1995) s. 478.1	*Computer and Abus of 1986* (C s.1030(a) *Electronic Communi Privacy A 1986* (EC *Stored Communi Act of 198* s. 2702
Identity Theft or Fraud	*Criminal Code of Canada* (1985) s. 402.2	*Computer Misuse Act*(1990) *Fraud Act*	*Criminal Code Act* (1995) s. 372.1(a)	*Identity Th and Assumpti Deterrenc*

	s. 403	(2006)		*of 1998*
Copyright Infringement	*Copyright Act*(1985) s. 41.1(1)	*Copyright, Designs and Patents Act* (1988)	*Copyright Act* (1968)	*Copyright 1976*
Spam	*Canada's Anti-Spam Legislation* (CASL) (2014)	*Privacy and Electronic Communications Regulations* (PECR) (2003)	*Spam Act* (2003)	*Controllin the Assau Non-Solic Pornograp And Mark Act* (CAN-SP/ (2003)

Applicable national laws related to cybersecurity

Which Law Applies to Which Parties in Which Country?	**Canada**	**United Kingdom**	**Australia**	**United Stat**
Federal/National Government	*Canadian Charter of Rights and Freedoms* (1982) *Privacy Act* (1985)	*GeneralData Protection Regulation* (GDPR) (2018) *Data Protection Act* (2018) *NIS Regulations* (2018)	*Privacy Act*(1988) *Privacy Amendment (Enhancing Privacy Protection) Act* (2012) *Australian Government Agencies Privacy*	*Privacy Act 1974Federa Information Security Managemer Act* (FISMA) (2002)

			Code (2017)	
Private-Sector: All Corporations, Businesses, and Non-Governmental Organizations	*CanadianCharter of Rights and Freedoms* (1982) *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000)	*General Data Protection Regulation* (GDPR) (2018) *Data Protection Act* (2018) *NIS Regulations* (2018)	*Privacy Act*(1988) *Privacy Amendment (Enhancing Privacy Protection) Act* (2012) *Australian Government Agencies Privacy Code* (2017)	Based on state-specifi legislation, rather than f federal legislation.
Private-Sector: Health Care Specific	*CanadianCharter of Rights and Freedoms* (1982) *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000) Canadian health care privacy legislation is	*GeneralData Protection Regulation* (GDPR) (2018) *Data Protection Act* (2018)	*Privacy Act* (1988) *Privacy Amendment (Enhancing Privacy Protection) Act* (2012)	*Health Insurance Portability a Accountabil Act of 1996* (HIPAA)

	comprised of 14 government jurisdictions each with its own legislative framework for protecting the privacy of personal health information.			
Private-Sector: Banking and Financial Services Specific	*CanadianCharter of Rights and Freedoms* (1982) *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000)	*GeneralData Protection Regulation* (GDPR) (2018) *Data Protection Act* (2018)	*Privacy Act* (1988) *Privacy Amendment (Enhancing Privacy Protection) Act* (2012)	*Gramm–LeachBliley* (GLBA) aka *Financial Services Modernizati Act of 1999*
Commercial Electronic Messages (CEMs)	*Canada's Anti-Spam Legislation* (CASL) (2014)	*Privacy and Electronic Communications Regulations* (PECR) (2003) *General Data Protection Regulation*	*Spam Act* (2003)	*Controlling the Assault Non-Solicite Pornograph And Marketi Act* (CAN-SPAM (2003)

		(GDPR) (2018) *Data Protection Act* (2018)		

Individuals	*Criminal Code of Canada*(1985) *Copyright Act* (1985) *Protecting Canadians from Online Crime Act* (2014)	*Criminal Law Act* (1967) *Copyright, Designs and Patents Act* (1988) *Computer Misuse Act* (1990) *Theft Act* (1990) *Terrorism Act* (2000) *Fraud Act* (2006)	*Copyright Act* (1968) *Criminal Code Act* (1995)	*Copyright A 1976Compu* *Fraud and Abuse Act c 1986* (CFAA) *Electronic Communica* *Privacy Act 1986* (ECPA *Identity The and Assumption* *Deterrence of 1998* *Title 18 of th* *United State Code* Note: Indivic states have own Penal, Criminal or Crimes Cod legislation dependent c jurisdiction.

Table 2: Which law applies where and to whom?

Conclusion

In considering the cybersecurity laws of four countries: Canada, the United Kingdom, Australia, and the United States, it is evident that

they have each taken different approaches to legislate, and regulate, data privacy and cybersecurity-related concerns within their respective borders. While all four are considered to be "common law" countries, their unique national needs, historical interests, and constitutional values have contributed to the individualized evolution of their statutory law.

Statutory laws often evolve in parallel with (or in response to) social and/or technological change. With the rapid technological advancements that have inundated our nations over the past few decades — indeed since the age of industrialization — the national statutory laws have had to adjust and accommodate to remain applicable to the changing society in which we live. This exceptional period of technological growth, and our increased reliance on digital communications, has culminated in the need for each of these nations to re-evaluate their current national data privacy and cybersecurity-related statutory schemes to adequately protect the interests of the nation and the people who live and work within it.

At the time of writing, all four of these nations have, individually and collectively, been engaged in consultation processes to address their statutory provisions relating to cybersecurity, data privacy, and cybercriminal activities. Indeed, these four international allies (and New Zealand) have been collaborating, through their respective cybersecurity research centres, to create new and improved global cybersecurity standards and report on possible strategies for approaching potentially malicious cybersecurity threats. As we enter into 2021, we can anticipate (with great certainty) that the applicable data privacy, cybersecurity, and cybercriminal provisions in these countries will continue to develop, evolve, and expand over the next decade.

In the next article in our Understanding Canadian Cybersecurity Laws series (Article 9), we will discuss the implications of the newly proposed *Digital Charter*, which aims to keep pace with modern society while also continuing to provide the programs and services that enrich the lives of many Canadians.

Would you recommend this article?

Thanks for taking the time to let us know what you think of this article!

We'd love to hear your opinion about this or any other story you read in our publication. **Click this link to send me a note →**

Jim Love, Chief Content Officer, IT World Canada

Related Download

Sponsor: **CanadianCIO**

Cybersecurity Conversations with your Board – A Survival Guide

A SURVIVAL GUIDE BY CLAUDIO SILVESTRI, VICE-PRESIDENT AND CIO, NAV CANADA

Download Now