itworldcanada.com

Understanding Canadian cybersecurity laws: Interpersonal privacy and cybercrime — Criminal Code of Canada (Article 4)

Melissa Lukings and Arash Habibi Lashkari

20-26 minutes

Introduction

The global spread of COVID-19 has been a huge catalyst in our increased reliance on digital technologies, particularly our networked communication infrastructure. With the rapid influx of demand for online communication programs, existing online criminal activities have just as quickly transformed. The criminal exploitation of new and emerging technologies, like social media and cloud computing, requires new legislative measures to keep pace with our digital era. As criminals continue to exploit new information technologies, their corresponding cybercriminal threats are becoming more sophisticated, more complex, and more prevalent. While governmental institutions, private companies, and organizations are bound by the *Privacy Act* and *PIPEDA*, individual malicious actors are not governed by the same set of laws. For malicious parties participating in cybercriminal activity, the *Criminal Code of Canada* provides the Canadian criminal

justice system with the applicable laws and penalties.

We have previously outlined the provisions in the *Privacy Act* and the *Access to Information Act* which regulate federal government institutional access to, use of, and disclosure of personal information. We have also examined the laws regulating private sector access to, use of, and disclosure of personal information, which apply to both federally-regulated and private sector commercial organizations, and were established in the *Personal Information Protection and Electronic Documents Act*.

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)

In this article, we will venture into the realm of Canadian cybersecurity laws as they relate to interpersonal privacy, data breaches, network attacks, and other computer-related activities of a criminally malicious nature.

***Criminal Code of Canada* (RSC 1985, c C-46)**

With the implementation of the *Constitution Act, 1867,* it was established that criminal law is to be under the exclusive legislative jurisdiction of the federal Parliament of Canada. This means that all criminal laws in Canada are created by federal bodies and apply across all provinces and territories. The first *Criminal Code,*

1892 went into force on July 1, 1893 and was sponsored by the then Attorney General of Canada, Sir John Thompson. Along with the *Criminal Code* being a source of Canadian law, criminal law in Canada at the time also included the common law of each province and any remaining imperial criminal statutes which had not already been superseded by existing Canadian legislation. The *Criminal Code of Canada* (RSC 1985, c C-46) sets out and codifies most of the criminal offences, procedures, and some of the defences which are available to the defendant in Canadian criminal law. Additional criminal law provisions have since been given in the *Controlled Drugs and Substances Act*, in the *Youth Criminal Justice Act*, and in a few others.

The *Criminal Code* provides for three different types of criminal offences: (1) summary conviction offences; (2) indictable offences; and (3) hybrid offences.

Summary conviction offences are the less serious of the criminal offences in Canada. These crimes generally carry a maximum sentence of up to a $5000 fine or between 6 months' imprisonment, however, there are some exceptions. Pure summary conviction crimes include activities like trespassing at night, solicitation, and causing a disturbance.

Indictable offences are the most serious types of criminal offences, including murder, drug trafficking, robbery, some types of sexual assault, treason, and terrorism. These crimes are typically more complicated and are likely to result in very serious consequences, including maximum sentences of up to imprisonment for life.

Hybrid offences are those which can proceed either by summary

conviction or by indictment, at the Crown's discretion. The majority of *Criminal Code of Canada* offences fit under this category. Examples of hybrid offences include assault, assault with a weapon and/or causing bodily harm, sexual assault, drug possession, theft and fraud under $5000, etc. Most of the cyber-related crimes would fall under this category of offence.

Defining 'cybercrime'

There are four categories for activities that can fall under the label of "cybercrime": (1) cyber-dependent crimes; (2) cyber-enabled crimes; (3) computer-supported crimes; and (4) national security offences.

Cyber-dependent crimes are those which can only be committed using a computer, a computer network, or other technology. Examples of cyber-dependent crimes include hacking, DoS and DDoS attacks, criminal botnet operations and malware. These are examples of "true cybercrime" in that they would not exist at all without a the use of a computer and the target itself is typically one or more computers or the networks between them. The RCMP distinguishes these types of crimes as "technology-as-target" cybercrime offences.

Cyber-enabled crimes are crimes which can be committed without the use of technology, but which are increased in their scale or reach by the use of computers, computer networks, and other technology. Cyber-enabled crimes can include activities like cyber-stalking, fraud, extortion, child pornography, various trafficking offences, and cybercriminal-for-hire services. The RCMP has identified these types of crimes as "technology-as-

instrument" cybercrime offences.

Computer-supported crimes are those in which the use of the computer or network is only incidental to the actual commission of the crime, but which may be legally relevant for evidentiary purposes. As an example, data recorded on a computer or through a computer network could be an integral part of an investigation for murder, which would make that murder a "computer-supported" crime.

National security offences ("cyberterrorism") and civil violations involving computers, computer networks, and other technologies will be addressed in future articles within this series. For our purposes, we will focus on **cyber-dependent** and **cyber-enabled** crimes. It is important to note that these two categories are not mutually exclusive, as some types of crimes may fit into multiple categories.

Common specific cybercrime Offences

The field of cybercrime is large and encompasses a wide variety of *Criminal Code* offences. The main themes we see throughout the offences which are specific to cybersecurity are those which relate to fraud, theft, interception, and mischief. We can examine how the law deals with some of the more common cyber-specific offences by looking at the law in relation to: hacking, DoS attacks, malware, phishing, identity theft and fraud, and criminal copyright infringement.

Hacking is a broad term that refers to someone exploiting a computer system or private network through a computer to gain access to digital files or systems without permission. Hackers use

brute force, security exploits, social engineering, and other means to gain access to systems without proper authorization. In law, hacking refers to the unauthorized access to, control of, and/or wilful interception of, personal information, private communication, and other private data over computer network systems for some illicit purpose. Variations of offences which could relate to hacking involve themes of interception, fraud, and mischief with maximum sentences ranging from 5 to 14 years of imprisonment.

Possession of "Hacking Tools" which are designed or adapted primarily to commit either computer/network "hacking" (under s. 342.1) or computer/network "mischief" (under s. 430) and knowing that the device has been used or is intended to be used for those purposes is an offence. This also includes making, selling, importing, distributing, or making available such a device. An offence of this nature can lead to a sentence of up to 2 years in prison.

Denial-of-Service (DoS) Attacks occur when a (likely nefarious) individual either temporarily or indefinitely disrupts services of a host connected to the internet, which makes the legitimate users unable to access information systems, devices, and other network resources. In a DoS attack, the attacker typically uses one computer and one internet connection to flood the target. These types of attacks can result in a prison sentence of up to 10 years for mischief.

Distributed Denial of Service (DDoS) Attacks are similar to a DoS attacks, but much larger. The difference between DoS and DDoS attacks is that whereas DoS typically involves one computer, a DDoS attack uses multiple computers and multiple internet connections to disrupt network traffic. DDoS attacks can

result in devastating consequences for the target, including unauthorized data access, email spamming, data theft, and massive data leaks. These types of attacks can be incredibly large-scale, global attacks when they are distributed through botnets.

Botnet is a portmanteau formed by shortening the combination of “robot” and “network”. In this topic, botnets are groups of connected computers or devices that perform a number of repetitive tasks. When a botnet is infected by malicious code, the network becomes under the control of the attacking party.

Malware, or “malicious software” is a general term (and portmanteau) that can refer to adware, ransomware, spyware, trojans, viruses, worms, and other types of harmful software. The differentiating factor between malware and software is that malware must be intentionally malicious. This distinguishes malware from software that unintentionally causes harm, but is not created or intended to be used for malicious purposes. Like DoS and DDoS attacks, malware is considered to be a form of mischief and can result in sentences of up to 10 years in prison.

Phishing is a type of cybercrime in which a target (or targets) are contacted by email, telephone or text message by someone posing as a legitimate institution to lure those individuals into providing private data such as personally identifiable information, banking and credit card details, and passwords. This type of fraud is covered under s. 380(1) of the Criminal Code as “defrauding the public or any person of property, money, valuable security or a service” and can be penalized with up to 14 years of imprisonment.

Identity Theft and **Identity Fraud** tend to go hand-in-hand. Identity theft is covered in the *Criminal Code* under s. 402.2 as "obtaining or possessing another person's identity information with the intent to use it to commit an indictable offence". Identity fraud involves fraudulently impersonating someone "with the intent of gaining an advantage, obtaining property, causing disadvantage to another, or to avoid arrest or prosecution". This can include pretending to be another person or using that other person's identity, personal information, signature, legal name, user name, password, etc. to intentionally accomplish a goal which is an indictable offence, like fraud. Identity theft and identity fraud can be penalized with up to 5 and 10 years of imprisonment respectively.

Criminal Copyright Infringement is a type of electronic theft that involves circumventing a technological protection measure. This particular offence is covered under s. 41.1(1) of the *Copyright Act* rather than the *Criminal Code*. Charges of criminal copyright infringement have the potential for fines of up to $1 million, imprisonment for up to 5 years, or a combination of both.

For a more complete breakdown of the cyber-specific criminal offences, please see the table below, called Cybercriminal Laws in Canada.

Cybercriminal Laws in Canada			
Type of Cybercrime	***Criminal Code* Provision(s)**	**Criminal Offence**	**Maximum Sentence**
Hacking	s. 184 s. 342.1	Wilful interception, use, or retention	Up to 5 years' imprisonment

	s. 380(1) s. 430	of private communications. Fraudulently obtaining any computer service or intercepting any function of a computer system. *(This includes the use of a computer system with intent to commit such an offence and use or possession of a computer password to enable such an offence.)* Defrauding the public or any person of property, money, valuable security or a service. Mischief,	Up to 10 years' imprisonment Up to 14 years' imprisonment Up to 10 years' imprisonment

		including: wilfully destroying or damaging property; rendering property useless, inoperative or ineffective; and obstructing, interrupting, or interfering with the lawful use, enjoyment or operation of property. *(i.e. "smurfing" or causing chaos by overloading computer systems)*	
Denial-of-Service Attacks	s. 430(1.1)	Mischief, including obstructing, interrupting or interfering with the lawful use of	Up to 10 years' imprisonment

		computer data and denying access to computer data to a person who is entitled to such access.	
Malware	s. 430 s. 430(1.1)	Mischief, including: wilfully destroying or damaging property; rendering property useless, inoperative or ineffective; and obstructing, interrupting, or interfering with the lawful use, enjoyment or operation of property. Mischief, including: wilfully destroying, damaging, or altering	Up to 10 years' imprisonment Up to 10 years' imprisonment

		computer data; rendering computer data meaningless, useless or ineffective; obstructing, interrupting or interfering with the lawful use of computer data; and denying access to computer data to a person who is entitled to access it.	
Possession of "Hacking Tools"	s. 342.2	Making, possessing, selling, offering for sale, importing, obtaining for use, distributing, or making available a device that is designed or adapted	Up to 2 years' imprisonment

		primarily to commit either “hacking” (s. 342.1) or “mischief” (s. 430), knowing that the device has been used or is intended to be used to commit such an offence.	
Phishing	s. 380(1)	Defrauding the public or any person of property, money, valuable security or a service.	Up to 14 years’ imprisonment
Identity Theft or Fraud	s. 402.2 s. 403	Obtaining or possessing another person’s identity information with the intent to use it to commit an indictable offence, such as fraud. Fraudulently	Up to 5 years’ imprisonment Up to 10 years’ imprisonment

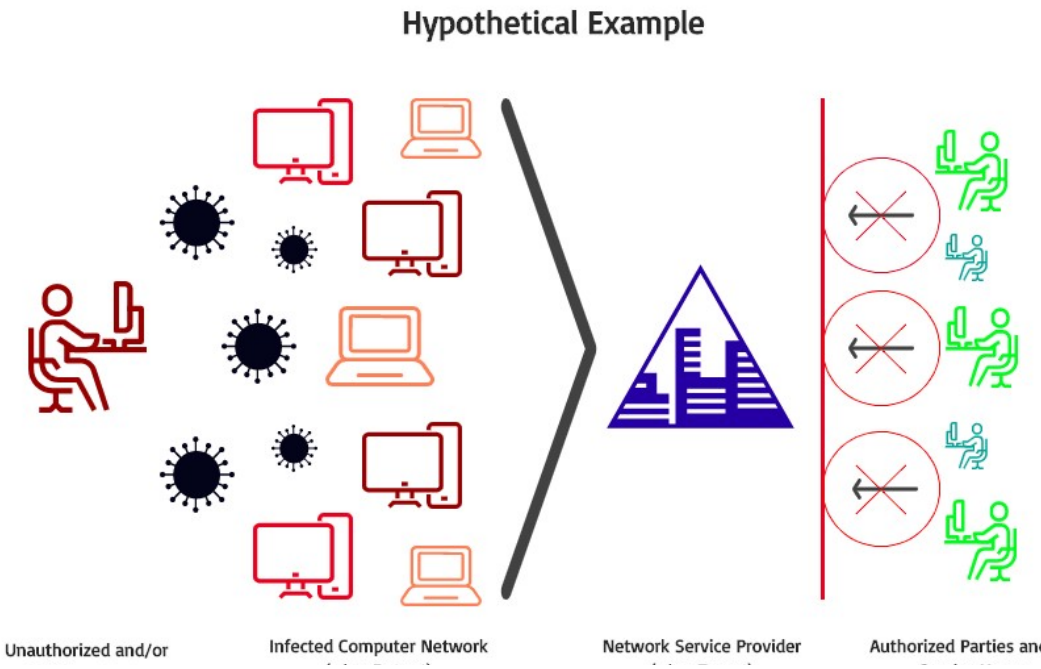
		personating someone with the intent of gaining an advantage, obtaining property, causing disadvantage to another or to avoid arrest or prosecution. *(This can include pretending to be the person or using the person's identity, information, signature, legal name, user name, password, etc.)*	
Electronic Theft (i.e. criminal copyright infringement)	This is covered under s. 41.1(1) of the	Circumventing a technological protection measure, including any	Potential for fines of up to $1 million, imprisonment for up to 5

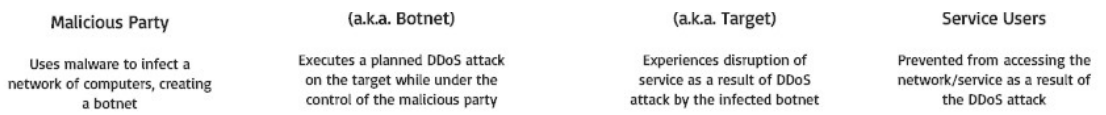
	Copyright Act, RSC 1985, c C-42.	technology, device or component that controls access to a work or sound recording or restricts violations of certain copyright provisions.	years, or a combination of both.
National Security Offences ("Cyberterrorism")	s. 83.2	Committing an indictable offence for the benefit of, at the direction of, or in association with an organization that commits a terrorist activity. *(This includes an act or omission that intentionally causes serious interference with or disruption of an essential service, facility or system.)*	Imprisonment for life

Hypothetical application

Person “A” has taken to a life of cybercrime. “A” has decided, for whatever reason, to wreak havoc on a network service provider (the target). “A” does this using a combination of malware, botnets, and DDoS attacks.

In our case, Person “A” is an unauthorized party, acting maliciously, who intentionally infects a network of computers with malware. This malware infection creates a “botnet” (robot network). The infected network (botnet) of computers, now under the control of “A” (the unauthorized party) works in tandem to execute planned DDoS (distributed denial-of-service) attacks on the targeted network. The target experiences a disruption to their network traffic and services as a result of the heavy influx of requests from the botnet. This disruption of service prevents the authorized parties from having access to the network, further disrupting the traffic and potentially resulting in devastating consequences, including unauthorized data access, widespread email spamming, data theft, and massive organizational leaks.





In this hypothetical example, Person “A” could be charged under the following *Criminal Code* provisions:

1. Mischief under s. 430 and s. 430(1.1) for the malware and DDoS attacks. This carries a maximum penalty of 10 years in prison.
2. If the crime is considered to be a national security offence, then “A” could be charged under s. 83.2 for cyberterrorism and face a maximum penalty of life in prison.
3. If private communications were intercepted, then “A” could be charged under s. 184 for interception and be at risk of facing up to 5 years in prison.
4. If “A” continues to possess the tools used to do the hacking, malware, and DDoS attacks, then “A” could be charged with possession of tools and receive a penalty of up to 2 years of prison time.
5. If electronic theft involving criminal copyright infringement occurs, then Person “A” could also be charged under Section 41.1(1) of the *Copyright Act* and be fined substantially.

What we can see from this hypothetical example of a malware/DDoS attack, is that criminal charges involving cyber-specific criminal activities can very quickly escalate and these charges can rack up some very serious consequences.

Large-scale, collaborative, and organized cybercriminal activity

Darknets are online file-sharing networks that provide users with

anonymity through encryption and other cybersecurity technologies. They enable criminals to broker their illegal goods and services on the Internet and avoid detection through anonymous online networks. These networks attract criminal activity by concealing online transactions, such as the online buying and selling of illegal drugs, pirated media,g counterfeit goods and other illicit products.

Through darknets and other anonymous online forums, criminals can easily purchase cybercrime tools, services and supporting infrastructure. This service-based online market enables more criminals to take part in technologically advanced cybercrime activities, such as DDoS attacks or malware distribution through botnets. The online availability of such tools and services means that more criminals can outsource their cybercrime operations in part or in whole.

Virtual currency schemes, such as Bitcoin, can also be used by criminals to launder their proceeds online. These types of currency schemes provide organized criminal networks with new ways to hide their earnings. The criminal use of virtual currencies is quite often associated with darknets, in which virtual currencies and anonymous online networks are used to obtain payments for illegal goods and services and launder revenue associated with criminal transactions

Growing prevalence of cybercrime

Where the Internet and its related technologies have been fundamental in reshaping Canada’s society and economy, they have also changed Canada’s criminal landscape fundamentally.

Online marketplaces, anonymous forums, and Internet-connected devices provide the same opportunities and benefits for serious and organized criminal networks as they do for legitimate businesses. Through new and evolving information technologies, criminals are expanding their reach to commit entirely new crimes and old crimes in new and creative ways.

The vast popularity and ever-increasing interconnectedness of our mobile devices have made them an especially attractive target for criminal exploitation, with malware increasingly being developed to target vulnerabilities found within our mobile operating systems. Mobile device features, including text messaging and downloadable applications, can be used to deploy malware and gain unauthorized remote access to those same mobile platforms. This can be done for a variety of illicit purposes including, but not at all limited to: interception or theft of personal data; obtaining GPS coordinates; cyber-surveillance; revenge porn; and cyberstalking.

Conclusion

Widespread months-long lockdowns of cities around the world during the COVID-19 pandemic have shown that we are more dependent on our ties with technology than ever before. With this reliance must come an increase in legal protective measures to prevent malicious actors from causing widespread harm to individuals, businesses, organizations, and governments.

Widely available, ready-made malware and other hacking tools provide both professional and amateur criminals with new and simplified ways to steal information and financially impact

Canadian businesses and citizens. Criminal activities in cyberspace are complex and often transnational, where potential evidence can be transient or spread across multiple legal jurisdictions. As so much of our daily lives moves online, such online criminal activity should be a growing concern for everyone. Addressing these challenges requires both domestic and international cooperation and legislative engagement with public and private sector organizations.

In our next article, we will discuss the implementation of Canada's Anti-Spam Law (CASL) and its application to the field of Canadian cybersecurity law.

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