Vulnerable Connections

Expert Panel on Public Safety in the Digital Age

CCA | CAC

Vulnerable Connections

Expert Panel on Public Safety in the Digital Age

CCA | CAC

THE COUNCIL OF CANADIAN ACADEMIES
180 Elgin Street, Suite 1401, Ottawa, ON, Canada, K2P 2K3

The project that is the subject of this report was undertaken with the approval of the Board of Directors of the Council of Canadian Academies (CCA). Board members are drawn from the Royal Society of Canada (RSC), the Canadian Academy of Engineering (CAE), and the Canadian Academy of Health Sciences (CAHS), as well as from the general public. The members of the expert panel responsible for the report were selected by the CCA for their special competencies and with regard for appropriate balance.

This report responds to a request from Public Safety Canada (PS) for an independent assessment. PS had no involvement in either panel selection or report development; any opinions, findings, or conclusions expressed in this publication are those of the authors, the Expert Panel on Public Safety in the Digital Age, and do not necessarily represent the views of their organizations of affiliation or employment.

Library and Archives Canada

ISBN: 978-1-990592-22-5 (book)
978-1-990592-23-2 (electronic book)

This report should be cited as:

CCA (Council of Canadian Academies). (2023). *Vulnerable Connections*. Ottawa (ON): Expert Panel on Public Safety in the Digital Age, CCA.

Disclaimer

The internet data and information referenced in this report were correct, to the best of the CCA's knowledge, at the time of publication. Due to the dynamic nature of the internet, resources that are free and publicly available may subsequently require a fee or restrict access, and the location of items may change as menus and webpages are reorganized.

CCA | CAC

Printed in Ottawa, Canada

Canada

This assessment was made possible with the support of the Government of Canada

The Expert Panel on Public Safety in the Digital Age would like to acknowledge the First Nations, Inuit, and Métis peoples who have stewarded the lands now known as Canada since time immemorial.

The Council of Canadian Academies (CCA) acknowledges that its Ottawa office is located on the unceded, unsurrendered ancestral home of the Anishinaabe Algonquin Nation, who have cared for the environment of this territory for millennia. Though our offices are in a single location, our work to support evidence-informed decision-making has potentially broad impacts across Canada. We at the CCA recognize the importance of drawing on a wide range of knowledges and experiences to inform policies that will build a stronger, more equitable, and more just society.

The Council of Canadian Academies

The Council of Canadian Academies (CCA) is a not-for-profit organization that supports independent, science-based, authoritative expert assessments to inform public policy development in Canada. Led by a Board of Directors and advised by a Scientific Advisory Committee, the CCA's work encompasses a broad definition of science, incorporating the natural, social, and health sciences as well as engineering and the humanities. CCA assessments are conducted by independent, multidisciplinary panels of experts from across Canada and abroad. Assessments strive to identify emerging issues, gaps in knowledge, Canadian strengths, and international trends and practices. Upon completion, assessments provide government decision-makers, researchers, and stakeholders with high-quality information required to develop informed and innovative public policy.

All CCA assessments undergo a formal peer review and are published and made available to the public free of charge. Assessments can be referred to the CCA by foundations, non-governmental organizations, the private sector, and any order of government.

www.cca-reports.ca

@cca_reports

The Academies

The CCA is supported by its three founding Academies:

The Royal Society of Canada (RSC)

Founded in 1882, the RSC comprises the Academies of Arts, Humanities and Sciences, as well as Canada's first national system of multidisciplinary recognition for the emerging generation of Canadian intellectual leadership: The College of New Scholars, Artists and Scientists. Its mission is to recognize scholarly, research, and artistic excellence, to advise governments and organizations, and to promote a culture of knowledge and innovation in Canada and with other national academies around the world.

The Canadian Academy of Engineering (CAE)

The CAE is the national institution through which Canada's most distinguished and experienced engineers provide strategic advice on matters of critical importance to Canada. The Academy is an independent, self-governing, and non-profit organization established in 1987. Fellows are nominated and elected by their peers in recognition of their distinguished achievements and career-long service to the engineering profession. Fellows of the Academy are committed to ensuring that Canada's engineering expertise is applied to the benefit of all Canadians.

The Canadian Academy of Health Sciences (CAHS)

The CAHS recognizes excellence in the health sciences by appointing Fellows based on their outstanding achievements in the academic health sciences in Canada and on their willingness to serve the Canadian public. The Academy provides timely, informed, and unbiased assessments of issues affecting the health of Canadians and recommends strategic, actionable solutions. Founded in 2004, CAHS appoints new Fellows on an annual basis. The organization is managed by a voluntary Board of Directors and a Board Executive.

Expert Panel on Public Safety in the Digital Age

Under the guidance of its Scientific Advisory Committee and Board of Directors, the CCA assembled the **Expert Panel on Public Safety in the Digital Age** to undertake this project. Each member was selected for their expertise, experience, and demonstrated leadership.

Jennifer Stoddart, O.C., C.Q., Ad.E. (Chair), Lawyer, Strategic Advisor, Fasken; former Privacy Commissioner of Canada (Montréal, QC)

Benoît Dupont, Professor, School of Criminology, Canada Research Chair in Cybersecurity, University Research Chair in the Prevention of Cybercrime, Université de Montréal; Scientific Director, Human-Centric Cybersecurity Partnership (Montréal, QC)

Richard Frank, Associate Professor, School of Criminology, Director of the International CyberCrime Research Centre, Simon Fraser University (Burnaby, BC)

Colin Gavaghan, Professor, Bristol Digital Futures Institute and University of Bristol Law School, University of Bristol (Bristol, United Kingdom)

Laura Huey, Professor, Department of Sociology, Western University (London, ON)

Emily Laidlaw, Canada Research Chair in Cybersecurity Law and Associate Professor, Faculty of Law, University of Calgary (Calgary, AB)

Arash Habibi Lashkari, Associate Professor and Canada Research Chair in Cybersecurity, School of Information Technology, York University (Toronto, ON)

Christian Leuprecht, Class of 1965 Professor in Leadership, Department of Political Science and Economics, Royal Military College of Canada; Director, Institute of Intergovernmental Relations, School of Policy Studies, Queen's University (Kingston, ON)

Florian Martin-Bariteau, Associate Professor of Law and University Research Chair in Technology and Society, University of Ottawa; Fellow, Berkman-Klein Center for Internet and Society, Harvard University (Ottawa, ON)

Shannon Parker, Director, Risk Advisory/Cyber and Strategic Risk, Deloitte (Saskatoon, SK)

Christopher Parsons, Senior Technology and Policy Advisor, Information and Privacy Commissioner of Ontario; formerly, Senior Research Associate and Managing Director of the Telecom Transparency Project at the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (Toronto, ON)

Jad Saliba, Founder and CTO, Magnet Forensics (Waterloo, ON)

Heidi Tworek, Canada Research Chair, Director, Centre for the Study of Democratic Institutions; Associate Professor, School of Public Policy and Global Affairs, and Department of History, University of British Columbia (Vancouver, BC)

Message from the President and CEO

Technology is fundamentally changing how we live, work, and interact online. Navigating the digital environment — from protecting a myriad of passwords to staying alert for scams — can be complex at the best of times. For those who find themselves the target of nefarious actors, the fallout can be particularly fraught. The impacts of cyber-fraud, harassment and abuse, and other online harms, are significant and can be profoundly life changing. In Canada, and around the world, these types of activities are on the rise.

When someone does become a target of cyber-enabled harm, determining how and where to seek recourse can present its own set of hurdles. Canadian criminal law that applies to cyber-related crime was originally designed for offline activities and may not apply as directly. Law enforcement is grappling with gaps in training, data limitations, and resourcing issues. Perpetrators meanwhile often use anonymity, encryption, and the speed of technological change to their advantage.

Further complicating matters is the fact that not all online harms are the result of illegal behaviour; they take place on a spectrum of legality and criminality — consider online misinformation and some forms of hateful speech for example, which may push the socially accepted limits of ethically appropriate behaviour, while not passing the threshold of illegal. For this reason, law reform alone will not solve the challenges presented by the growth and misuse of information and communication technologies (ICTs). Rather, all facets of society will have a role to play in addressing cyber-related crimes and harms.

Recognizing the changes and challenges ICTs have created in the digital public space, Public Safety Canada asked the CCA to examine leading practices that could help reduce risks to public safety while respecting human rights and privacy.

Vulnerable Connections explores the ever-evolving threats shaping the online environment. The report considers the challenges and opportunities of regulating, preventing, investigating, prosecuting, and countering of technology-enabled crimes and harms, and describes various regulatory approaches from Canada and abroad.

On behalf of the CCA, I'd like to thank the Panel for its diligent work on this report, which was informed by their depth of expertise in cybersecurity, history, criminology, law enforcement, and law and governance. As Chair, Jennifer Stoddart skillfully led the Panel through a process conducted both virtually and in person. As always, guidance and oversight provided by the CCA's Board of Directors and Scientific Advisory Committee throughout this process, was greatly appreciated.

Eric M. Meslin, PhD, FRSC, FCAHS
President and CEO, Council of Canadian Academies

Message from the Chair

Information and communication technologies have had a profound impact on day-to-day life and our digital and physical worlds are now practically inseparable. Over recent decades, digital technologies have become essential for obtaining healthcare and education, accessing public services, participating in the workforce, maintaining social connections, and more. While these technologies have led to considerable benefits, their ubiquity also means that it is possible for anyone, even those who are offline themselves, to become a target of cyber-enabled crimes or harmful behaviours. Furthermore, the proliferation of digital technologies has had a profound impact on privacy, an essential component of personal security and dignity.

Cyber-enabled harmful activities are on the rise in Canada, leading to substantial physical, economic, psychological, and reputational harms for people across the country. However, existing public safety structures and private sector approaches have not adequately adapted to a landscape radically altered by digital technologies. Accordingly, governments in Canada are playing catch up as they grapple with how to enhance the safety of the online ecosystem, while also protecting constitutional rights and freedoms. At the same time, the justice system is facing considerable challenges in applying existing legal frameworks that prohibit some harmful online behaviours. Police are often hindered in their abilities to investigate these criminal activities.

Vulnerable Connections examines how harmful and illegal activities have evolved as a result of digital technologies, ensuing challenges this causes for policy-makers and law enforcement, and possible opportunities in regulation, prevention, and investigation of cyber-enabled harm. The report illustrates both the complexity and the urgency of these issues and demonstrates that promoting a safer online ecosystem can not be accomplished through the actions of a single public agency, be it provincial, federal, or foreign. Cooperation and coordination across jurisdictions are essential as cyber-enabled harm crosses borders and continues to evolve quickly. Additionally, solutions do not lie solely in the hands of governments; the private sector, including social media platforms, have a critical role to play, as do civil societies.

My fellow Panel members brought a wide range of experience and knowledge to the table, and I would like to thank them for their hard work and sustained engagement on this critical project. In my view, their rigorous discussions and debates have led to a comprehensive and engaging report. I would also like to thank the CCA staff for their critical support and responsiveness throughout this process. Finally, on behalf of the Panel, I would like to thank Public Safety Canada and the seven supporting federal departments and agencies* for sponsoring and submitting this timely and critical question.

Jennifer Stoddart.

Jennifer Stoddart, O.C., C.Q., Ad.E.
Chair, Expert Panel on Public Safety in the Digital Age

*Canadian Heritage; Communications Security Establishment; Global Affairs Canada; Innovation, Science, and Economic Development Canada; Justice Canada; Privy Council Office; Royal Canadian Mounted Police

CCA Project Staff

Assessment Team:	**Becky Chapman,** Project Director
	Adam Fortais, Researcher
	Teresa Iacobelli, Research Associate
	Anastasia Konina, Research Associate
	Ricardo Pelai, Research Associate
	Kate Hemstreet, Project Coordinator
	Jenn Snider Cruise, Project Coordinator
	Tijs Creutzberg, Director of Assessments

With assistance from:

Editor	Jody Cooper
Layout	gordongroup
Translator, En-Fr	François Abraham

Peer Review

This report was reviewed in draft form by the individuals listed below who were selected by the CCA for their diverse perspectives and areas of expertise.

The reviewers assessed the objectivity and quality of the report. Their confidential submissions were considered in full by the Panel, and many of their suggestions were incorporated into the report. They were not asked to endorse the conclusions, nor did they see the final draft of the report before its release. Responsibility for the final content of this report rests entirely with the authoring Panel and the CCA.

The CCA wishes to thank the following experts for their review of this report:

Aengus Bridgman, PhD Candidate in Political Science, McGill University; former Director of the Media Ecosystem Observatory (MEO) as part of the Centre for Media, Technology and Democracy (Montréal, QC)

Aurélie Campana, Professor, Department of Political Science, Université Laval; former Canadian Research Chair on Conflicts and Terrorism (2007–2017) and Executive Member of the Canadian Research Network on Terrorism, Security and Society (TSAS) (2015–2022); (Quebéc, QC)

Ritesh Kotak, Digital and Cybersecurity Strategist and Co-Founder, jusTech; E-Crime Cyber Council (ECC) Member, Canadian Association of Chiefs of Police; Chair of the Dean's Alumni Advisory Council on Technology, Faculty of Law, University of Ottawa (Toronto, ON)

Vivek Krishnamurthy, Samuelson-Glushko Professor of Law and Director, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), University of Ottawa; Faculty Associate, Berkman Klein Center for Internet & Society, Harvard University; Senior Associate (Non-Resident), Center for Strategic and International Studies (Ottawa, ON)

Jacques Marcoux, Director of Research and Analytics, Canadian Centre for Child Protection (C3P); former data journalist and investigative reporter, CBC News (Winnipeg, MB)

Brenda McPhail, Director, Privacy, Technology & Surveillance Program, Canadian Civil Liberties Association (CCLA) (Toronto, ON)

Steven Penney, Professor, Faculty of Law, University of Alberta; Chair, Centre for Constitutional Studies Advisory Board; Member, Alberta Law Review Advisory Board (Edmonton, AB)

Tamara A. Small, Professor, Department of Political Science, University of Guelph (Guelph, ON)

Thorsten Wetzling, Head of Research, Digital Rights, Surveillance and Democracy Unit, Stiftung Neue Verantwortung e.V. (Berlin, Germany)

The peer review process was monitored on behalf of the CCA's Board of Directors and Scientific Advisory Committee by **Neena L. Chappell, C.M., FRSC, FCAHS**, Professor Emeritus, Institute on Aging & Lifelong Health and Department of Sociology, University of Victoria. The role of the peer review monitor is to ensure that the Panel gives full and fair consideration to the submissions of the peer reviewers. The Board of the CCA authorizes public release of an expert panel report only after the peer review monitor confirms that the CCA's report review requirements have been satisfied. The CCA thanks Dr. Chappell for her diligent contribution as peer review monitor.

Executive Summary

Digital technologies and platforms — including smartphones, and social media and other online applications — have drastically altered day-to-day life in Canada, bringing considerable benefits along with the risk of substantial harm. Everyone's experiences are shaped in some way by digital technologies, whether they are online or not. Digital technologies permeate all institutions and, as a result, everyone in Canada is increasingly exposed to a wide range of potential online threats to their public safety. Some of the threats facilitated by information and communication technologies (ICTs) are not new, but they are now occurring in digital spaces and on a larger scale, while other harms are emerging and rapidly evolving. In this context, the role of law enforcement and governments in protecting digital public safety is in flux, and it is unclear where, how, and from whom people can seek help when experiencing cyber-enabled harms.

All people living in Canada are digital-by-default, even if they are offline or rarely use digital technologies. While the digital context brings considerable benefits, it can also compromise everyone's safety.

Recognizing the importance of understanding and addressing the challenges that ICTs pose for digital public safety, Public Safety Canada (hereafter, "the Sponsor") asked the Council of Canadian Academies (CCA) to convene an expert panel tasked with examining leading practices that could help reduce risks to public safety while respecting human rights and privacy. To answer the charge, the CCA assembled a multidisciplinary panel of 13 experts with backgrounds and expertise in cybersecurity, history, criminology, law enforcement, and law and governance.

In line with the interests of the Sponsor, the Expert Panel on Public Safety in the Digital Age ("the Panel") focused its research and analysis on activities that use technology as an instrument (*cyber-enabled*) to inflict harm on individuals.[1] These include activities such as radicalization, online abuse and cyber-fraud that take place on a spectrum of legality and criminality. While the activities that are the focus of this report are harmful, the line between lawful and unlawful behaviour is not always clear, nor is there a consensus on where that line ought to be.

1 Cyber-dependent harmful activities (e.g., malware) are outside of the scope of this report but are discussed in some instances where evidence is relevant for cyber-enabled harms.

Answering the Charge

How have activities relating to serious criminal activity (including organized crime and child sexual exploitation) and online harms (including disinformation, violent extremist and terrorist use of the internet) in Canada changed to exploit the evolving information and communications technologies (ICTs) landscape?

Cyber-enabled crimes are largely under-reported, but existing data demonstrate that the frequency of police-reported cyber-enabled crimes, as well as the number of cyber-threat actors, are rising in Canada. Importantly, the proliferation of cyber-enabled crime is not only the result of the increased use of digital technologies but can be linked to social and economic factors such as polarization, isolation, and economic and political disenfranchisement.

There is considerable evidence showing how people can exploit ICTs to commit a wide range of harmful acts, both lawful and unlawful, that lead to serious physical, psychological, and financial impacts. For example, digital platforms have been used to facilitate the trafficking of women and children by making it easier for perpetrators to recruit, advertise, and communicate; online harassment and abuse are becoming increasingly prevalent on large social media platforms, leading to physical and psychological harms, and causing a chilling effect on the freedom of expression of victims and survivors; and ICTs have made it easier to both engage in fraudulent activities (e.g., by using social media to find and communicate with potential victims) and enable more sophisticated fraud tactics, such as spoofing and phishing, which are difficult to detect. The rapid proliferation of online misinformation has further exacerbated cyber-fraud and the spread of hate.

Technologies have drastically altered day-to-day life in Canada, yet the approaches taken by governments and the private sector, including laws and policies, have not always kept up with new challenges.

A key factor that enables harmful use of digital technologies is the provision of anonymity. For instance, the high levels of user anonymity in cryptocurrency exchanges, on the Dark Web, and over virtual private networks (VPN) enables malicious actors to conceal their identities, as well as their illegal or harmful activities. Digital technologies have also created new mechanisms for funding criminal activities; cryptocurrencies, for example, are creating challenges for law enforcement, as they can be used to fund crimes across jurisdictions, pay for illegal goods or services, and launder money.

What challenges do advances in ICTs (including encryption and 5G) pose for preventing, countering, investigating, and prosecuting crimes and addressing online harms?

An important pillar of preventing cyber-enabled harms is having data on where and how frequently they occur, and their effects on victims and survivors. In the realm of criminal activities, police reports are important data sources that provide some insight, however, a plethora of factors limit the utility of this data. Cyber-enabled crimes are not reported consistently across police jurisdictions, in part due to capacity constraints within police units, resulting in significant variations in numbers across municipalities. The result is that data on cybercrimes are severely limited in Canada, as is research and data on other harms. Further, research on cybersecurity and law enforcement practices in general is also insufficient. These data gaps hinder the ability of law enforcement and different orders of governments to direct resources, evaluate the appropriateness and potential of new approaches, and determine the effectiveness of measures that are implemented.

Data volume, resource limitations, and skills gaps, as well as outdated organizational structures, and technological advancements, present challenges for law enforcement in the prevention, investigation, analysis, and prosecution of cyber-enabled crimes.

The speed of technological change complicates the application, interpretation, and enforcement of laws. Each emerging technology (e.g., 5G, end-to-end encryption) creates its own challenges that warrants a full report; however, there are also common cross-cutting challenges. A fundamental problem is that Canadian criminal law that applies to cyber-enabled crimes was designed for offline activities. When new digital technologies are released into the market, typically with little or no regulatory oversight or preparation, serious public safety and privacy implications can follow. The rapid pace of contemporary ICT innovation means that law enforcement, policy-makers, and ICT users are routinely forced to respond reactively to new ways in which crimes are being perpetrated. Furthermore, a lack of guidance and oversight on the use of new technologies by law enforcement can lead to missed opportunities or the misuse of tools in ways that violate privacy or other rights.

Jurisdictional barriers pose substantial challenges to countering cyber-enabled harms. Cyber-threat actors can be physically located anywhere in the world and, often, victim and perpetrator are not located in the same jurisdiction. With the high levels of anonymity and multiple layers of encryption that some digital platforms afford users, it can be difficult to collect relevant evidence, including

the origin of a particular criminal activity. For example, crimes committed on the Dark Web are notoriously difficult to detect and counter. Specialized police operations may disrupt certain cybercriminal activities, but these have limited impacts, over the long term, on the cyber-threat ecosystem as a whole.

Prominent gaps exist in legislation, regulation, standards, and policies aimed at countering online harms. For example, non-consensual intimate content that originates outside of Canada complicates and lengthens domestic prosecution efforts. Additionally, regulatory tools in Canada are fragmented or ambiguous. A notable example is the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which prohibits private organizations from collecting, using, or disclosing personal information without an individual's consent; however, it generally does not apply to non-commercial activity. Regulatory gaps in, and confusion around, monitoring crowdfunding sites outside the country, as well as some forms of cryptocurrency exchanges, also persist.

Beyond jurisdictional and regulatory challenges, some agencies lack necessary statutory enforcement powers. For instance, federal and provincial or territorial privacy commissioners are mandated to investigate breach of privacy complaints, but their respective enforcement powers vary. Most commissioners are unable to enforce their decisions or award monetary compensation to affected individuals, unlike commissioners in other jurisdictions. Additionally, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is statutorily mandated to combat money laundering and the financing of terrorist activities, but it does not have investigative powers and law enforcement relationships equivalent to similar agencies in the United Kingdom and the United States. In Canada, enforcement of financial crimes falls to police agencies, whose capacity to trace transactions as part of criminal investigations is limited, especially given the increasing use of emerging ICTs such as cryptocurrencies.

On the ground, the persistent shortage of financial, technological, and human resources within law enforcement and the broader criminal justice system is a key barrier to investigating and prosecuting cyber-enabled crimes in a timely manner. In Canada, there are insufficient specialized resources and expertise needed to deal with the growing volume of digital evidence, and the generalist model of policing organizations does not incentivize the recruitment and retention of officers who possess the required skills. A lack of appreciation for the role of cyber-specialists working in the policing ecosystem, coupled with their low visibility, may also contribute to capacity constraints. One of the implications of a lack of expertise is that the criminal justice system is deeply constrained in its ability to effectively deal with the increasingly digital nature of crime and the associated increase of evidence that needs to be examined. People in Canada have

a constitutional right to a trial within a reasonable time,[2] and delays in processing digital evidence can lead to proceedings being stayed while insufficient resources may lead to certain cases not being pursued at all. Furthermore, poor coordination and a misunderstanding of what can be shared within and across law enforcement agencies can lead to confusion and inefficient allocation of existing resources.

Law enforcement agencies in Canada often describe existing mechanisms for accessing criminal evidence and data housed outside Canada as too slow, cumbersome, or resource-intensive. Similarly, encryption has been cited by law enforcement as a challenge for investigating criminal activities, especially when it is necessary to rely on service providers to share relevant evidence in an accessible format. At the same time, weakening encryption would lead to considerable privacy risks, as it is essential for protecting users' information.

Alongside various government and law enforcement actors, the private sector has an important role to play in governing online environments. For instance, social media companies largely self-regulate when it comes to content moderation on their platforms and have had some limited success in countering harmful content online. However, online misinformation and hate speech are difficult to contain because they can spread rapidly on a large scale; this is due, in part, to the current design of many social media algorithms, which amplify inflammatory content that generates more engagement. Content removal policies are inconsistent across social media platforms, and moderation efforts are often outsourced and under-resourced. Some existing and proposed moderation methods, especially those that use automation, can lead to the over-removal of content and are more likely to flag content posted by members of marginalized groups.

Considering the impact that advances in information and communications technologies have had on a global scale, what do current evidence and knowledge suggest regarding promising and leading practices that could be applied in Canada for investigating, preventing, and countering threats to public safety while respecting human rights and privacy?

The experience of jurisdictions that share some sociopolitical similarities with Canada can provide insights about potential challenges and opportunities associated with different regulatory approaches. For example, Australian legislation enables the eSafety Commissioner to investigate and address some cyber-enabled harms outside traditional law enforcement, while the European Union enacted requirements for a notice and take-down mechanism for illegal content that will apply to some online intermediaries across all member states. Some measures implemented elsewhere, however, have led to the over-removal of

2 In its 2016 decision in *R. v. Jordan*, the Supreme Court of Canada stated that the time between someone's arrest and trial could be no more than 18 months in provincial courts and 30 months in superior courts.

legal, or even non-harmful, content, raising concerns about freedom of expression and privacy. These issues, as well as differences among legal systems and legal cultures, need to be considered when assessing the extent to which other jurisdictions' approaches are appropriate for the Canadian context.

Reforms to legal and policy frameworks for the digital context are underway around the world. While Canada can learn from foreign approaches, all orders of governments must consider the Canadian legal context when assessing the extent to which foreign approaches are appropriate in their jurisdiction.

Law reforms alone will not solve the challenges presented by ICTs. The structure of law enforcement needs to adapt to the changing context of policing in Canada, and small-scale changes will not address the substantial capacity and skills shortages in policing. Promising and emerging practices in this realm include the professionalization of policing, including a greater differentiation of roles within law enforcement—as opposed to a reliance on generalist police officers—which could support the development and retention of officers with specialized digital skills. Affordable and accessible training in general digital skills made available to all police officers, at low cost, could also improve the ability of law enforcement to investigate cyber-enabled crimes. There are opportunities for the private sector and academia to play a more active role in training the police and, in the case of the former, working with certain types of digital evidence. Finally, initiatives such as the North American Cyber Classification Compendium (NACCC) have the potential to fill data gaps and facilitate accurate and consistent categorization of cyber-enabled crimes and harms across multiple actors and jurisdictions.

ICTs are not only used to perpetrate harm. A range of digital technologies are used by law enforcement agencies to respond to, prevent, detect, and investigate criminal activity. While many of these technologies have considerable benefits, ongoing guidance and oversight are needed, since each tool has its own ethical and privacy considerations. For example, facial recognition technology (FRT) has been used by law enforcement in Canada to identify individuals of interest during criminal investigations but has also led to privacy violations and questions around equity and the targeting of marginalized groups. These issues were not unforeseen. Moving forward, appropriate regulation, oversight, transparency, and accountability in the use of new technologies can help ensure their proper integration and deployment by law enforcement in Canada. Comparatively, bodies such as the New Zealand Advisory Panel on Emergent Technologies, can provide a

mechanism to critically evaluate the policy and ethical implications of new technologies before they are used by police.

While many harmful cyber-enabled acts violate the Canadian *Criminal Code*, the criminalization of harmful online activities is not always appropriate, and it may not be the most effective means of combatting a particular online harm, nor be victims' and survivors' preferred response method. In some cases, tort law — a form of private law concerned with compensating those injured by the wrongdoings of others — contains important privacy remedies and can incentivize legal online behaviour. Although litigating these cases is resource-intensive and time-consuming, introducing a broad cause of action for invasions of privacy in the form of torts has been successful in some Canadian provinces. Other non-criminal legal avenues include defamation law, Quebec civil law, privacy legislation regulating public and private sector data collection, and anti-spamming legislation. All of these legal avenues have their own challenges and limitations.

Not all online harms meet the threshold of criminal behaviour. While legal reform may be necessary to address some online harms, in other cases, non-legal approaches will be more effective and responsive to victims' and survivors' preferences.

The governance of digital spaces is not limited to state-sanctioned tools and rules, and in some cases no legal avenue is suitable. Alternatively, a variety of instruments are available to create a responsive governance system, including corporate self-governance policies and voluntary codes of conduct. Some large social media companies have developed policies that dictate what qualifies as harmful content and have demonstrated the ability to reactively moderate and remove large volumes of such content from their platforms in specific instances. Additional emerging practices implemented by large social media companies include partnering with third-party fact-checking enterprises and institutions, forming independent review committees to make high-profile content moderation decisions, and using automated tools (although this has been shown to lead to over-removal of content). Despite these efforts, harmful content continues to proliferate, and other challenges persist, including limited transparency, accountability, and consistency in moderation decisions.

Some victims and survivors may also prefer non-criminal means of addressing cyber-enabled harms. For instance, in the case of non-consensual distribution of intimate images, a victim or survivor's immediate focus may be on the removal of those images from online spaces rather than criminal investigation. Prevention,

both on the side of the perpetrator and the target, can also play a role. For example, peer-driven education programs and school-led initiatives and policies can be part of the solution to online harassment and abuse, particularly among youth. Similarly, there are promising digital literacy education initiatives that can equip people with the tools to critically assess information online, identify harmful content, and reduce privacy risks.

Privacy and human rights are often seen to be at odds with security in digital contexts, but these can be mutually reinforcing.

Compounding these governance challenges is the fact that privacy is highly contextual, and societal conceptions of privacy are constantly evolving. Finding some form of aspirational balance between privacy and security is not feasible, nor is it a suitable construct in digital contexts. Rather, there is often a complex, dynamic, and contextual interplay among privacy, security, and other rights and freedoms, including freedom of association. In some cases, certain forms of security supersede the right to individual privacy. Importantly, privacy and security can be mutually reinforcing, and a degree of privacy is required to ensure one's personal security or the security of a community in which an individual resides.

The right to privacy is protected under Canadian law while, at the same time, growing amounts and types of digital information make protecting individual privacy and digital security increasingly complicated. Governments, law enforcement agencies, and private companies have substantially expanded their collection, use, and disclosure of data, often without consent, across borders and with limited oversight. Existing regulatory tools to protect and govern how personal information is managed need to be reformed and strengthened in a coordinated and transparent way. In this context, it is also vital for individuals and communities to have the ability to make informed decisions about their privacy. Some provinces have developed their own approaches to protecting privacy. For example, Quebec's *Charter of Human Rights and Freedoms* recognizes privacy as a human right and guarantees that right by providing a direct right of action to affected individuals; likewise, Quebec's private sector privacy law has a broader scope and stricter enforcement measures than similar federal legislation.

What opportunities exist to enhance the overall health of the online ecosystem (e.g., support resilience of platforms and services against exploitation)?

There are no panaceas when it comes to enhancing the overall health of online ecosystems, nor any single actor with the ability to protect public safety online. Diverse legal and non-legal avenues exist in which different orders of government, law enforcement agencies, private sector companies, civil society, educational institutions, and individuals all play important roles in cultivating resilience to online harms. While social media companies have undertaken some actions to moderate abusive and hateful content, considerable amounts of harmful content remain; but there are opportunities to continue to innovate, adapt, and collaborate proactively. Meaningfully engaging victims and survivors, and adopting victim-centric and trauma-informed approaches, are paramount to any efforts to improve the health of the online ecosystem.

Early investments and interventions that consider human rights have enabled Canada to more effectively investigate and prosecute some cyber-enabled crimes.

Within public governance of digital spaces, some emerging policies seek to establish sufficient mechanisms to deter individuals from behaving unlawfully while, at the same time, not unduly intruding on users' freedom of expression and privacy. However — as existing and proposed regulatory approaches in Canada and abroad demonstrate — it is difficult to fully reconcile these elements, in part due to the rapidly evolving nature of digital technologies.

Many of the barriers preventing an adequate response to cyber-enabled harms are systemic and necessitate substantial reforms. Promising and emerging approaches, led by different countries, provinces, and sectors, provide valuable lessons for Canada. While this report is replete with examples of how technological tools can be used by various actors to commit harmful acts, technology can also be part of the solution in combination with a collective, cross-national governance approach that includes appropriate transparency and oversight. Overall, cultivating a safer online ecosystem will not be accomplished solely through incremental steps or the actions of a single entity. Enhancing the digital public safety of people in Canada demands a collective approach that includes civil society, policy-makers, law enforcement agencies, and the private sector, and includes legal and non-legal approaches.

Abbreviations

AI	artificial intelligence
BSI	basic subscriber information
C3P	Canadian Centre for Child Protection
CASL	Canada's anti-spam law
CRTC	Canadian Radio-Television and Telecommunications Commission
CSAM	child sexual abuse material
CSIS	Canadian Security Intelligence Service
CUSMA	Canada, the United States, and Mexico Agreement
DEX	decentralized cryptocurrency exchange
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FRT	facial recognition technology
GDPR	General Data Protection Regulation
ICTs	information and communication technologies
IMVE	ideologically motivated violent extremism
MLA	mutual legal assistance agreement
MLAT	mutual legal assistance treaty
MSB	money service business
NACCC	North American Cyber Classification Compendium
OCSP	online communication service provider
ODIT	on-device investigation tool
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	Personal Information Protection and Electronic Documents Act
PMVE	politically motivated violent extremism
RMVE	religiously motivated violent extremism
TVEC	terrorist and violent extremist content
VPN	virtual private network

Contents

1

Introduction

The development and proliferation of online systems have led to immeasurable good, thanks in large part to more accessible and powerful methods of communication, data collection, and analysis. The internet and its associated information and communication technologies (ICTs) (including social media and other online applications) are essential to the everyday lives of people living in Canada — and their ubiquity makes everyone in Canada *digital-by-default*, whether they are online or not. Online systems also enable malicious actors to inflict serious harm on individuals and communities. This report investigates the nature of these threats as they apply to the safety, security, privacy, and human rights of people in Canada.

As more activities and information move online, people have become increasingly susceptible and vulnerable to cyber-threats and cybercrimes. This is not only costly to organizations and individuals; technology-facilitated crime and harmful online activities also pose a threat to the safety and well-being of people in Canada and abroad. This report addresses the ever-evolving nature of ICTs and the challenges and opportunities they pose for all orders of governments, law enforcement agencies, and other actors working to prevent and address illegal and harmful behaviours.

1.1 The Charge

Recognizing the importance of understanding and addressing the challenges created by ICTs, Public Safety Canada (hereafter "the Sponsor") asked the CCA to convene an expert panel tasked with examining leading practices that could help reduce risks to public safety while respecting human rights and privacy. Specifically, the CCA was asked to answer the following question and sub-questions:

Considering the impact that advances in information and communications technologies have had on a global scale, what do current evidence and knowledge suggest regarding promising and leading practices that could be applied in Canada for investigating, preventing, and countering threats to public safety while respecting human rights and privacy?

- How have activities relating to serious criminal activity (including organized crime and child sexual exploitation) and online harms (including disinformation, violent extremist and terrorist use of the internet) in Canada changed to exploit the evolving information and communications technologies (ICTs) landscape?
- What challenges do advances in ICTs (including encryption and 5G) pose for preventing, countering, investigating, and prosecuting crimes and addressing online harms?
- What opportunities exist to enhance the overall health of the online ecosystem (e.g., support resilience of platforms and services against exploitation)?

1.2 The Panel's Approach

To answer the charge, the CCA assembled a multidisciplinary panel of 13 experts (the Expert Panel on Public Safety in the Digital Age, hereafter "the Panel") with backgrounds and expertise in cybersecurity, social sciences, criminology, law enforcement, and law and governance. Each member served on the Panel as an informed individual rather than as a representative of a specific discipline, organization, region, or set of values. The Panel met several times virtually and once in person over a period of 12 months to review and collect evidence and deliberate on its charge.

At the beginning of the assessment process, the Panel met with the Sponsor to acquire a fuller understanding of the charge and to confirm which issues were in and out of scope. The Sponsor noted that it wanted the Panel to focus on serious cyber-enabled criminal and harmful activities that directly affect people's lives in non-digital spaces in Canada. The Sponsor also noted that pure cybercrimes where technology itself is the target (e.g., data release) were not in scope for the assessment. Given this direction, the report centres on cyber-enabled activities that create the greatest harm to individuals rather than focusing on the subset that is considered to be criminal activity alone (Figure 1.1). That is, the Panel centred its work on activities and practices — facilitated by ICTs — that cause, or have the potential to cause, the most harm to people in Canada, regardless of

whether they are reported and/or legally considered crimes. Notably, many (though not all) of these threats are realized through services that depend on user-generated content.

Part of this reasoning stems from the fact that the line between criminal and harmful is often unclear, particularly in the case of ICT-mediated activities. Further, what is considered a crime varies over time and across jurisdictions. For example, while the negative impacts of cyber-bullying are well documented, only certain cyber-bullying actions (e.g., criminal harassment, uttering threats) are against the law in Canada (PS, 2021a). The same is true for hate speech; while hate propaganda is included in the *Criminal Code*, it can be challenging to determine the point where hateful speech crosses the threshold that constitutes criminal offence, which can make it difficult to prosecute. Moreover, as requested by the Sponsor, topics such as misinformation, conspiracy beliefs, and the spread of extremist or hateful content are included in this report because of the disruptive and harmful effects they can have on public discourse, potentially facilitating movements and actions that can threaten or harm the public.

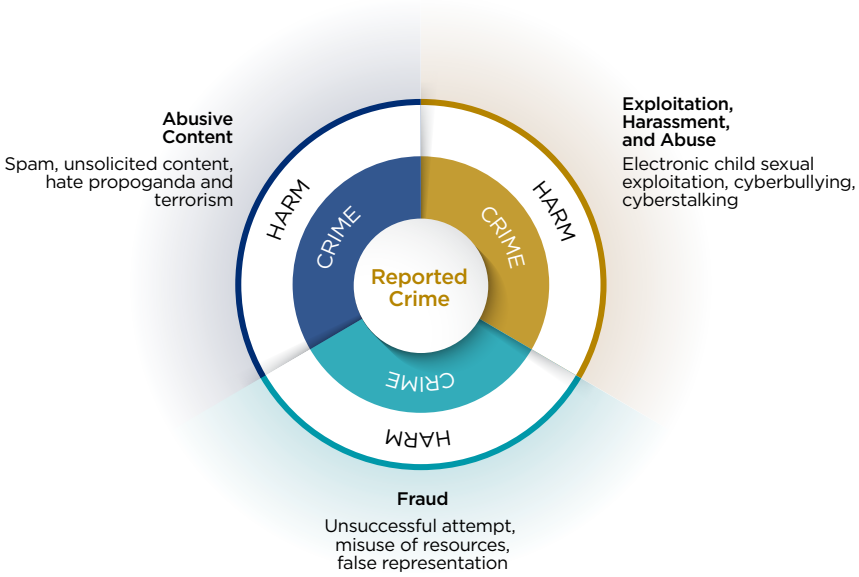


Figure 1.1 Conceptualization of the Universe of Harms

What is legally considered a criminal act varies across time and jurisdiction and does not account for all harm experienced online. At the same time, it is known that reported crime makes up only a subset of all cyber-enabled criminal acts. The scope of this report is limited to the types of harms that would be considered cyber-enabled (technology-as-instrument) crimes and harms, as defined by the North American Cyber Classification Compendium (NACCC) Division of Cybercrime — that is, harms whereby digital technology is used to target people.

1.3 Contextualizing the Charge

The report covers cyber-enabled crimes and harms that pose threats to the safety of individuals

From the outset, the Panel emphasized the importance of contextualizing cyber-related criminal and harmful activities, both historically and socially. Throughout history, advances in technology have altered the targets of crime, the types of crimes committed, the methods for committing crimes, and law enforcement approaches and tools to prevent and combat crime (Brey, 2017). ICTs (and technology, more broadly) have historically benefitted both malicious actors and law enforcement (Brey, 2017). Similarly, there is a well-documented history of concerns about various technologies that could enable crime, along with fears that technology could be used for societal control (McGuire, 2017).

From a sociological perspective, Brey (2017) argues that ICTs reproduce (in a digital form) many social actions, objects, values, practices, and institutions that already exist. Consequently, behaviours occurring online (including criminal ones) are often an extension of what occurs offline, if not the exact same behaviours brought online (Lukings & Lashkari, 2022b). From this perspective, it is unsurprising that many crimes and harms that have historically been committed offline (e.g., fraud, exploitation of children) have migrated to digital platforms (Brey, 2017). Likewise, the emergence of cybercrime and cyber-enabled harm can be a result of many factors, some of which are not related to the proliferation of ICTs, including increased societal polarization and isolation (Canada Centre, 2018; Waller & Anderson, 2021).

While ICTs have led to an evolution in crime and harmful behaviour, they also provide numerous benefits for society. They are vital for accessing essential services (e.g., education, healthcare), the functioning of the economy (e.g., labour market participation, shopping, innovation, business operations), maintaining social connections, and accessing information (CCA, 2021; StatCan, 2021a). Law enforcement agencies also use and depend on ICTs to respond to, investigate, prevent, and communicate about crime (RCMP, 2020a; FBI, 2022). Moreover, digital technologies are important for upholding human rights and democratic goals. For example, a United Nations Human Rights Council Special Rapporteur report noted that ICTs are key enablers that help people exercise fundamental human rights, such as freedom of opinion and expression (UN HRC, 2011a). Applications such as encryption allow human rights defenders, journalists, and others to securely exchange and store information and data (Parsons, 2019). These issues are expanded on in Chapter 2.

Cyber-enabled crimes are both on the rise and under-reported in Canada

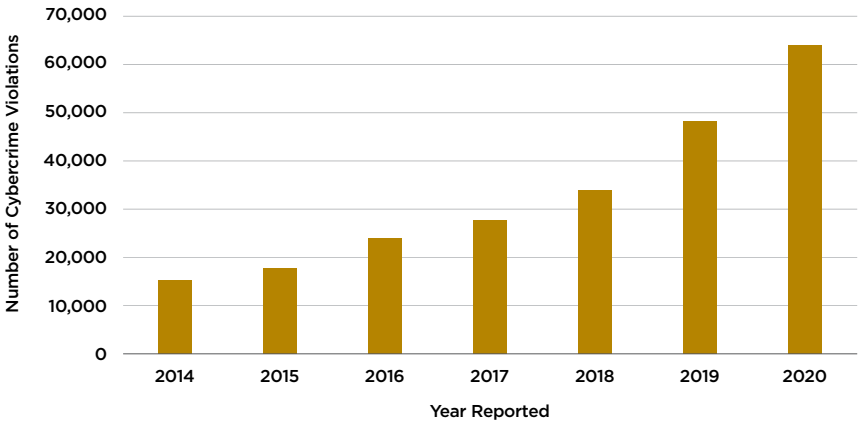
While digital technologies provide substantial benefits, they can also lead to substantial harm, including a rise in activities that qualify as cyber-enabled crimes. Although many instances of cybercrime go unreported, there is evidence that the frequency of cyber-related crimes and number of cyber-threat actors in Canada are increasing (RCMP, 2014; Canadian Centre for Cyber Security, 2020a; Lukings & Lashkari, 2022b). At the same time, the Canadian Centre for Cyber Security (2022a) notes that "cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations."

The number of reported cybercrimes has risen every year since 2014, when Statistics Canada started reporting these numbers using a set methodology[1] (StatCan, 2021b). In 2020, 63,523 cyber-related criminal violations were reported to police in Canada, which constitutes a more than 400% increase compared to 2014 (StatCan, 2021b) (Figure 1.2). That said, cybercrimes that are reported to police make up only a small fraction of all reported crimes in Canada. For example, one study found an average of 44 cybercrime occurrences per 100,000 people compared to almost 5,000 per 100,000 people for all crimes — excluding traffic violations — in Canada's eight largest municipalities between 2014 and 2017 (Popham *et al.*, 2020).

The rise of cyber-related crime from 2020 to 2022 may be attributed to several things (both related and unrelated to the COVID-19 pandemic), including easier and less expensive access to ICTs and internet connectivity in most countries (Lukings & Lashkari, 2022b) as well as increasing levels of isolation and societal polarization (Waller & Anderson, 2021). It is known that people in Canada have spent more time online during the pandemic, because many aspects of daily life moved into that sphere (StatCan, 2020a), creating more opportunities for cyber-threat actors (Moreau, 2021a).

In Canada, nearly half of cyber-related crimes reported to police in 2020 were related to fraud (StatCan, 2021b) (Section 3.3). After fraud, the most common police-reported, cyber-related crimes linked to the Panel's charge are indecent/harassing communications, making or distributing online child sexual abuse material (CSAM), and uttering threats (StatCan, 2021b). The reporting incidence of all categories of cybercrime is increasing, however (CAFC, 2021a; Dupont, 2021). For example, uttering threats online (reported to police) increased by nearly 500% between 2014 and 2020 (StatCan, 2021b).

1 Statistics Canada defines cybercrime as "any criminal act as outlined in Canada's Criminal Code where Information and Communication Technology (ICT) is the target of the offence, or whereby ICT is integral and vital in the commission of the offence" (CCJCSS, 2021). This definition includes, but is not exclusive to, the cyber-enabled crimes central to this report.



Data Source: StatCan (2021b)

Figure 1.2 Number of Police-Reported, Cyber-Related Criminal Violations in Canada

The number of cybercrime violations reported to police each year in Canada has increased annually since Statistics Canada began reporting these totals. A cybercrime violation is one where a computer or the internet was the target of the crime, or the instrument used to commit the crime.

Data suggest most cyber-related crime victims or survivors are women and minors, while most perpetrators are men

While anyone can be a target of cyber-enabled harm, the frequency and impact of these types of activities are not the same across all sociodemographic groups. The latest and most comprehensive publicly available information on the characteristics of victims or survivors of cybercrimes in Canada was collected in 2012, and only includes crimes reported to police (Mazowita & Vézina, 2014). That year, 69% of victims or survivors in police-reported violent incidents associated with cybercrime were women; similarly, 84% of sexual cybercrime victims or survivors were women. Overall, in 2012, 42% of police-reported cybercrime victims or survivors in Canada were under 18 years old. Most victims or survivors of sexual violations associated with cybercrime (96%) were under 18 years of age, and 10% were 12 years old or younger (Mazowita & Vézina, 2014). Additional statistics related to specific types of cybercrimes and harms can be found in subsequent chapters of this report.

Businesses and organizations are also targets of cybercrime, though much of it goes unreported (Wanamaker, 2019). One survey of Canadian businesses showed that, among reported corporate cybercrime attacks, most involved attempts to steal money or demand ransom. However, many other cybercrimes targeting businesses involved the theft of personal customer data and financial information (Wanamaker, 2019).

In Canada, men constitute the majority (76%) of those accused of committing cyber-related crimes (Mazowita & Vézina, 2014). The percentage jumps to 94% when cybercrimes are of a sexual nature. Often, however, no suspects are identified in cybercrime cases, and many remain unsolved. In 2012, for example, there were no suspects identified for 69% and 45% of reported sexual cybercrime and cyber-intimidation violations, respectively (Mazowita & Vézina, 2014).

The cyber-threat ecosystem and motivations of cyber-threat actors are complex

Cyber-threat actors may be individuals, groups, organizations, or states with a malicious intent to negatively impact people's well-being or safety (Canadian Centre for Cyber Security, 2021a). They may also include actors who are politically or ideologically motivated. Cyber-threat actors vary in their capability and location as well as in technical and logistical sophistication, available resources, training, and support for their activities. The motivations of cyber-threat actors also vary (Canadian Centre for Cyber Security, 2021a), although the Panel notes that any given actor may be driven by a number of motivations, including personal satisfaction, geopolitical factors, discontent, entertainment, profit, ideological violence or other ideological factors (Figure 1.3). Furthermore, as with digital spaces as a whole, the cyber-threat ecosystem is itself continually evolving and changing (Canadian Centre for Cyber Security, 2022a).

According to Dupont (2019), the cybersecurity space involves interactions among three interdependent communities:

- an industrial community (one that often introduces digital advancements and digital risks);
- a criminal community (which capitalizes on digital advancements for criminal purposes); and
- a security community (e.g., law enforcement, international organizations).

Figure 1.3 Different Types of Cyber-Threat Actors and Their Motivations

Cyber-threat actors can be states, groups, organizations, or individuals maliciously committing illegal or otherwise harmful activities online. They can be physically located anywhere in the world and their motivations vary; actors may be driven by one or more of the listed motivations.

To this end, a global social network analysis showed that, of 657 organizational cyber-security actors studied, nearly half were part of the private sector, followed by national law enforcement and judicial actors (31%) and non-governmental and professional organizations (16%) (Dupont, 2016). This distribution suggests there may exist polycentric cybercrime governance models whereby multiple centres make decisions semi-autonomously. However, this analysis omits the efforts of civil society, which contributes in different ways (e.g., creating community-driven organizations, generating studies and reports, advocating for civil society protections). Maschmeyer *et al.* (2021) suggest the lack of emphasis on harm to civil society is a result of multiple incentives driving the cybersecurity industry toward protections for high-profile entities that have the resources to pay for high-end cyber defences.

1.3.1 Areas of Focus and Terminology

Cyber-enabled threat actors use digital technology to harm individuals

The breadth of threats and harms that can be considered *cyber* is vast and includes activities that are both in and out of scope of the Panel's work. From a law enforcement perspective in Canada, cyber*crime* is broadly defined as "any crime

where *cyber* — the internet and information technologies, such as computers, tablets, personal digital assistants or mobile devices — has a substantial role in the commission of a criminal offence" (RCMP, 2014). Cybercrimes are generally differentiated between cyber-enabled and cyber-dependent. Cyber-dependent crimes are those targeting technology. They are also known as *technology-as-target* crimes and can "only be committed using computers, networks and digital devices;" examples of these include hacking and spreading malware (RCMP, 2021a). In contrast, cyber-enabled crimes — also known as *technology-as-instrument* or *cyber-assisted* crimes — are those that primarily target people directly. While this category is often associated with crimes that could be committed without ICTs, such crimes are able to increase their scale when technology is used as the instrument to commit the crime (INTERPOL, 2021; RCMP, 2021a). However, not all illegal activities are criminal, and not all harmful activities are illegal. Yet, harmful but legal activities can still represent threats to public safety. For this reason, the scope of the report includes activities that do not necessarily reach a threshold of illegality. Moreover, the Panel notes that the jurisdiction where these activities occur influences applicable law and enforcement mechanisms (e.g., criminal, tort, and common law) (Box 1.1).

Many traditionally offline threats have been adapted for the online ecosystem

In line with the interests of the Sponsor, the Panel's research and analysis were concerned with harmful activities that are generally considered to be cyber-enabled.[2] Many of the activities within the scope of this report blur the line between online harms and *traditionally* offline analogues that have adapted to or enhanced by technology. For example, police report that some car thieves have planted small tracking devices on high-end vehicles parked in public places, so they can locate these vehicles later to steal them (YRP, 2021). Another example is fraud committed after someone's phone, computer, or network is attacked to gather personal data (INTERPOL, 2021). Given the prevalent use of ICTs, most crimes can be expected to have some sort of digital component (Beesley, 2021).

Terminology choices adopted by the Panel, including those related to people who suffer the effects of the activities described in this report are explained in Box 1.1.

2 While the Panel notes that threats considered to be *cyber-dependent* can also result in substantial harms to people, they are not the focus of this report.

Box 1.1 Terminology Used by the Panel

- **Criminal offence** — an act or omission against the state or public order, punishable under criminal law.
- **Cyber-enabled crime** — criminal offences committed using technology.
- **Cyber-enabled harm** — criminal offences or other harmful illegal and legal acts committed using technology.
- **Law enforcement** — the agencies responsible for enforcing Canadian laws within the country. This includes the four levels of policing in Canada: national, provincial, municipal, and Indigenous. Law enforcement is only one type of *public safety agency*, which also includes intelligence, border, correctional, and parole services.
- **Online platforms** — a range of online services, including social media, online marketplaces, content sharing, search engines, and more. These services typically use ICTs to connect users to each other, often collecting data about users and their online activity at the same time. In general, online platforms are not designed to facilitate *cross-platform interoperability* (for example, Facebook users cannot send messages to Twitter users) or offer *data portability* options that would allow users to move data from one platform to another.
- **Regulation** — depending on the context, a term used to refer to rules promulgated by administrative agencies under enabling statutes (e.g., *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulation*) or a system of rules applicable to a certain area or activity (e.g., regulation of social media). In the European Union, regulations are binding legislative acts that must be applied in their entirety by all Member States (e.g., *General Data Protection Regulation*).
- **Tort** — an act or omission that causes harm or injury to a person and results in a civil wrong for which courts impose civil liability.
- **Victim, Target, Survivor** — the cyber-enabled crimes and harms covered in this report target people across all demographics in ways that can be emotionally painful and difficult to discuss. People targeted in this way may be left feeling vulnerable, exploited, and victimized, but everyone's experience is unique. There is no single way of working through these feelings; being characterized as a victim or survivor will not accurately reflect everyone's experiences; for some, transitioning from identifying as a victim to a survivor can be empowering (Pollino, 2021). While certain terms have been adopted throughout this report for the sake of consistency, effort has been made to be sensitive to the unique experiences of those who have been the target of such attacks. For this reason, readers will find the report uses terms such as target, victim, or survivor in various sections.

In addition to the considerations described in Box 1.1, the Panel uses the terms *harm* and *cyber-harm* throughout this report, which together encompass a spectrum of impairments to a person's or entity's welfare and interests (Agrafiotis *et al.*, 2018). Based on a systematic review, Agrafiotis *et al.* (2018) propose a comprehensive taxonomy of cyber-harms that includes physical harms (e.g., injury, pain, loss of life); economic harms (e.g., financial loss, job loss); psychological harms (e.g., anxiety, depression); reputational harms (e.g., damaged relationships, reduced opportunities); and societal harms (e.g., disruption of daily life, negative impact on a nation). While this full range of harms covers substantial negative impacts, based on the priorities of the Sponsor, the report focuses on physical harms, psychological harms, societal harms, and, to a lesser extent, economic harms at the individual level. Additionally, while the charge implies there exists delineation between the digital and non-digital worlds, the Panel makes no such distinction in terms of potential harms and impacts.

The report uses the terminology of the North American Cyber Classification Compendium (NACCC) where possible

Given the complexity and evolution of cyber-harm, it is unsurprising that terminology used by different law enforcement agencies, victims and survivors, civil society, and the criminal justice system varies (INTERPOL, 2021; NACCC, 2021a). The difficulties created by these variations in definition have long been recognized in Canada (Kowalski, 2002). As a way to help address this challenge in relation to activities considered criminal, the NACCC was co-developed by the Cybercrime Support Network (a U.S.-based non-profit), the Canadian Association of Chiefs of Police, and the Canadian E-Crime Cyber Council, along with a group of international cyber experts (NACCC, 2021a). The NACCC seeks to facilitate accurate and consistent categorization of cyber incidents across multiple actors and jurisdictions, and can also be used to broadly categorize types of harm (NACCC, 2021a). Its classification and language system divides cyber-related harmful incidents (those in which harm and/or illegal activities occur) into nine categories, which are in turn divided into sub-categories aligned with Canadian, American, and European governance of cybercrimes and other harmful activities (NACCC, 2021b; Parker, 2021).

The Panel uses NACCC terminology throughout this report to describe harms that fall under the heading of *cyber-enabled*, including abusive content, exploitation, harassment, and abuse, as well as fraud (Figure 1.1). The report does not, however, cover cyber-dependent harms (e.g., malware, intrusion, information gathering, data release, or system and service availability attacks). The Panel notes that there are other classification schemes and terminologies in the literature; while not endorsing any particular classification scheme, it has selected the NACCC to maintain consistency throughout the report.

1.3.2 Sources of Evidence

The evidence used to develop this report comes from a variety of sources and was not limited to peer-reviewed literature

The Panel's assessment is based on a review of various sources of evidence, drawn from peer-reviewed publications, publicly available government information and data, investigative journalism, submissions to proposed legislation, informational interviews with experts, and other relevant grey literature[3] related to digital public safety in Canada. To inform its consideration of promising and leading practices, the Panel reviewed evidence from other jurisdictions (Chapter 5). This report was also informed by a comprehensive peer review, whereby additional experts from Canada and around the world provided further evidence and guidance.

Data limitations related to cyber-enabled harm created evidence challenges for the Panel

While there is clear evidence demonstrating an increase in cyber-enabled crime, it is challenging to paint an accurate picture of frequency and effect, even for those crimes that are reported, let alone harms that do not meet the threshold of illegality. As noted, cybercrimes are not consistently defined, and their impacts are difficult to quantify (Furnell *et al.*, 2015). For example, cybercrime, including cyber-enabled crime, is not an option in some Canadian crime-reporting tools (Malone, 2021), and reporting varies widely by municipality (Popham *et al.*, 2020). The Panel notes that municipalities are generally responsible for tracking their own crime data, using one of several report management systems; these systems will typically only have a box that can be checked if there was a cyber component to the activity in the report. One study found a negative correlation between cybercrime rates and the number of police calls, suggesting that busier police service regions are less likely to record cybercrime incidents (Popham *et al.*, 2020).

Given the different methodologies used to measure cyber-enabled crime and infrequent data collection efforts in some jurisdictions, it is often not possible to accurately compare changes over time, or meaningfully compare statistics among countries (Reep-van den Bergh & Junger, 2018; Caneppele & Aebi, 2019). There are also methodological difficulties in counting and accurately estimating the costs of crime where online and offline components overlap (Levi, 2017). Beyond measurement challenges, it is important to critically examine the origin and validity of available statistics related to cybercrime (Dupont, 2021).

3 "Grey literature stands for manifold document types produced on all levels of government, academics, business and industry in print and electronic formats that are protected by intellectual property rights, of sufficient quality to be collected and preserved by library holdings or institutional repositories, but not controlled by commercial publishers i.e., where publishing is not the primary activity of the producing body" (Schöpfel, 2019).

Cybercrime data collected and shared by private companies are often used to promote their cybersecurity services and therefore may not be reliable or methodologically robust on their own (Dupont, 2016a; Caneppele & Aebi, 2019). In other words, since cybersecurity companies primarily focus on corporate- and government-targeted cybercrime, there are fewer civil-centric cybercrime datasets that can be used to inform online safety and security initiatives (Maschmeyer *et al.*, 2021).

It is also known that cybercrime, including cyber-enabled crime, is under-reported globally and in Canada (Wanamaker, 2019; RCMP, 2021b). People may perceive these types of crime as less serious than others, believe there will be no consequences for offenders, or be unaware that a crime was committed at all (Bidgoli & Grossklags, 2016). One study estimates that fully digital cybercrimes and those with a cyber component (i.e., hybrid crimes) could represent between one-third and one-half of all crimes committed in high-income countries, suggesting massive under-reporting of cybercrime (Caneppele & Aebi, 2019). These challenges in reporting and measuring cybercrime have led some researchers to suggest that the rise in cybercrimes has contributed to an apparent decline in reported non-cybercrime in many countries since the 1990s. In other words, dropping crime rates may represent, in part, the emergence of undetected cybercrime, the evolution of traditionally offline crime into internet-enabled crime, or the migration to more accessible or lucrative forms of cybercrime. As noted earlier, not all harms discussed in this report constitute criminal behaviour and are also likely on the rise, but data related to non-criminal harms are severely limited.

Law enforcement agencies recognize the challenges related to measuring and reporting cybercrime, and more detailed and consistent cybercrime reporting tools are in development in Canada. Statistics Canada has announced its intention to use the NACCC as a basis to consistently collect more accurate statistics involving cybercrime incidents (Parker, 2021). The changes seek to ensure consistent terminology across different actors in the cybercrime space, both in Canada and internationally (StatCan, 2021c). The NACCC was endorsed by the Canadian Association of Chiefs of Police, which supported its use in all Canadian municipal, provincial/territorial, and federal law enforcement organizations (Parker, 2021).

1.4 Report Structure

The report answers the charge by considering digital safety through a human rights lens

To answer the charge, the report first sets out to explain the current and emerging threats shaping the online environment, and how these threats relate to human rights in Canada. Chapter 2 lays the groundwork for the Panel's discussion of digital safety by describing the interplay among privacy, security, and human rights in the context of personal data, surveillance, and personal and relational freedoms. In particular, Chapter 2 focuses on the individual rather than the societal collective, and describes how privacy, security, and human rights are treated in online spaces — and how infringements on these values can lead to harmful if not criminal activity.

Chapters 3 and 4 consider the ways harmful or criminal activity has adapted to incorporate ICTs. Chapter 3 describes harms that are a direct result of digital technologies. Some harms, such as the distribution of CSAM and non-consensual intimate content, are criminal offences, but they can be difficult to detect and enforce because of digital technologies. Other activities discussed in Chapter 3, such as some instances of online harassment, may be harmful, exploitative, or otherwise reprehensible yet legal. In some cases, criminalization is not found to be the most effective means of addressing cyber-enabled harms.

Chapter 4 discusses digital enablers of harm, including the Deep Web and Dark Web, cryptocurrencies, and social media platforms. The chapter includes discussions on services and technologies that may not have been developed with the purpose of perpetuating harms but have been used to (or have the potential to) create opportunities for illegal and harmful activities and also discourse that may encourage people to engage in harmful activities. It also considers the ways online platforms self-moderate but may lack transparency, accountability, and consistency in doing so. In some cases, this is caused by a lack of incentives, public pressure, or strong regulation to motivate desirable moderation practices.

Chapters 5 and 6 address the challenges and opportunities that have emerged relating to the regulation, prevention, investigation, prosecution, and countering of cyber-enabled crimes and harms. Chapter 5 describes existing and emerging regulatory approaches in Canada and abroad. Despite attempts to establish deterrence, protection, and compensation through legal avenues, the speed of technological development makes the interpretation and application of laws surrounding cyber-enabled harms and crimes challenging. Policy-makers in Canada and abroad are considering how law reform might overcome some of the challenges ICTs pose to public safety. However, state-based governance of digital spaces faces challenges when trying to balance the protection of victims or

survivors of cyber-enabled crimes with constitutional rights and freedoms, such as freedom of expression and privacy.

Chapter 6 discusses on-the-ground challenges facing law enforcement and the broader criminal justice system in investigating and prosecuting cyber-enabled crimes, and considers some emerging practices that may help address these barriers. Skills deficits and insufficient resources (including a shortage of personnel) are identified as key barriers to both investigating and prosecuting cyber-enabled crimes, along with poor cooperation across agencies, and critical data gaps in the frequency and impact of cyber-enabled crime. Challenges stemming from obstacles in obtaining digital evidence and encryption are considered, as is the importance of these tools for protecting public safety. There are new technologies to help law enforcement overcome a range of challenges, but each comes with its own ethical considerations; inappropriate use can lead to privacy or human rights violations.

Chapter 7 concludes by outlining the Panel's reflections on the key issues raised in the report and emphasizes the importance of accountable, human-centric and trauma-informed approaches to addressing cyber-enabled crimes and harms.

2

Digital Technology, Privacy, and Security

Chapter Findings

- ICTs are ubiquitous. Many essential services have a digital component, making everyone digital-by-default, even if they are rarely online. Thus, issues related to privacy and digital security affect the application of the Charter and the human rights of everyone in Canada.
- Adoption of ICTs can amplify the complicated interplay among privacy and digital security, personal and associational freedoms, and security in other online contexts. Privacy and security tools do not have to be at odds with each other and can be mutually reinforcing.
- The expanding ways that public and private organizations collect, use, and disclose data necessitate reforming and strengthening the existing legislation meant to protect personal information and govern its management in Canada.
- Privacy is contextual and based on relationships; individuals and communities require the ability to make informed decisions about their online privacy.

It is important to consider which aspects of a person's wellbeing are at risk of being compromised by cyber-enabled harms. This chapter lays the foundation needed to address the charge. It contextualizes the relationship among digital technologies, privacy, security, and human rights, and examines how these values may be violated not only when we are exposed to cyber-enabled harms, but also when the tools and measures used to prevent them are applied inappropriately. The chapter unpacks this complex relationship, which can often impose a series of conditions that beg to be considered during the process of enacting laws, policies, or regulations intended to mitigate or prevent cyber-enabled harms. In doing so, it addresses the potentially complementary relationship between privacy and security, explores how individual and collective privacy and security interests relate to human rights, and describes some ways in which technology has affected society's contemporary understanding of these concepts.

The chapter begins by introducing privacy as a human right that is contextual and defined by the control and flow of information and data related to individuals and their communities. Privacy is then linked to security, emphasizing how privacy and data security can be mutually reinforcing. Finally, these concepts are used to introduce some of the general challenges encountered in the design and enforcement of privacy and security regulations, such as keeping up with or

anticipating technological changes, ensuring corporate and private entities respect user privacy and security (and are held accountable for breaches of trust), and cooperating across borders with respect to regulation and enforcement.

2.1 Privacy, Human Rights, and Digital Public Safety

2.1.1 Merging the Digital and Physical Worlds

Online capabilities have developed rapidly and must be considered an extension of the physical world

Digital technologies permeate nearly every aspect of modern life. Health, family, finance, education, and romance — to name a few — are all affected by and constantly adapting to evolving digital spaces. Connectivity is increasingly necessary for accessing essential services such as education and healthcare, participating in the labour market, shopping, and maintaining social connections (CCA, 2021; StatCan, 2021a). In the past, the digital world was limited to anonymous message boards and basic data sharing, and it was largely separate from everyday life. Today, the digital world is practically inseparable from the physical world such that the division has become vestigial (Dubois & Martin-Bariteau, 2020a), making it possible for anyone to fall victim to the kinds of cyber-enabled crimes and harms discussed in this report.

Design choices made during the birth of the internet have had an enormous impact on modern life and the nature of online harms

The internet was founded on principles of the free flow of information and the decentralization of control (Krasodomski-Jones, 2021), but these principles have had unforeseen consequences. As the inventor of the internet, Tim Berners-Lee, wrote on the 30th anniversary of the technology:

> *I had hoped that 30 years from its creation, we would be using the web foremost for the purpose of serving humanity [...] However, the reality is much more complex. Communities are being ripped apart as prejudice, hate, and disinformation are peddled online. Scammers use the web to steal identities, stalkers use it to harass and intimidate their victims, and bad actors subvert democracy using clever digital tactics.*
>
> Berners-Lee (2019)

With the help of information and communication technologies (ICTs), many contemporary societies have become social and connected in ways that have significantly changed how their members perceive privacy and security. Increased connectedness has also revealed that the meaning and importance of privacy and

security vary — often depending on personal and societal values (Bambauer, 2013). For instance, in Canadian society, privacy and security are often cast as being in opposition to one another, insofar as security requires intrusive surveillance of individuals, and data protection and privacy require limiting access to data. This chapter instead describes the two concepts as often being complementary, and notes that the degradation of privacy in favour of security can have counter-productive consequences.

Because of the dynamic nature of these issues, debates surrounding the definition of *privacy* and its limits can be contentious among scholars (e.g., Etzioni, 2005; Bailey, 2008; Solove, 2008; Kerr & Barrigar, 2012; Krishnamurthy *et al.*, 2021), legislators (Sections 5.2 and 5.4), and the courts (e.g., SCC, 2014a, 2016a, 2021). Managing one's privacy and digital security is increasingly complicated as people live more of their lives online. The amount and types of online information shared about any given person have grown rapidly, become more difficult to manage, and can be highly sensitive. Therefore, any new security apparatus must be weighed carefully, with the acknowledgement that privacy benefits may come at the cost of freedoms, anonymity, or security in other areas (Landau, 2011; Hartzog, 2018). Moreover, as international entities (including private companies) set out to collect massive amounts of user data, these calculated infringements must be considered in a rapidly changing global context (Hartzog, 2018; Farrell & Newman, 2019).

2.1.2 Understanding Privacy

Privacy is an individual right and a collective social value

The concept of privacy often captures several rights and freedoms, such as freedom of thought, freedom of choice over one's body, freedom from surveillance, and freedom to control information about oneself (Solove, 2002, 2015; Cockfield, 2007; Bernier, 2012). Conceptions of privacy are also dynamic, rooted in a state's history, and have evolved over time (Hartzog, 2018). Personal privacy (especially privacy from non-government entities) is arguably a relatively new development that requires more protections as technology creates multiple opportunities for that privacy to be compromised (Becker, 2019). It is worth noting that, while this chapter focuses on how digital technologies can influence the way an individual experiences privacy and security, there are collective dimensions of privacy and security that can be considered, as well (Thompson & Lyon, 2021).

Contemporary debates on privacy have centred on understandings of individual rights, such as "the right of individuals to have their *own domain*, separated from the public" (Becker, 2019). Importantly, privacy is a recognized human right (Scassa, 2020), and one that "enables the enjoyment of other rights: the free development and expression of an individual's personality, identity and beliefs,

and their ability to participate in political, economic, social and cultural life" (OHCHR, 2021). Privacy can also be understood as a collective social value that enables "democratic values that are critical to the promotion of long term security" (Cockfield, 2007). In 2021, the Supreme Court of Canada wrote, in *Sherman Estate v. Donovan*, that, "[al]though an individual's privacy will be pre-eminently important to that individual, the protection of privacy is also in the interest of society as a whole. Privacy therefore cannot be rejected as a mere personal concern: some personal concerns relating to privacy overlap with public interests" (SCC, 2021). The court went on to concede that "privacy is a complex and contextual concept, making it difficult for courts to measure" (SCC, 2021). In some cases, it may be determined that the security of a societal group may supersede individual or collective privacy considerations. For example, bulk data collection and mass surveillance can be useful techniques in a national security context but may negatively affect the public good if they compromise the kind of collective privacy expected within a democratic state (Thompson & Lyon, 2021). However, this discussion falls outside of the scope of this report.

2.1.3 Privacy and Data Security

Data security can be considered a fundamental human right, or the result of the right to privacy

Limits to privacy can be fluid or unclear; sometimes the law determines that individual privacy should be subject to reasonable limitations in the service of other interests, such as the need for certain forms of security (Cockfield, 2007; Kerr & McGill, 2007; Chandler, 2009; Aquilina, 2010). Making informed decisions about online privacy, however, requires an understanding of how privacy relates to personal data.

Conceptions of privacy and security are not static across time and jurisdictions. Governments and organizations have their own various ideas about privacy, security, and how to protect them, and they have had to adapt alongside ICTs in order to address the volume of personal and public data accessible (and indeed collected) online. For example, both Canada and the European Union recognize that privacy is a human right but differ in how data security is protected. The E.U. approaches privacy and data protection (which includes data security) as separate but overlapping rights; this is reflected in section 8 of the *Charter of Fundamental Rights of the European Union*, and it is comparable to the protection of personal privacy outlined in the *Universal Declaration of Human Rights* (UDHR) and *International Covenant on Civil and Political Rights* (ICCPR) (OPC, 2021a) (Box 2.1). In a 2020–21 annual report, Canada's Office of the Privacy Commissioner identified the E.U. approach as an important influence in Canada (OPC, 2021a); this

understanding can colour the application of tools such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to cases of data protection, but data protection as a human right is not an explicit feature of Canadian legislation (Bygrave, 2010).

Privacy is contextual, relational, and includes consensual data sharing

The practice of collecting personal data by private and public entities has led to privacy and security being described as social constructions capable of adapting, contextually, in response to people's relationships with other entities (Steeves, 2009). Privacy, then, requires an understanding of the interactions among those who are either expecting or respecting privacy — a relationship that Steeves (2009) notes is constantly changing and up for negotiation. Privacy norms allow us to control social identity — the self that is presented to the world — but technological advancements, such as big data analytics, endanger this control (Austin, 2012) (Box 2.1).

Box 2.1 Controlling Personal Data and the Right to Self-Determination

Evidence-based policy is informed by data, but the data collected (and, notably, not collected) can disproportionately affect the way certain communities are seen by the state. For example, Walter *et al.* (2020) explain that "for Indigenous Peoples, the slice of our social and cultural realities represented in data collected about us is limited to those aspects of interest to the nation state." Walter adds that "the specific and limited slice of Indigenous life of interest to the state is heavily implicated in the how and why Indigenous policy continues to go dangerously awry. These data are the support system of the long history of failed policy schemes that attempt to 'remake native societies.'" *The United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP), an international human rights instrument officially signed by Canada in 2016 and made law in 2021, is consistent with the Indigenous Data Sovereignty movement that seeks to give Indigenous communities the ability to mould certain policy decisions to their benefit — a privacy principle that underscores the community-shaping power and control of data collected about them (UN, 2007; Kukutai & Taylor, 2016; Duncanson *et al.*, 2021; Lukings & Lashkari, 2022a).

(Continues)

(Continued)

As a signatory of the UDHR and ICCPR, Canada has agreed that legal protection of one's privacy is a human right (UN, 1948, 1966; GC, 2019a). These protections can be discussed in a personal context (e.g., we have the ability to develop and express our personality, identity and beliefs without interference) or a social context (e.g., the protection of a societal structure that values such individual freedoms). In either case, and given the constantly evolving ways personal information and data can be collected digitally, interpreting these rights and providing these protections together form an ever-moving target (Kukutai & Taylor, 2016; Walter *et al.*, 2020; Duncanson *et al.*, 2021).

The concept of *contextual integrity* developed by Nissenbaum (2010) describes the relationship between privacy and society in further detail while considering social structures and values. One's social context (determined by politics, education, healthcare, and other factors) may determine expectations of privacy, and these norms are further influenced by geographic, historical, and cultural contexts. The author notes that, when considering privacy protection in the digital age, "what people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*" (Nissenbaum, 2010). This does not amount to a forfeiture of privacy, but rather a reasonable expectation that individual privacy will be protected.

Summarizing several privacy theorists, Bambauer (2013) writes that privacy in the digital age "is no longer about a binary division between data revealed and data concealed. It is about competing claims to information." In other words, the question rests on which actors should be allowed to use data, and why those actors (and not others, particularly in racialized and marginalized communities) are afforded this power (Bambauer, 2013; Walter *et al.*, 2020). The issue of privacy in the digital age is about more than control over the collection of information; it is also about "the process by which the information is collected, processed, and used — a process which itself is out of control" (Solove, 2002). The problem of privacy resides in the aggregation of data, the lack of meaningful regulation of those data, and control over how one's data are used (Solove, 2002).

Waldman (2018) expands on this concept within the context of information privacy, which "is not about excluding others, but rather about regulating the flow of information to some, restricting it from some, and opening it up to others." The author builds on the work of Nissenbaum by noting the importance of trust in enacting disclosure among individuals, and between users and their platforms, and by suggesting that trust in a system of privacy needs to be "administrable"

and "capable of being applied by lawyers and judges in real cases to answer real information privacy questions." In this context, privacy is about creating a relationship that allows for one to comfortably disclose (Waldman, 2018). In this sense, securing personal information and data can be understood as components of protecting one's privacy.

Privacy considerations change for victims and survivors of privacy-compromising harms

Privacy is nuanced and contextual, taking on different dimensions once it has been lost. Victims and survivors of harms such as non-consensual sharing of intimate images, child sexual abuse material (CSAM), and other forms of abuse are forced to contend with different privacy considerations than those whose privacy has not yet been compromised. In particular, regaining one's privacy may become a top priority for those who are harmed, despite it being difficult, if not impossible, to attain. This aspect of privacy is discussed in more detail in Chapter 3, particularly in the context of the removal and de-indexing of information that breaches privacy and other trauma-informed approaches to remedies.

2.2 The Nature of Security in the Digital Age

2.2.1 Privacy v. Security: A False Dichotomy

Digital security sometimes comes at the cost of privacy, personal and associational freedoms, and security in other areas

With new digital technologies come new threats, and as online capabilities grow, so too must security infrastructure. One person's phone can contain a wealth of data, including personal emails, financial information, login credentials, and access to business accounts (Bohannon, 2018). The sensitive nature of much of these data means they must be kept secure from online hacking, but the mobility of smartphones also makes them easy targets for theft. Because of this, developers are working to make these devices impenetrable, in order to reduce the risk of personal or identifying data becoming compromised in the event of theft. However, this type of data security creates challenges for law enforcement agencies when potential evidence is inaccessible (Landau, 2017) (Section 6.3). As a result, the Panel concludes that *security* can be thought of in terms of power — who can do what, on what terms, with a particular device, system, or piece of infrastructure. Technology aimed at enhancing security shifts where this power lies, making it crucial that changes resulting from the adoption of new technology be considered in terms of social acceptability, ethics, and with the understanding that individuals may have different perceptions of privacy and security.

2.2.2 Bulk Data Collection and Surveillance

Both surveillance and bulk data collection can compromise privacy, security, and safety

Technology also provides an unprecedented ability to collect, transfer, and store data. This ability gives institutions of all types (e.g., security, corporate, political) the power to surveil and profile individuals or specific groups, often without the individuals' or groups' knowledge (Alexander, 2015; Becker, 2019). Data collection for the purpose of surveillance — by law enforcement or government organizations — is a privacy and human rights concern, particularly when there is little transparency or oversight in the process (Robertson *et al.*, 2020).

However, this is not the only concern about online data collection. In addition to surveillance, data-driven profiling has the capacity to influence individual decision-making — for instance, through targeted advertising, which in part drives the estimated US$200 billion industry of data brokerage that commodifies personal data (Harris, 2017; Becker, 2019; McClelland, 2021). At the same time, the bulk collection and aggregation of citizens' data present security risks, even if a company adheres to acceptable and/or industry-standard security practices. Corporate security breaches (e.g., through malware, espionage, ransomware) represent not only a financial attack on a company but also compromise the privacy and security of its customers (Canadian Centre for Cyber Security, 2021b; The Canadian Press, 2021). The Canadian Centre for Cyber Security (2021b) explains that "an increasingly common tactic by ransomware operators is to publicly release a victim's data if they do not pay the ransom." While the number of such attacks is difficult to measure, the Canadian Centre for Cyber Security (2022a) states that "ransomware almost certainly has more impact on Canadian organizations [in 2022] than it did in 2020." Alternatively, data are sometimes stolen and released publicly by hackers, then used by others to blackmail and extort victims, as was the case in 2015 when the romantic affair dating service Ashley Madison was breached (Doffman, 2020). In another example, 520 patients of Ireland's Health Service Executive had their data leaked online in 2021 following a ransomware attack, which caused significant disruptions to vital patient services (Gallagher, 2021; McNamee, 2021) (Narrative 1).

Narrative 1 Ransomware and Collateral Harm in Ireland, 2021

Ransomware attacks often target companies and organizations with access to large sums of money, but the disruptions and resulting harms of an attack can also be felt by individuals. When Conti, a Russian-based ransomware group, targeted Ireland's healthcare services in 2021, it succeeded in encrypting important data that would force services to cancel up to 80% of their appointments. The attack cut access to important data and devices across the health system's network, impacting nearly every part of the Irish healthcare system and forcing staff to find ways to adapt.

One of those cancelled appointments affected Donna-Marie Cullen, who, on the day of the attack, was awaiting radiation treatment for an aggressive and deadly form of brain cancer. Fortunately, another oncology unit was able to separate its machinery from the rest of the system and, after several days of reworking Ms. Cullen's treatment plan for the new machine, that unit was able to resume her treatment. Though most services were restored after about a week (once the encryption key was obtained), disruptions persisted long after, particularly in oncology units and other areas heavily reliant on data processing and computational techniques.

(McNamee, 2021)

2.2.3 Human Rights and Algorithm-Based Tools

Data used out of context can create problems for privacy, human rights, and civil liberties

Predictive and algorithmic systems and services have been developed with the goal of using large collections of data to identify or respond to unlawful behaviour (Thompson & Lyon, 2021). However, "without human involvement in the process of data analysis, the likelihood of successful utilization of big data for security intelligence and surveillance will remain slim. The focus on algorithms and machines precisely takes attention away from the crucial matters of context" (Thompson & Lyon, 2021). Accordingly, the value of big data may only be fully realized through the appropriate human intelligence required to contextualize it (Van Puyvelde *et al.*, 2017; Thompson & Lyon, 2021). This does not mean that human intervention is sufficient to mitigate bias (Završnik, 2020), nor does it address people's unconscious biases. Every step of an algorithmic

decision-making process can introduce bias, including data collection, data preparation (i.e., which data are used or excluded), algorithm design, and implementation. Within such a complicated system, it may not be possible to identify where in the loop human decision-making would help, if it can at all (Završnik, 2020).

As promising as big data techniques seem, they depend on the input data, which may be biased, of questionable quality, or intentionally compromised (Robertson *et al.*, 2020; Bull, 2021). Considering the importance of some of the issues these techniques have been used to address (e.g., biases in policing), uncertainties about the way big data algorithms produce results remain the focus of much research (Ridgeway, 2018; Robertson *et al.*, 2020) and have led to calls for governments to restrict their use in law enforcement, immigration, and other security-related activities (Robertson *et al.*, 2020). Importantly, it is not only the political and societal climate into which these technologies are released that determines the way they will advance or hinder human rights, privacy, and security, but also their intrinsic designs (Winner, 1980; Starr, 2005).

What may be considered acceptable limits to privacy and surveillance are contextual and evolving

An essential question governing digital public safety is, to what extent can or should human rights, including the right to privacy, be supplanted by security needs? This is not a question with easy answers, because it depends on several factors, which can include (but are not limited to) one's personal security needs, ideology, social position, or cultural and historical context (Bellman *et al.*, 2004; Nordal, 2013; Igo, 2018). While various technologies are already used in monitoring, investigating, and prosecuting crime, debates continue on the limits to their use when that use conflicts with privacy, associational, religious, or other Charter-protected rights (Lucock & Black, 2009; Robertson *et al.*, 2020). For example, how effective must a particular technology be to justify its use, let alone its development in the first place? Alternatively, can the effectiveness and ease of use of a technique lead to excessively invasive practices? Proactive spam and phishing detection by email services, for example, has been used for many years with minimal concern over privacy. That said, an automated CSAM filter system proposed by Apple in 2021 to scan photos on iPhones and the iCloud was met with concern over possibly undermining Apple's end-to-end encryption (Porter, 2021).

Another consideration related to the adoption of new digital tools is how they compare to their analogue equivalents. For instance, improved digital technologies have drastically affected law enforcement agencies' surveillance capabilities. Bankston and Soltani (2014) estimate that the cost of tracking a

suspect via traditional covert pursuit is almost 30 times more expensive than tracking them with a GPS device. If a smartphone is used for tracking, covert pursuit is more than 50 times the cost. While technological progress has enabled law enforcement to track suspects more easily and effectively, it "poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" (Posner, 2007). Moreover, to what degree should law enforcement be held accountable when using a particular technology to monitor and surveil? For what purpose, and for how long, should the retention of personal data be allowed? Are people able to determine an acceptable level of security for themselves that satisfies their need for privacy and online safety, while also protecting their civil liberties (Van Puyvelde *et al.*, 2017; Ferguson *et al.*, 2020)? These are not philosophical "what-ifs?" but contemporary and practical considerations for law enforcement, and they are deeply linked to contestations on the appropriate extent to which state power can be exercised to intrude upon private and public life.

2.3 Regulation in the Context of Privacy, Security, and Human Rights

2.3.1 Privacy Is a National Concern

Despite existing governance tools, many people in Canada have privacy concerns

Privacy is an issue of concern for many people across Canada, despite the regulations currently in place. For example, a 2018–19 survey by the Office of the Privacy Commissioner found that 92% of respondents had some level of concern over the protection of their privacy compared to 88% of respondents in 2012; notably, the number of respondents who claimed to be "extremely concerned" rose from 25% in 2012 to 37% in 2018 (OPC, 2019a). Others have expressed concerns over whether the government itself can be relied on to protect privacy rights, especially when government security apparatuses can benefit from surveillance activities by, for example, having easier access to large volumes of information deemed necessary for meeting certain objectives, such as fighting crime or terrorism (Alexander, 2015; Talbot, 2021).

2.3.2 Privacy Regulation in Canada

Privacy in Canada is regulated by multiple orders of government, with approaches that differ among provinces and territories

In Canada, the right to privacy is protected, among others, under Section 8 of the *Charter of Rights and Freedoms*, the *Privacy Act*, and PIPEDA (GC, 1982, 1985, 2000a,

2020a; OPC, 2019b) (Section 5.1). In addition, each province and territory may address privacy through its own statutes applicable to public and private sector, as well as through common or civil law (OPC, 2018; GC, 2021a) (Chapter 5). Though it can be useful to consider privacy and data security within a human rights framework, much of the large-scale data collection and surveillance being undertaken are done by private companies and online platforms that are not beholden to documents such as the UDHR and ICCPR, but rather privacy legislation (which, for Canada, includes PIPEDA) (GC, 2000a, 2020a; Hartzog, 2018; OPC, 2019b). Despite these laws, the Citizens' Assembly on Democratic Expression is concerned that the right to *not* be subject to surveillance without due cause has been inadequately addressed in the design of digital platforms (CCADE, 2021).

PIPEDA regulates the relationship between businesses and individuals, and was not designed to protect privacy as a human right

PIPEDA, which was passed in 2000, was developed at a time when 51% of households in Canada had at least one member who was a regular user of the internet (StatCan, 2001), and before the popularization of social media and online marketing. In the years since PIPEDA was passed, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) has held hearings on how privacy laws relate to a variety of new, emerging, and otherwise hard-to-predict social and technological advances. Scassa (2020) identifies PIPEDA as relying too strongly on individual consent, which is often presented in challenging language and requested frequently enough that many users are unable to truly give informed consent. Privacy advocates have also argued that PIPEDA lacks adequate enforcement (Section 5.1.4) and does not generally address collective dimensions of privacy (Scassa, 2020).

The *United Nations Guiding Principles on Business and Human Rights* (UNGP) is an instrument meant to help address this issue by ensuring business activities do not interfere with human rights (UN HRC, 2011b). The UNGP has faced criticism for failing to hold businesses legally accountable, and "for setting a lower bar than international human rights standards in some areas, like ensuring a victim's right to redress" (Albin-Lackey, 2013). To address the issue of cyber-enabled harms, private companies are often subject to government-imposed requirements, such as reporting harmful or illegal activities occurring on their platform to law enforcement, or taking down harmful material in a timely manner (Chapter 5). These requirements complicate the relationship between government and private companies (Ferguson, 2017; Landau, 2017). Platform accountability also becomes an issue when platforms are transnational, requiring agreements brokered between foreign governments and private companies (Box 2.2).

Box 2.2 Private Companies as New Governors

Enormous amounts of personal data are collected by private companies, many of which operate internationally. Ensuring data security requires the efforts and cooperation of governments and their regulatory bodies, law enforcement, corporations, and citizens. Some argue that the regulations that apply to the largest digital companies, such as Meta, the parent company of Facebook, and Twitter, are best considered from a perspective of "private governance and self-regulation." Platforms in many cases develop their own features akin to a form of state governance, including a central governing body, policies and rules based on democratic values that can be used to adjudicate improper behaviour on the platform, and ways of amending and updating these rules. It has also been suggested that *governance* is indeed the best way to capture the idea of how much power these platforms have to shape international laws and regulations, dubbing them *New Governors* of our digital age. This view of the internet differs from its original conception as a decentralized online democracy. Now these New Governors form an additional layer of governance that sits between the state and its citizens. This represents an unprecedented shift in global power, one that has enormous repercussions for the digital safety and security of people in Canada.

(Klonick, 2018)

Like PIPEDA, the federal *Privacy Act*, which is administered by the Privacy Commissioner of Canada, sets out rules for how the government handles data and privacy, and has undergone review in recent years with an eye to the E.U.'s *General Data Protection Regulation* (GDPR) (Scassa, 2020). It has been suggested by Therrien (2021a) and others that the Canadian *Competition A*ct be examined and reformed together with the *Privacy Act* to better address the impacts of *platform* and *surveillance capitalism* on users' data security and privacy (Qarri, 2022). The argument essentially mirrors the effect of competition on consumer pricing; as market dominance (or monopoly) reduces market competition, consumers are left with few if any suitable alternatives, allowing for increased prices for a potentially inferior product or service (Therrien, 2021a; Qarri, 2022). In the case of online platforms that collect and monetize user data, an inferior product or service could include lower-quality privacy practices; notably, both effects can be at play simultaneously (Qarri, 2022). Article 20 of the GDPR requires data portability, and additional controls have been proposed, including platform interoperability (e.g., being able to send direct messages across different platforms) such that users are not locked into specific services to communicate

with their personal networks (De Hert *et al.*; OECD, 2021). Proponents argue that these features may foster competition that could empower users to influence the way their privacy and data security are handled through market pressure (Qarri, 2022) (Section 5.2). Those on the other side of the interoperability debate, however, point to the success of Apple as an end-to-end hardware and software company, as well as potential new privacy risks at the seams between different platforms (Graves, 2021).

2.3.3 Difficulties with Digital Regulation

The speed of technological change and adoption makes it difficult to regulate digital spaces

The speed of technological change means that questions of privacy and security are constantly evolving. Law enforcement agencies, as an example, may be pressed to creatively interpret law in order to justify the adoption of certain techniques or technologies, or to access classes of information that did not exist when enabling legislation was passed into law (Brownsword, 2008). This can establish a *regulatory disconnection*, insofar as technology has outgrown its relevant legal framework. Correcting this disconnection and passing laws that predict the future or technology-neutral laws can be difficult (Brownsword, 2008). For example, language being adaptable to different technologies does not mean the effect of those laws will be the same, nor is it always possible to ensure that adaptable language does not provide advantages (or disadvantages) to specific technologies or platforms (Reed, 2007). Moreover, laws relating to technology often take years to pass and may no longer be relevant once they enter into force (Alexander, 2015). Rushed laws may have unintended consequences (Box 2.3).
In the absence of strong guidance from legislatures or the courts, law enforcement agencies may choose to intrude into individuals' Charter-protected rights in unexpected ways, with the effect that good-faith attempts to safeguard public order can be accompanied by violations that are poorly received by the wider public (Parsons & Molnar, 2018).

Box 2.3 SESTA, FOSTA, and Sex Trafficking in the United States

In 2018, the United States passed the Stop Enabling Sex Traffickers Act (SESTA) and the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) (Gov. of the US, 2018). The intent of this legislation was to curb sex trafficking by criminalizing the online platforms used to advertise the sale of sex (NSWP, 2018). However, much like an 1873 effort by the U.S. Postal Service to suppress the spread of "immoral material" (resulting in the seizure of anatomy textbooks and reproductive health materials in addition to pornography), the legislation suffered from broad language and did not distinguish between trafficked and consensual sex workers (Romano, 2018; Tworek, 2021a).

While the law compelled many U.S.-based websites to monitor and remove sexual content, it also created dangers for consensual sex workers who relied on online platforms to screen potential clients and share information with other industry workers about potentially dangerous or problematic individuals (NSWP, 2018; Misitzis, 2021). Many workers had to return to the streets to attract clients (Williams, 2017; Misitzis, 2021). This came as no surprise to many sex-worker advocacy groups, which noted the predictable consequences of broad statutory language (Harmon, 2017). Unfortunately, while the impacts of SESTA and FOSTA on consensual sex workers have been well documented, it remains unknown whether these laws have lowered incidences of sex trafficking (Misitzis, 2021).

The decentralized nature of the internet poses privacy-related regulatory interdependencies and challenges

Perhaps anticipated by the early formation of collaborative state intelligence agencies such as The Five Eyes (Australia, Canada, New Zealand, United Kingdom, and United States),[4] it has become evident that democratic states can no longer determine how the privacy of their citizens' data is defined in isolation; it has necessarily become a global issue, one that has grown to include the influence of private, often international corporations (Hartzog, 2018; Farrell & Newman, 2019). Bennett and Raab (2018) argue that this interdependency can create two possible scenarios: (i) nations participating in a "race to the top" as they look for solutions

4 "The Five Eyes is an intelligence alliance [of] partner countries [that] share a broad range of intelligence with one another in one of the world's most unified multilateral arrangements" (PS, 2021b).

to safeguard the privacy of citizens, or (ii) nations participating in a "race to the bottom," where regulation is abandoned in favour of attracting companies.

In an alternative framework, Aaronson and Leblond (2018) suggest that, because of the free and wide flow of personal data across borders, states' policies may develop within data policy *realms* — virtual jurisdictions defined by their approaches to "tax, transparency, intellectual property protection, competition, and data protection policies among others." The major international players that appear to define these realms are the United States, the European Union, and China (Aaronson & Leblond, 2018), as well as the United Kingdom.

Despite the breadth of actors, one principle largely agreed upon, which features in many privacy and security frameworks, is *transparency* (Colliver *et al.*, 2021). Tworek and Wanless (2022) argue that what exactly constitutes transparency remains an open question. It is therefore important that proposed transparency frameworks be specific about what categories of information should be reported and who should have access to this information. Two concepts proposed as foundational to transparency practices (described in the context of corporate surveillance transparency reporting, though perhaps applicable more widely) are *verifiable* practices and *performative* practices; the former are described as ones that release the appropriate information to the right audiences, while the latter are ones that develop and prove an internal culture of transparency (however, it is also noted that more information does not necessarily translate to better online conduct) (Albu & Flyverbom, 2016; Ballard & Parsons, 2022). Ballard and Parsons (2022) further note that, "while these conceptualisations can be contrasted against one another, they can potentially both be integrated into transparency reporting documents such that reports can both satisfy conditions of verifiability and performativity alike." In other words, transparency practices that are both verifiable and performative require the release of useful, relevant, and pertinent information in a perpetual, dynamic, and adaptable way.

2.4 Summary

Privacy, security, and human rights play integral roles in the contemporary debates surrounding online harms, and how to best prevent and mitigate those harms. Understanding the relationship among cyber-enabled harms, privacy, and data security is essential to answering all elements of the charge, including the specific ways in which new digital technologies are being used to perpetrate cyber-enabled harms, as well as options for helping address these harms.

As outlined in this chapter, the following framework is worth considering when assessing Canada's privacy and data security laws: (i) the wide incorporation of ICTs into everyday life makes everyone *digital-by-default* and at risk of falling victim to cyber-enabled harms; (ii) privacy is contextual and relationship-based, and conditions for the use of data collected from individuals and communities hinge on consent and transparency; (iii) the power to control access to, and the collection and use of, an individual's or community's data are critical to securing (or infringing on) personal and collective privacy and security; and (iv) privacy and data security are considered human rights in certain foreign jurisdictions.

ICTs have become an indispensable part of modern life but, as suggested in the charge, they have also profoundly changed the way serious criminal activities are committed and facilitate a range of online harms. Their utility, widespread adoption, and potential for causing harm have forced regulators, policy-makers, researchers, and the public to adopt increasingly nuanced understandings of what is meant by *security* and *privacy*, and of how security and privacy play roles in mitigating or preventing cyber-enabled harms. The ability to create, disseminate, or store large amounts of information over the internet can make many services more functional while, simultaneously, generating a host of privacy and security concerns associated with the protection of people's information.

Subsequent chapters in this report consider the tensions among privacy, security, and different aspects of cyber-enabled harms. The Panel will go on to describe how cyber-enabled harms are facilitated by digital technologies while making clear these acts exist on a spectrum of illegality, often target specific demographics, and are not always best addressed through criminalization (Chapter 3). The Panel then considers some of the digital technologies that enable these harms, with an emphasis on the fact that, while the technologies are generally legal, their decentralized, distributed, and often anonymous nature presents significant regulatory and enforcement challenges when used for harmful acts (Chapter 4). These harms can potentially be addressed by regulatory (Chapter 5) or enforcement (Chapter 6) tools and activities, though each faces its own respective challenges resulting from the contemporary digital environment within which people in Canada live.

3

Digital Technologies and Harms

Chapter Findings

- Online harms occur on a spectrum of legality and criminality ranging from criminal offences that may have a high bar for prosecution to those that are harmful but lawful.
- ICTs impair public safety when individuals use them to facilitate harmful acts. They can be used to spread harmful content across online environments that have uneven or ineffective moderation policies.
- Not everyone is equally at risk of experiencing harms online. Women and youth, as well as racialized and minoritized communities, are most commonly targets of harmful acts and content online.
- Criminalization is not always the most effective means of combatting online harms, nor is it victims' or survivors' preferred mitigation method in all cases.

While information and communication technologies (ICTs) provide multiple benefits to society, they can also offer new methods and pathways for individuals to engage in harmful behaviours, which complicates prevention, containment, and investigation efforts. At the same time, ICTs have altered conceptions of privacy (Chapter 2), and of how privacy is supported or hindered by measures to ensure security. In this chapter, the Panel reviews a range of harmful activities to highlight their greater effects on some people and communities, along with the importance of a multifaceted and contextualized approach to addressing online harms. This approach invokes both legal and non-legal avenues, as well as the experiences of victims and survivors, when it comes to choosing appropriate prevention, mitigation, and compensation measures.

The chapter begins by demonstrating how advances in ICTs can be used to facilitate the exploitation, harassment, and abuse of people, particularly women, children, and members of the LGBTIQ+ community. Some of these activities, such as the distribution of child sexual abuse material (CSAM) and non-consensual intimate content, are criminal offences. Some instances of online harassment can also be prosecuted under criminal law, while others are not considered criminal or even unlawful behaviour. Regardless of their legal status, many instances of online harassment cause psychological harm and have a chilling effect on victims. Overall, providing various types of support and legal help to victims and survivors of different forms of criminal and non-criminal cyber-abuse remains difficult due to a lack of resources and information for those targeted, regulatory gaps, and enforcement challenges.

This chapter then reviews how ICTs facilitate the dissemination of content related to racism, xenophobia, incitement to violence, terrorism, and hate propaganda. Although cyber-enabled hate and harassment have devastating psychological effects and can put people in harm's way offline, it can be challenging, in some cases, to pinpoint when hateful content becomes illegal and, therefore, subject to investigation, prosecution, and punishment by law enforcement agencies.

Finally, this chapter describes fraudulent practices facilitated by ICTs, such as extortion, identity fraud, and unlawful access to personal information. Although cyber-fraud is the most reported cybercrime, its true scale is unclear due to reporting barriers. Among different demographic groups, older adults, new immigrants, and youth are particularly vulnerable to various types of fraudulent practices, resulting in significant financial losses and psychological harm.

The Panel finds that, while legal reforms may be necessary in some cases (e.g., to limit the dissemination of deepfakes, discussed in Section 3.1.1), a suite of alternative prevention and mitigation tools led by different actors can also address harmful acts. Content moderation policies and community guidelines for service providers and social media platforms, fraud prevention tactics at big banks, and educational programs on issues related to cyber-bullying all play an important role in reducing online hate, fraud, and abuse. None of the existing approaches, however, fully address the problem of cyber-enabled harms. Improving digital public safety is a moving target that requires responsive approaches grounded in the challenges experienced by people living in Canada.

3.1 Digital Technologies and Exploitation, Harassment, and Abuse

The North American Cyber Classification Compendium (NACCC) (Section 1.3.2) includes a category capturing the "exploitation, harassment, or abuse of a person" (NACCC, 2021a). This category covers activities that are unequivocally illegal, such as the online exploitation of women and children (e.g., human trafficking, CSAM, distribution of non-consensual intimate content), as well as activities that are illegal if and when they meet certain criteria, including online harassment and abuse (e.g., cyber-bullying). While all types of harassment and abuse are harmful, criminalization is not always the most effective way of combatting them. In the following sections, the Panel outlines the legality of these acts where possible to inform new or promising practices.

3.1.1 Online Exploitation of Women and Children

Women and youth are over-represented as targets of online violence (Henry & Powell, 2016; Bailey *et al.*, 2017). The exploitation of women and children online includes activities ranging from human trafficking to publicizing non-consensual intimate content. While ICTs have changed the ways in which women and children are exploited, online violence is part of a continuum of gender-based and age-based violence in society at large (PHAC, 2019; Khoo, 2021).

ICTs facilitate the trafficking of women and children

Human trafficking is defined as the "recruitment, transportation, harbouring and/or exercising control, direction or influence over the movements of a person in order to exploit that person, typically through sexual exploitation or forced labour" (JUS, 2021). The trafficking of women and children is the world's fastest-growing criminal enterprise, accounting for an estimated US$99 billion in profit annually (Equality Now, 2019). Traffickers in Canada and elsewhere use the internet to post advertisements, market women and children through websites, connect with buyers, and enter chatrooms and other online venues to connect with potential victims (Equality Now, 2019; Baird *et al.*, 2020). Online marketplaces for renting temporary accommodation (e.g., Airbnb) can also facilitate human trafficking, as they enable greater renter anonymity, making it more difficult for the police to collect relevant information. They are also subject to fewer regulations and enforcement mechanisms than licensed facilities, such as hotels (Mcquigge, 2018; O'Regan, 2019; Binns & Kempf, 2021).

Women and girls represent 95% of all victims of sex trafficking in Canada, 43% of whom are between the ages of 18 and 24 years (Ibrahim, 2021). Besides gender and age, other risk factors common to trafficking victims include immigration status, experience in the child welfare system, financial or social instability, and Indigeneity (PS, 2021c). Indigenous women are routinely over-represented in the sex trade in Canada (NWAC, 2014), and studies show that their recruitment is increasingly facilitated through social media, including sites as common as Facebook (Louie, 2017). In interviews conducted by Louie (2017) in Alberta, it was found that Facebook was a primary tool used to recruit teenagers and young women from surrounding First Nations reserves and lure them to cities for the purpose of sexual exploitation. Following recruitment, Facebook and other social media applications were used to facilitate so-called "dates" and kept trafficked victims in constant communication with their exploiters. These actions undermined the safety of spaces open to at-risk youth, including on-reserve community and cultural centres and after-school programs.

The use of social media tools has made the task of identifying at-risk Indigenous girls and women increasingly difficult by hiding recruitment attempts from parents and educators (Louie, 2017). In addition, by moving the networks for trafficking off the streets and onto the internet, victims become less visible and more difficult for outreach workers or police officers to identify and assist. To combat the sexual exploitation of girls and women in First Nations communities, Louie (2017) highlights the importance of implementing early and holistic interventions that consider community needs and culture.

The internet allows for the wide dissemination of CSAM

ICTs have created opportunities for CSAM to be illegally shared more readily than was historically the case (Negreiro, 2020). Child sex offenders take advantage of digital technologies to communicate with other offenders around the world, as well as share images and information about luring children or hiding digital footprints (Negreiro, 2020). Offenders often find support and legitimatization for their activities and behaviours in online communities (Jeney, 2015). They also rely on ICTs to communicate with, and groom, potential victims, often using these communications to lure minors to in-person meetings or coerce them to perform sexually explicit acts online (UNODC, 2015; Negreiro, 2020).

While there is no definitive tally of the amount of CSAM that resides online (Edwards *et al.*, 2021), there is ample evidence suggesting that the distribution and circulation of ICTs have had corresponding effects on the creation and circulation of CSAM and on child exploitation more generally. The Internet Watch Foundation (IWF) found a 16% increase between 2019 and 2020 in the number of confirmed reports of CSAM online (IWF, 2020), and the Canadian Centre for Child Protection (C3P) reported a steady increase in the detection of CSAM targeted for removal between 2018 and 2020 (C3P, 2021). These increases may be linked, in part, to the COVID-19 pandemic, during which both sex offenders and children spent more time online (Negreiro, 2020; UN News, 2020; NCMEC, 2021). While the Dark Web (Chapter 4) has played a significant role in directing child sex offenders toward sites hosting CSAM, the majority of images detected by CSAM discovery program Project Arachnid (Box 6.1) were hosted on the Open Web, on platforms such as Twitter, Facebook, messaging apps, or image-bucket and file-storage websites (Kristof, 2020; C3P, 2021).

Girls are more likely to be impacted by the online exploitation of minors. A report by C3P demonstrated that 80% of tens of thousands of unique sexually exploitative or abusive images they assessed were of girls (C3P, 2016). Furthermore, 78% of the images were of children under the age of 12, with nearly 50% of those appearing to be under the age of 8. C3P suggests that the likely true extent of abuse committed against post-pubescent minors is not represented, because the technology and

database used to identify abuse skew toward younger victims, and because older victims are less likely to seek assistance due to fear, shame, or the possibility of having images of their abuse repeatedly viewed (C3P, 2021).

The removal of CSAM encounters obstacles in part because some service providers do not take certain content moderation measures to block illegal images when they are uploaded by users (C3P, 2021). In many cases, service providers oppose specific CSAM take-down requests because content moderators assume that materials depict an adult. This delays the removal of illegal content and allows it to spread (C3P, 2021). Some private companies have been introducing policies that limit access to and dissemination of CSAM. For example, in 2020, Visa, Mastercard, and Discover terminated the use of their cards on the Canadian-based website Pornhub, after investigations confirmed that many videos posted depicted the sexual assault of children (Goodwin, 2020; Kristof, 2020; Price, 2022). After the credit card companies cancelled their services, Pornhub banned unverified uploaders from posting new content and deleted at least 10 million videos posted by them (Kan, 2020). As such, private intervention caused meaningful changes to Pornhub's content moderation policy (Pornhub, 2020).

The distribution of non-consensual intimate content can lead to shame, anxiety, declining physical health, and damaged relationships

People may voluntarily produce and share intimate images of themselves. However, such intimate images can also be subsequently distributed on websites or social media without consent (Daswani & Pearson, 2014; Short *et al.*, 2017; Bothamley & Tully, 2018). In some cases, the distributed images are captured without the person's knowledge via hacking or surveillance videos (Citron & Franks, 2014; Henry & Powell, 2016; Short *et al.*, 2017). Such activities are sometimes referred to as *revenge porn*, though this is a misnomer, since reasons for distribution may extend beyond revenge to include blackmail, intimidation, and pleasure (Henry & Powell, 2016). Furthermore, the term can potentially minimize the harm caused to victims, since pornography is notoriously hard to define and may depend on the perspective of the person viewing the image (Henry & Powell, 2016).

While anyone can be a victim of the distribution of non-consensual intimate content, the crime is more likely to impact women and girls (Henry & Powell, 2016; Short *et al.*, 2017). Victims often report high levels of anxiety, shame, negative impacts to their physical health, as well as damage to their careers and relationships (Short *et al.*, 2017; Wells, 2019) (Narrative 2). There are thousands of websites devoted to the distribution of non-consensual intimate content — an estimated 2,000 in 2017 (Short *et al.*, 2017) — as well as a number of other

websites that, while not specifically created for the genre, may be co-opted for it (e.g., Pornhub). Many of these sites can cast a long-term shadow over victims and survivors, as digital imprints can remain online for an extended period and be downloaded and shared among multiple users and across platforms (Dodge, 2019).

Narrative 2 The Origin of Women Against Cyberrape

In 2010, Rebekah Wells was googling her name when she discovered an online gallery of her nude photos. The explicit photos, along with her address and contact information, had been posted by an ex-boyfriend without her knowledge or consent two years after their relationship ended. The photos appeared on a number of commercial pornography sites, where users left misogynistic comments under her photos. Some malicious users said they had downloaded the images, reminding Ms. Wells that her nude photos could never be fully removed from the internet.

Ms. Wells filed a report at her local police station and was eventually able to file a lawsuit against her ex-boyfriend, the hosting site, and Cloudflare, the proxy server that supported the hosting site. While the images were removed from the hosting site, they continued to emerge on other pornography sites. Ms. Wells suffered emotional, psychological, and physical stress. She was admitted to hospital for a year after losing over 20 pounds. In November 2012, Ms. Wells founded the organization Women Against Cyberrape (formerly Women Against Revenge Porn) to provide support for and guidance to other victims of this harm. Her experiences also motivated her to apply to law school in 2017, and she has since become a victim's rights attorney in Florida.

(Wells, 2019, n.d.-a,-b)

It remains difficult to legislate, detect, and prosecute the distribution of non-consensual intimate content

Legislation against the distribution of non-consensual intimate content is evolving. Canada developed laws that make the non-consensual distribution of intimate images illegal, regardless of the age of the individuals involved, under Section 162.1 of the *Criminal Code* (GC, 1985; Dodge & Spencer, 2018), while several provinces and territories have civil laws pertaining to non-consensual intimate content (Laidlaw & Young, 2020). Since their enactment, the number of reported cases in every province and territory has risen (Allen, 2019). However, in 2021,

only 17% of cases reported to police in Canada led to charges being laid (StatCan, 2022).

To better harmonize laws throughout Canada, Laidlaw and Young (2020) recommend the implementation of statutory laws that would fast-track proceedings intended to force a defendant or (more likely) third-party intermediary (e.g., Google) to remove violating content and de-index search results, as well as civil laws that would allow plaintiffs to access damages if clear evidence of harm is provided. However, as noted elsewhere in this report, even if a case is prosecuted in Canada, images may exist outside Canadian jurisdiction. The law may have limited power over countries hosting the sites and foreigners living abroad who are distributing the images (Henry & Powell, 2016).

To supplement legal avenues, some sites, such as OnlyFans, implemented additional checks for content creators, in order to ensure the platform does not offer services to, or collect personal data from, minors or people using a false identity. These checks involve requiring passport copies and selfies of creators holding their government-issued IDs and using facial analysis software to verify identity (OnlyFans, 2020). Pornhub implemented policies, enforcement, and moderation mechanisms (including digital tools) to report and remove non-consensual content (Pornhub, 2022), but many sites — especially ones devoted to non-consensual content — do not (Dodge, 2019).

Deepfake technology is used to create non-consensual intimate images and videos

Deepfake technology (Box 3.1) has value in some contexts for the production of movies and games, and also has applications for healthcare. Aside from any artistic or satirical merit this technology may have, the ease with which it can be used for harm has made the detection of deepfakes a high priority among government agencies (Chesney & Citron, 2019; Rao *et al.*, 2021). Early concerns over the use of deepfake technology focused on the risks it poses to democracy, political stability, celebrities, and politicians (Ajder *et al.*, 2019; Chesney & Citron, 2019). However, a report issued by DeepTrace — an industry leader in visual threat intelligence — concluded that, overwhelmingly, deepfake technology is being used to create non-consensual intimate images (Ajder *et al.*, 2019). Additionally, it was found that, across the top five most popular deepfake pornography websites, women were the exclusive targets (Ajder *et al.*, 2019).

Box 3.1 Deepfakes

Deepfakes are a type of synthetic media that use machine learning techniques to "merge, combine, replace and superimpose images and video clips" to create a seemingly authentic video or image of someone or something that is not real (Maras & Alexandrou, 2018). Software (e.g., Adobe After Effects) and open-source programs (e.g., Face Swap, DeepFaceLab, FakeApp) make it possible to produce realistic audio and video content, provided the creator has enough reference data to work with, such as still images, video clips, and voice samples (Maras & Alexandrou, 2018; Paris & Donovan, 2019).

Deepfake editing differs from traditional media editing and computer-generated imagery techniques in its use of deep-learning algorithms (Khoo *et al.*, 2021). These algorithms train the system to map one person's features onto another — typically by showing the program many hours of video of someone shot from various angles and under different lighting (Adee, 2020). Since the training process is often done autonomously, it is possible for developers to create programs that require little to no technical expertise to operate (Khoo *et al.*, 2021). In many cases, these programs are available for free on open-source software repositories such as GitHub, while users on forums such as Reddit can be available to help with troubleshooting (Tolosana *et al.*, 2020; Khoo *et al.*, 2021). Some deepfakes can be challenging to spot even using special software. The difficulty of detecting manipulations depends, among other things, on "the level of compression, image resolution, and the composition of the test set" (Bernaciak & Ross, 2022).

Most pornographic deepfakes employ techniques that take real media and alter it to represent information "not contained within the original data or not consistent with reality" (Khoo *et al.*, 2021). Image manipulation can take on several forms and be used to alter the identity of a person depicted in media (i.e., face-swapping), alter the attributes or characteristics of a person (e.g., skin colour, facial features), or change the facial expressions, facial movements, or speech of a person — in effect, putting words they never spoke into their mouth (Tolosana *et al.*, 2020).

With these techniques, an individual can realistically incorporate a victim's face and voice into compromising videos (Cook, 2019) as well as simulate the removal of their clothing with nothing more than an image or video of the subject (notably most app-based programs for generating non-consensual intimate content only works on female-presenting bodies) (Cook, 2021). Because images and videos of celebrities are widely accessible, deepfake pornography has predominately

targeted famous women. However, there are also reports of non-famous women and children suffering similar attacks, often in the context of blackmail or the distribution of non-consensual intimate content, or to otherwise humiliate or traumatize victims (MacDonald, 2021). The women whose bodies are featured in these videos are also victims on the basis that their depictions are being used in ways unknown to them and without their consent (Paris & Donovan, 2019; MacDonald, 2021).

There is a regulatory gap in combatting deepfake content

Current regulatory and legal tools in Canada and elsewhere are fragmented and ill-equipped to address harms associated with deepfakes (Chesney & Citron, 2019; Karasavva & Noorbhai, 2021). Some deepfake-related harms may be crimes if they involve online CSAM (Karasavva & Noorbhai, 2021), and Canada's *Criminal Code* does penalize the distribution of intimate images (including those by means of film or video recording) without a person's consent (GC, 2014). However, whether algorithmically synthesized deepfakes fall under this definition is open to interpretation (Karasavva & Noorbhai, 2021). Beyond criminal charges, copyright infringement and defamation laws can be applied to deepfake cases, each with its own limitations (Chesney & Citron, 2019; Karasavva & Noorbhai, 2021).

A complete ban on deepfakes may have negative unintended consequences given the beneficial applications of the technology (e.g., filmmaking), while also infringing on freedom of speech and expression (Chesney & Citron, 2019; Karasavva & Noorbhai, 2021). Karasavva and Noorbhai (2021) have suggested that the expansion of existing Canadian laws to include more specific language around falsely created intimate images and videos would be more appropriate. Chesney and Citron (2019) suggest making it easier for private citizens to sue platforms for disseminating harmful content uploaded by their users, in order to incentivize the swift removal of deepfake content. This approach may lead to the over-removal of some legal content, however (Chapter 5).

3.1.2 Online Harassment and Abuse

Online harassment and abuse take many forms, and they can target a collective (e.g., issuing broad hateful comments), individuals (e.g., cyber-stalking), or both (e.g., cyber-bullying). Harassment and abuse might be linked to personal relationships (e.g., divorces) or connected to broader social and cultural identities (e.g., race, gender, religion). As shown in this section, many instances of harmful online aggravation and annoyance are not considered criminal behaviour. The Panel uses the term *harassment* broadly to capture both criminal offences and non-criminal harmful acts. Determining whether an activity constitutes a

criminal offence is challenging, and criminalization is not necessarily the most effective or preferred avenue to address all online harms.

Cyber-harassment and online abuse are deemed criminal in some instances

Harassment, according to Canada's *Criminal Code*, refers to repeated behaviours that cause another person "reasonably, in all circumstances, to fear for their safety or the safety of anyone known to them" (GC, 1985). Cyber-bullying involves the use of ICTs to "bully, intimidate or harass others" (RCMP, 2021c). Some forms of cyber-harassment, cyber-stalking, and cyber-bullying are investigable and prosecutable under Section 264 of the *Criminal Code* if they are deemed criminal harassment or involve the uttering of threats (GC, 1985). Stalkerware applications are used to harass or intimidate victims, or to covertly monitor a victim's messages or online activity (Khoo *et al.*, 2019). These applications are widely available to consumers and can "enable real-time and remote access to text messages, emails, photos, videos, incoming and outgoing phone calls, GPS location, banking or other account passwords, social media accounts, and more" (Khoo *et al.*, 2019), which may constitute criminal offences under Canadian law (GC, 1985).

While cyber-harassment, cyber-stalking, and cyber-bullying take place online, either publicly (e.g., social media, blog posts) or on private channels (e.g., email, direct messaging), they often leave the digital realm and result in physical stalking and contact (Al-Khateeb *et al.*, 2017; Brown *et al.*, 2017). It is increasingly common, in fact, for digital technology to be used to facilitate offline crimes related to stalking or harassment. For example, readily available spyware can monitor a victim's physical movements (Khoo *et al.*, 2019).

Youth, women, and the LGBTIQ+ community are common targets of online harassment

A global survey of 14,000 girls and young women between the ages of 15 and 25, in 22 countries, found that 58% experienced some form of online harassment (Plan International, 2020a). The most common forms of reported harassment were abusive or insulting language (59%), purposeful embarrassment (41%), body shaming (39%), and threats of sexual violence (39%). In addition, 37% of girls who self-identified as being from an ethnic minority reported harassment because of that distinction, while 56% of those identifying as LGBTIQ+ reported abuse specifically related to that part of their identity. Overall, however, research on the relationship between cyber-victimization and LGBTIQ+ identity is limited (Abreu & Kenny, 2018). Online abuse occurred on every major platform, with surveyed respondents reporting the most abuse on Facebook (39%) (Plan International, 2020a).

Women are also disproportionately targeted by the use of spyware and malware; these tools are often used in the context of intimate partner violence, harassment, and abuse (Shahani, 2014; Siminovic, 2017; Khoo *et al.*, 2019) and the overlap between physical stalking and cyber-stalking is especially pronounced among women; for many, cyber-stalking is a facet or extension of their offline domestic abuse (Nobles *et al.*, 2014; Henry & Powell, 2016; Al-Khateeb *et al.*, 2017).

There is evidence that youth, women, and members of the LGBTIQ+ community in Canada are especially vulnerable to cyber-bullying and online harassment, and that such actions can result in significant psychological and physical harms (Hango, 2016; Broll *et al.*, 2018; Lam *et al.*, 2019). For example, 17% of Canadian youth (ages 15–29) who used the internet between 2009 and 2014 experienced cyber-bullying or cyber-stalking (Hango, 2016). These incidents are typically sustained attacks rather than one-time occurrences. One youth survey found that, for 65% of the youth who had been cyber-bullied in the last month, their victimization began over a year ago (PrevNet, 2014).

Indigeneity is an online harassment risk factor

The cyber-bullying literature shows that Indigeneity increases the risk of certain forms of cyber-victimization. Studies show that increased social media use has made Indigenous youth and women easier targets for hate, racism, and bullying online (Bailey & Shayan, 2016; Rice *et al.*, 2016), highlighting the intersectional nature of online harassment. A study of 204 Indigenous youth (ages 10–16) living on-reserve within the Saskatoon Tribal Council found that 30% of students reported experiencing cyber-bullying in the month preceding the survey (Lemstra *et al.*, 2011). This compares to 10% of students within the same age range reporting cyber-bullying in the city of Saskatoon.

While the evidence in this study — and the wider field of research — is limited, it does indicate that Indigenous youth living on-reserve experience cyber-bullying (and other forms of bullying) at rates higher than the national average (Lemstra *et al.*, 2011). The limited data, and the relationship between Indigeneity and online harms, demonstrate that further attention from both researchers and policy-makers is needed. In addition, there is a "need to develop research that treats Indigeneity as more than just a variable or as a monolithic entity or static identity" (Huey & Ferguson, 2022). This research will "consider the various ways in which Indigeneity intersects with class, gender, sexual and other factors to create unique risk pathways" (Huey & Ferguson, 2022).

Certain professions are common targets of online harassment

Some professions that require an online presence are more likely to be targets of online harassment. For example, a survey found that 65% of journalists in Canada — mostly women — received threats or were harassed online at least once in the last 12 months, and 20% of them experienced this on a daily or weekly basis (Ipsos, 2021). Additionally, online attacks against female journalists appear to be increasing, both globally and in Canada (Ipsos, 2021; Posetti *et al.*, 2022). Sexualized images or messages and physical threats are the most common forms of online harassment experienced by journalists, leading almost a third of those surveyed to consider leaving their professions (Ipsos, 2021). Besides journalists, researchers, public health communicators, and politicians — particularly women — are also more likely to get harassed online (Tenove & Tworek, 2020; Wagner, 2022; Wright *et al.*, 2022).

Online harassment and abuse cause psychological harms and limit freedom of expression

Online harassment and abuse are experienced at individual and societal levels. While impacts vary based on the type of harm, targets of online harassment face a heightened risk of anxiety and depression. Even when there is no physical contact, victims of cyber-stalking may suffer severe mental health-related consequences that affect their relationships and careers, and may lead to isolation or other outcomes (Strawhun *et al.*, 2013; Al-Khateeb *et al.*, 2017). Like physical bullying, young people who experience cyber-bullying are at greater risk of experiencing depression and anxiety than their non-bullied peers (Wang *et al.*, 2011; Broll & Huey, 2015; Abreu & Kenny, 2018). Unlike physical and verbal bullying in the schoolyard, social media applications allow for targets to be reached long after school hours and within the confines of their own homes. Because of this, they get little reprieve from the bullying and may find it harder to escape its impacts (Broll & Huey, 2015).

Online harassment and abuse have a significant impact beyond affecting the individual. The Plan International global survey found online harassment can cause many girls and young women to leave social media (12%), use it less (19%), or allow the harassment to change the ways in which they would normally express themselves online (12%) (Plan International, 2020b). There are social consequences stemming from the online harassment of girls and women, as the CEO of Plan International noted upon the release of the organization's survey results: "These attacks may not be physical, but they are often threatening, relentless, and limit girls' freedom of expression. Driving girls out of online spaces is hugely disempowering in an increasingly digital world, and damages their ability to be seen, heard and become leaders" (Plan International, 2020a).

Online harassment and abuse have a chilling effect

Online threats and harassment are often intended to silence, or impose a chilling effect on, the voices of victims, who are disproportionately women and other marginalized groups (Pew Research Center, 2017). This effect is dramatic and has led women and girls to self-censor their views and opinions in non-digital spaces out of a fear of potential abuse or backlash (Jankowicz *et al.*, 2021). Other women have withdrawn from politics or social activism, or reconsidered pursuing a future in these fields, due to the potential for online abuse (Campbell & Lovenduski, 2016; Di Meco, 2019; Jankowicz *et al.*, 2021). Online abuse can threaten the fabric of participatory democracy by targeting diverse, new, or alternative voices and perspectives (Citron & Penney, 2019).

This chilling effect has an impact in other areas of expertise beyond politics and activism, affecting the quality of information communicated by experts and made available to the public. For example, in a survey by *Nature* of over 300 scientists who had conducted media interviews related to the COVID-19 pandemic, over two-thirds of respondents reported negative experiences related directly to their media appearance or social media statements (Nogrady, 2021). While attacks on credibility were the most reported form of online abuse, 22% of those surveyed received threats of physical or sexual violence, while 15% reported the receipt of death threats.

Mirroring other online abuse studies, *Nature* found that women, people of colour, and other marginalized groups were more frequently the targets of online abuse, and that the derogatory comments they received were often personal in nature (i.e., related to gender, race, or ethnicity) rather than targeting their opinions or scholarship. Online threats had profound effects among those surveyed. In a quintessential example of the chilling effect, scientists who experienced online trolling or personal attacks indicated that they were less likely to speak with media outlets or communicate their findings and professional views to the public (Nogrady, 2021). The decision to withdraw from the media landscape has tangible consequences for career advancement, especially among young, up-and-coming, and female researchers who may lose valuable opportunities to develop their professional profile (Nogrady, 2021).

It is difficult to prosecute online harassment and abuse

Prosecuting online crimes such as harassment and cyber-stalking can be difficult. In some cases, the offending language may be considered an expression of free speech; in other cases, victims may not report abuse sent in private communications,

or may be unaware that they can report harmful content to service providers (Al-Khateeb *et al.*, 2017). In many cases, they do not have access to information or resources on what to do if they are harassed online (Ketchum, 2020) and experience a sense of shame or fear of retribution; these perceptions can manifest as reasons for not advocating on their own behalf (Al-Khateeb *et al.*, 2017). Finally, depending on jurisdiction, victims may need to suffer a certain amount of harassment or stalking before they are entitled to file charges against the perpetrator (Al-Khateeb *et al.*, 2017). Despite extensive evidence documenting the abuse and harassment of women online, and some action taken by technology companies, the problem persists (Khoo, 2021). It has been suggested that the ineffective response may be linked, in part, to the technology sector itself, where there is a lack of gender and racial diversity among all ranks, including within leadership and management positions (Khoo, 2021).

The sale of spyware and stalkerware tools facilitate cyber-harassment (Box 3.2). If the technology is sold with the stated purpose of spying on another's personal communications, for instance, developers and sellers in Canada could potentially be held criminally liable. In these cases, developers and sellers may also be vulnerable to civil lawsuits brought by victims and survivors. However, it is more often the case that these apps are developed and sold for entirely legal purposes (e.g., monitoring children and employees), but are repurposed for malicious use. In these cases, proving culpability may be more difficult (Khoo *et al.*, 2019).

Box 3.2 Emerging Safety Concerns Related to Small Tracking Devices

As new ICTs are released into the market with little regulatory oversight or preparation, unintended harms, with safety and privacy implications, may arise. Apple AirTags and similar devices, such as Tile, Samsung Galaxy SmartTag, and Chipolo ONE, exemplify how legal surveillance devices can be exploited for criminal purposes; this creates challenges for law enforcement when officers are forced to respond reactively to these emerging approaches to crime. Small tracking devices are designed to help people find personal objects (e.g., keys, purses, backpacks) through a mobile app using Bluetooth (Apple, 2022; Samsung, n.d.; Tile, n.d.). Since these devices were launched, they have been used to facilitate malicious and criminal acts.

(Continues)

(Continued)

Women have found devices that did not belong to them in their cars and belongings, making them feel unsafe and suggesting the devices could be used for stalking (Willey, 2018; Suares, 2019; Ingram, 2021; Mac & Hill, 2021); stalking concerns were indeed raised by privacy advocacy groups when AirTags were introduced (Mac & Hill, 2021). Law enforcement agencies in Canada and the United States have reported that AirTags are also being used to track and steal cars, and warn that the devices pose a danger to potential victims of domestic violence (Mac & Hill, 2021; Tsekouras, 2021). While iPhones and Android phones can sometimes be equipped to notify individuals when an unknown tracking device is routinely proximate to the phone's owner (Samsung, 2021; Apple, 2022; Tile, 2022), some victims and survivors have expressed concerns that law enforcement agencies do not always take reports of phone notifications seriously (Mac & Hill, 2021). In 2022, Apple announced their intention to introduce additional features, including tools to allow "recipients of an unwanted tracking alert to locate an unknown AirTag with precision" (Apple, 2022). There is no evidence so far that governments in Canada or the United States have attempted to regulate tracking devices.

Criminalization may not always be an effective response to online harassment and abuse

Studies show that police are often hesitant to pursue criminal charges for cyber-bullying. In focused interviews with 12 Canadian police officers, interviewees expressed wariness about using their already strained resources to monitor online bullying and speech, while also voicing concerns about the increase in criminal prosecutions against youth that would inevitability result from criminalizing cyber-bullying. The police expressed their belief that existing laws were sufficient and effective in demarcating the line between criminal and non-criminal online behaviour (Broll & Huey, 2015). Cautions against criminalizing cyber-bullying were also voiced in an Australian study by Pennell *et al.* (2022), which found that criminalizing the behaviour will likely have the biggest impact on youth, many of whom may be engaging in cyber-bullying as a result of their own cyber-victimization. Pennell *et al.* (2022) argue that a legal approach to cyber-bullying may unnecessarily jeopardize a young person's future, and that an educational approach may provide a more appropriate solution.

The police officers interviewed by Broll and Huey (2015) reported a preference for less punitive measures than criminal sanctions, and for working toward preventative solutions alongside school resources officers and other relevant

parties. Solutions focused on prevention and early intervention have also been recommended by researchers in the field. Within the specific context of the bullying of LGBTIQ+ youth, Abreu and Kenny (2018) recommend prevention and intervention programs specifically tailored to particular needs and issues. The authors cite peer-driven education programs; school-administered online forums for students at risk of being cyber-bullied; channels for anonymous reporting of bullying; explicit school policies that address cyber-bullying and the targeting of specific groups; and training for school staff on the signs and impacts of cyber-bullying (Blumenfeld & Cooper, 2010; Hillier *et al.*, 2010; Abreu & Kenny, 2018). Evidence suggests that holistic approaches — those involving parents, schools, and other community partners (Box 3.3) — have been the most effective in decreasing cyber-bullying among youth (Couvillon & Ilieva, 2011; Bailey, 2015; Abreu & Kenny, 2018).

Box 3.3 Community-Led Actions and Cyber-Enabled Crimes

Civilian volunteers — both individuals and groups with varying degrees of coordination — can play active roles in combatting cyber-enabled crime (Huey *et al.*, 2013; Chang *et al.*, 2018). There is a wide range of these types of actions, including collecting digital information on suspected cyber-threat actors and sharing it with law enforcement agencies, online shaming of harmful acts, content self-policing in online forums, and online vigilantism (Huey *et al.*, 2013; Seering *et al.*, 2019; Loveluck, 2020). There are documented examples of evidence, collected by volunteer groups partnering with law enforcement, leading to the arrest and conviction of people committing online child sexual abuse (Huey *et al.*, 2013), and of user-led content moderation contributing to the positive development of online communities (Seering *et al.*, 2019). While the involvement of civilian volunteers in online policing can be beneficial in some instances, law enforcement often views community participation as unnecessary or undesirable, with the exception of providing tips (Huey *et al.*, 2013; Chang *et al.*, 2018). Concerns related to community-led actions include legal liability, the safety of volunteers, the privacy of people suspected of committing cybercrimes, and the perceived erosion of trust in law enforcement (Huey *et al.*, 2013; Chang *et al.*, 2018).

Evidence indicates that more training is needed to help relevant professionals recognize the ways that technology is used to facilitate gender-based violence, especially within the context of intimate partner relationships. Training for

members of police services, legal professionals, and support workers may be an important consideration moving forward (Siminovic, 2017; Khoo *et al.*, 2019). Furthermore, the law is but one component in addressing this type of online harassment. In addition to legal measures addressing the culpability of perpetrators, experts argue that the corporate responsibility of service providers and social media platforms, including content moderation policies and community guidelines, also plays a crucial role in reducing harassment, and in monitoring and removing offensive content (Henry & Powell, 2016).

3.2 Digital Technologies and Abusive Content (Terrorism and Hate Propaganda)

In this section, the Panel discusses abusive content that, according to the NACCC, falls under a separate category of *terrorism and hate propaganda*. This category includes the dissemination of content "pertaining to racism, xenophobia, or incitement to violence" (NACCC, 2021a). The dissemination of this content is harmful and sometimes considered to be criminal in nature — although, in some circumstances, it is difficult to establish when hateful content becomes illegal. To be prosecuted under criminal law, hate speech must meet certain requirements established in the *Criminal Code*, such as public communication of statements inciting hatred against an "identifiable group" that is "likely to lead to a breach of the peace" (GC, 1985). Evidence suggests that some forms of abusive content are more effectively addressed through non-criminal means, and the Panel does not argue for criminalizing all such harmful acts.

3.2.1 Terrorism (Radicalization and Extremist Content)

Violent extremism can be defined as the use of "violence to achieve extreme ideological, religious, or political goals" (Canada Centre, 2018). While politically and religiously motivated violent extremism (PMVE and RMVE, respectively) are driven by particular sets of political or religious beliefs, the targets of ideologically motivated violent extremism (IMVE) vary widely (CSIS, 2021a). IMVE includes xenophobic violence (targeted at racial or ethnic groups), gender-driven violence (targeted at women and the LGBTIQ+ community), or anti-authority violence (targeted at government or law enforcement).

In general, radicalization to extremism and violence is driven by several behavioural, historical, and societal factors, including an individual's social networks, grievances, vulnerabilities, desire for belonging, an inclination toward violence, and isolation (Canada Centre, 2018). The COVID-19 pandemic has exacerbated factors that commonly support extremism, such as social isolation, perceived government overreach, and economic downturns. Many extremist groups have harnessed the pandemic to spread narratives supporting their own

ideologies (Paikin, 2020; CSIS, 2021a). Contrary to those driven by PMVE or RMVE, individuals driven by IMVE usually act on their own and are unaffiliated with larger groups or organizations, although they can be influenced by online communities (CSIS, 2021a).

The online environment is linked to radicalization

While violent extremism is not primarily rooted in digital contexts, and ICTs alone do not radicalize people, there is some evidence showing that exposure to extremist online content could lead to political, religious, or other radicalization, or accelerate it (Mullins, 2013; Canada Centre, 2018; Hassan *et al.*, 2018; SECU, 2022a). Many extremist groups use tools such as encrypted messaging apps, media-sharing platforms, and major social media networks such as Facebook, Twitter, and YouTube (PS, 2019a; Hart *et al.*, 2021; Moonshot CVE, 2021). Studies on right-wing and jihadi extremism in Canada found that the internet facilitated radicalization of people because it provided easy access to extremist content and a network of like-minded individuals (Mullins, 2013; Gaudette *et al.*, 2020; Dawson & Amarasingam, 2021).

Participating in online discussions via forums, chatrooms, and social media platforms lets individuals immerse themselves in violent extremist content and networks (Gaudette *et al.*, 2020). Social media has, in some cases, a higher influence on radicalization processes than in-person acquaintance groups, friends, family, or faith leaders (Bastug *et al.*, 2020). Immersion in online environments is a factor that can strengthen beliefs and ideological affirmation (Perry & Scrivens, 2016; Selim, 2019). Similar patterns were found in far-right Facebook groups in Quebec that engage in digital vigilantism (Tanner & Campana, 2020). A study of content from *Stormfront Canada*, one of the most-visited web forums among right-wing extremists, found that the volume, severity, and duration of antisemitic, anti-Black, and anti-LGBTIQ+ content posted by users increased over a 15-year period, which suggests there was increased radicalization (Scrivens *et al.*, 2020).

Extremist groups communicate and recruit members using social media

ICTs provide platforms for individuals to recruit others to their causes, share propaganda, and communicate about and plan attacks (Canada Centre, 2018; PS, 2019a). Most people with extremist views are unaffiliated with organized crime groups; however, online forums allow isolated extremists to expand their reach and "become more active in virtual campaigns of ideological recruitment and radicalization" (Selim, 2019), in part by facilitating the publication and dissemination of extremist material (Perry & Scrivens, 2016). Social media allows extremists to identify and target specific groups with customized materials and

messaging for recruitment (Canada Centre, 2018). Engagement tactics such as humour, memes, and video games are also used by extremist groups to target youth (Box 3.4), which is a concern given the growing number of young people being radicalized (Ahmad, 2017; ASIO, 2021).

Box 3.4 Use of Humour, Memes, and Video Games by Extremist Groups

Humour can effectively attract people to extremist ideologies. A document alleged to be the style guide for prospective writers of a known neo-Nazi blog encourages authors to use humour as a delivery method for their hateful content (Feinberg, 2017). Presenting hateful ideas online under the guise of humour, satire, or parody offers the protection of plausible deniability, where, "in the absence of an author indicating his or her intentions, it can be difficult to distinguish between [...] extremism and a parody of extremism" (Greene, 2019). Extremist groups increasingly use these tactics to deliver messages and recruit new followers (Donovan, 2019; Greene, 2019); humour allows neo-Nazi organizations to publish hateful work under the guise of facilitating camaraderie, pleasure, or fun, which is particularly useful in attracting younger audiences (Askanius, 2021).

Humour and memes can also be used to promote an us-versus-them narrative by dehumanizing and making light of the struggles of people outside of one's subculture (Greene, 2019; Mortensen & Neumayer, 2021). Meme culture, which involves remixing and appropriating well-known media, takes advantage of the source material's familiarity and provides shock by subverting the viewer's expectations (Greene, 2019). To truly engage with the media, viewers need to be fluent in the group's subculture and in-jokes. In this way, meme creators can tailor their message to resonate with their target audience through humour and knowledge of internet culture (Marwick & Lewis, 2017).

Online multiplayer video games also facilitate the recruitment of youth to extremist groups, the dissemination of propaganda, and the interactive communication within extremist groups (Robinson & Whittaker, 2020). The online store and in-app chat function of Twitch, a popular livestreaming service for video game developers and players, have both been used by extremists to easily promote their content to a large audience (O'Connor, 2021). Twitch has approximately 30 million daily visitors on average, nearly half of whom are 18–34 years old (O'Connor, 2021). Far-right influencers and conspiracy theorists have made thousands of dollars broadcasting misinformation and extremist content on Twitch (Browning, 2021).

While the internet enables right-wing extremist organizations to communicate across borders, most extremist content circulating in Canada originates within the country

In Canada, there has been a rise in the threat posed by "gender-driven, xenophobic, anti-authority, and other grievance-driven violence" (CSIS, 2022). Canada's national security and counter-terrorism communities have been focusing their surveillance efforts on far-right nationalist and white supremacist groups (Crosby, 2021). The global reach of the internet means that people across Canada can search out and access radical online communities (Moonshot CVE, 2021), and right-wing extremists are increasingly networking and cooperating across borders (Musharbash, 2021). Many right-wing extremist organizations in Canada have direct links to similar groups in the Unites States and Europe (Perry & Scrivens, 2016), and Canadian right-wing extremist content is influenced by events in the United States (Hart *et al.*, 2021). However, most of the extremist content circulating in Canada originates in Canada itself (Hart *et al.*, 2021; SECU, 2022a). Extremism is a problem that occurs domestically in Canada, not one that is solely imported into the country.

The amount of online right-wing extremist activity is small relative to social media use in Canada more broadly; there is one active right-wing extremist page or group for every 235,420 Facebook users (Hart *et al.*, 2021). That said, one analysis identified 2,467 active accounts, channels, and pages of right-wing extremist content in Canada, which collectively, on average, created over 60,000 unique content pieces per week (Hart *et al.*, 2021). In 2020, this content generated approximately 44 million reactions on Facebook and more than half a million comments on YouTube, was re-shared on Twitter almost 9 million times, and was viewed more than 16 million times on Telegram (Hart *et al.*, 2021).

Some extremist online content incites violence

Some, though not all, extremist content is considered criminal. As an example, approximately 31,000 out of 3 million pieces of right-wing extremist content analyzed in Canada involved "abusive, aggressive, dehumanizing, or violent language targeting an individual or group of individuals," including calls for violence (Hart *et al.*, 2021). Violence is a common theme in Canadian extremist circles, insofar as members often share guides on preparing for violence (Hart *et al.*, 2021), include words that relate to violence, and contain more mentions of lethal firearm violence than similar content originating in Australia (Hutchinson *et al.*, 2021). The publishing and subsequent online spread of extremist manifestos in one country can also inspire violent extremist acts offline in other countries (Berger, 2019).

Young men are most likely to search for online extremist content

Some data exist about the demographics of those who carry out extremist content searches in Canada. Moonshot CVE (2021), as an example, used keywords related to ISIS, Al-Qaeda, and far-right content that incites violence and promotes conspiracy theories, and captured 171,382 Google searches in Canada between February 2019 and March 2020. Subsequent analysis suggests that extremist content from across ideological, religious, and political spectrums is being sought out by people online across Canada. Notably, users between the ages of 25 and 34 were more likely to search such content (close to 30% of searches), and men conducted approximately 75% of searches (Moonshot CVE, 2021).

3.2.2 Hate Propaganda

As with online harassment, it can be challenging to identify the point where hateful content shifts from awful (but legal) to unlawful. Hate speech (called *hate propaganda* in the *Criminal Code*) is illegal in Canada (GC, 1985). Advocating for genocide, incitement of hatred against an "identifiable group" that is "likely to lead to a breach of the peace," and communications that "willfully promote hatred against an identifiable group" in a public place are criminal offences (GC, 1985; Walker, 2018). An "identifiable group" can refer to religion, ethnicity, gender identity, sexuality, or race. Section 320 of the *Criminal Code* allows for hate propaganda material, including computer data, to be confiscated upon orders from the court and Attorney General (GC, 1985). Charges under Sections 318 and 319 are primarily used in cases where someone incites others to hate and require the consent of the Attorney General — an important process that can sometimes extend the length of investigations (Corb, 2015; Proctor, 2020).

Many incidents that might include hateful actions may be charged as other offences, such as assault or harassment, with hate considered as an aggravating factor during sentencing (Walker, 2018; Proctor, 2020). There is no written definition of *hatred* in Canada's *Criminal Code*, but one was proposed in Bill C-36 (2021) (Chapter 5); cases involving hate propaganda in Canada have resulted in a legal interpretation of *hate* that refers to extremely strong emotions of "detestation, calumny and vilification" (SCC, 1990a) against a target group, and which denies respect and dignity toward the targets (SCC, 1990b).

Online hate crimes appear to be rising, but are under-reported

It is difficult, and likely impossible, to obtain complete and accurate information about incidences of online hate speech (Gill, 2020). That said, Statistics Canada reported 572 hate-motivated cybercrimes recorded by police between 2010 and 2019 (Moreau, 2021b). This number is a known undercount given that the Ontario

Provincial Police (OPP) did not report the cybercrime indicator from 2010 to 2018, and several other municipal police services were unable to do the same for various years during this period. Among the hate-motivated cybercrimes that were reported, uttering threats (38%) was the most common type of cyber-hate crime between 2010 and 2019, followed by public incitement of hatred (17%), indecent or harassing communications online (17%), and criminal harassment (12%) (Moreau, 2021b).

Companies operating social media platforms have also provided snapshots of the prevalence of online hate speech. For example, within a three-month period spanning from July to September 2021, Meta reportedly took action against 22.3 million instances of hate speech on Facebook (Facebook – Meta Transparency Center, 2021); between April and June 2021, YouTube took action against 57.8 million comments described as "hateful or abusive" and removed 42,013 channels for the same reason during that same period (Google, 2021). However, hateful content is not always removed in a timely fashion (JUST, 2019), accounts that spread hateful content can reappear after being removed (Velásquez *et al.*, 2021), and the content removed may not be consistent across platforms (Chapter 4).

Hateful content can reach large audiences online

While hate speech has historically been shared through mail, pamphlets, or audiovisual formats such as videotapes, DVDs, and CDs, the widespread adoption of ICTs has provided new platforms through which individuals can spread hateful content online. These ICTs tend to be more effective at reaching larger audiences with less effort than prior, analogue-based methods (Rohlfing, 2015). The communication and spread of hate speech vary depending on the ICT employed; content hosted on platforms such as Telegram or 4chan, which have less content enforcement, more commonly contain slurs compared to content posted on platforms such as Facebook (Hart *et al.*, 2021).

Hateful content can move across social media platforms, making it difficult to control

Even robust content moderation policies may not effectively work to prevent the spread of hate speech given that users who consume this content often do so on multiple platforms. A study that focused on the spread of malicious COVID-19 material among online hate communities found that less-moderated platforms (e.g., 4chan) impact the ability of mainstream platforms (e.g., Facebook) to moderate hate content, because the former permit the rapid spread of malicious materials across platforms via interconnected hate communities (Velásquez *et al.*, 2021). The authors note that "malicious activity can appear isolated and largely eradicated on a given platform, when in reality it has moved to another platform. There, malicious content can thrive beyond the original platform's control, be

further honed, and later *reintroduced into the original platform* using a link in the reverse direction." That is, people can be directed from moderated sites to less-moderated ones by way of a hyperlink, with the effect that "a user of mainstream social media communities, such as a child connecting with other online game players or a parent seeking information about COVID-19, is at most a few links away from intensely hateful content" (Velásquez *et al.*, 2021). Inconsistent content moderation policies across different platforms facilitate the migration of de-platformed and extremist users to alternative digital spaces, where they disseminate hateful content (Rogers, 2020).

Offline events influence the frequency and type of hate speech appearing online

Mounting evidence points to a correlation between external events and an increase in online hate speech. For example, a 2018 study that monitored Twitter and Reddit posts found a rise in hate speech against Arab and Muslim communities following attacks perpetrated either by or against Arab and/or Muslim people in countries where they are minority groups (Olteanu *et al.*, 2018). These results align with other studies that examined the proliferation of online hate in the wake of what are described as "triggering events" (Awan & Zempi, 2015; Benesch *et al.*, 2016; Faris *et al.*, 2016). COVID-19, which operated as one of these events, led to a rise in hate crimes and hate speech against Asian communities across the world (Macguire, 2020). Online, this abuse has been tracked by the prevalence of derogatory and racist language, with some individuals appearing to blame the pandemic on Asian communities and countries (Macguire, 2020).

Even in the absence of triggering events, emerging evidence points to a link between online hate and offline victimization. A U.K. study, which drew on data obtained from London's Metropolitan Police Service and social media posts, found "a positive association between Twitter hate speech targeting race and religion and offline racially and religiously aggravated offences in London" (Williams *et al.*, 2020). The study's authors describe the role of social media in facilitating offline victimization as "non-trivial" and one that plays a significant part in the overall formula that inspires hate-based crimes. That formula includes other known factors such as historical, political, social, and geographic contexts (Williams *et al.*, 2020). The study confirms findings elsewhere that link offline hate crimes against Muslims in the United States to inflammatory Twitter activity by Donald Trump during his presidential campaign (Müller & Schwarz, 2020a), and online hate speech to violent incidents against refugee and immigrant communities in Germany (Müller & Schwarz, 2020b). In aggregate, this evidence suggests that commonly targeted communities could expect (and prepare for)

possible online harassment prior to major events or have in place plans to react in the face of unexpected triggering events.

Marginalized and minoritized communities are at higher risk of experiencing online hate

A 2021 survey found that 47% of people using the internet in Canada have either experienced or seen racist comments or content online, 38% have seen or experienced homophobic comments or content, and 30% have seen or experienced sexist comments or content (Abacus Data, 2021). Racialized and young people in Canada are more likely to encounter the aforementioned types of content on major platforms such as Facebook and YouTube (Andrey *et al.*, 2021a). Among hate-motivated cybercrimes reported to police in Canada between 2010 and 2019, people were most often targeted because they were Muslim (17%) or Jewish (13%), because of their sexual orientation (13%), or because they were Black (10%) (Moreau, 2021b).

Another 2021 survey of 2,500 people aged 16 or older that represented an ethnic cross-section of Canada found that 26% of respondents reported receiving hateful messages on private messaging applications (e.g., Facebook Messenger, WhatsApp, Snapchat) at least once a month (Andrey *et al.*, 2021a). These rates rose considerably when selected for people of colour (e.g., Latin American 58%, Middle Eastern 44%, Southeast Asian 44%). The platforms on which the messages were sent had user content policies that prohibit hate speech and enable users to report the receipt of harmful messages (Andrey *et al.*, 2021a). Despite these policies and platform functions, the messages were still issued and received and, as such, could cause harm even while there was a way to report or address them after reception.

3.3 Digital Technologies and Fraud

Fraud is broadly defined by the NACCC as the "loss of property (including data) caused with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person" (NACCC, 2021a). The nature of fraud, however, is changing. Fraud campaigns can use ICTs to quickly adapt to current events, such as elections, tax season, news stories, or global health crises such as the COVID-19 pandemic (Canadian Centre for Cyber Security, 2020a). The result is that some types of cyber-fraud and associated extortion attempts are becoming more sophisticated, in part due to cybercrime marketplaces such as the Dark Web letting relatively unsophisticated actors purchase the tools and services required to carry out online fraud campaigns (Canadian Centre for Cyber Security, 2020a) (Section 4.2).

Other forms of cyber-fraud may not be technologically sophisticated (e.g., text scams), but they can cause significant harms without much effort through the use

of social media (FTC, 2022). Fraud operations routinely occur across jurisdictions, making it challenging or nearly impossible, in some cases, for law enforcement agencies to investigate crimes and bring charges against offenders (ESDC, 2019). While the Panel recognizes that multiple forms of cyber-fraud exist, it focuses on those involving false representation (e.g., scams) while paying special attention to the predatory online fraud practices that target vulnerable communities due to the acute harms these practices can incur.

3.3.1 The Scale and Impacts of Cyber-Fraud

While reporting barriers persist, cyber-fraud is the most common reported cybercrime

Like other types of cybercrime, cyber-fraud is under-reported. Some estimates suggest "only around 5% of fraud incidents are reported to law enforcement, which makes it difficult to gather evidence and intervene" (ESDC, 2019). At the same time, cyber-fraud is the most commonly police-reported cybercrime in Canada and has increased more than 150% since 2016 (StatCan, 2021b). There were over 138,000 incidents of fraud reported to police in Canada in 2020 (Moreau, 2021a), almost 30,000 of which were classified as cyber-fraud (StatCan, 2021b). The most common type of reported fraud in Canada involves extortion (i.e., someone illegally obtaining money, property, or services from a person through coercion), followed by identity fraud and unlawful access to personal information (CAFC, 2021b).

In 2020, there were over 17,000 incidents of extortion-related fraud reported, affecting approximately 6,700 people in Canada (CAFC, 2021b). Cyber-threat actors will often threaten to conduct cyber-attacks or steal (or claim to have stolen) incriminating information in order to extort money from victims (Canadian Centre for Cyber Security, 2020a). Some forms of fraud documented in Canada include using fake profiles on social media and dating sites to facilitate extortion and fraud (Canadian Centre for Cyber Security, 2020b). In some instances, cyber-threat actors get access to intimate videos of their victims and extort money by threatening to send the videos to the victim's contacts (Canadian Centre for Cyber Security, 2020a).

The prevalence of cyber-fraud reports relative to other cyber-enabled crimes may be partially due to Canada having a specific online reporting mechanism for cyber-fraud (CAFC, 2021a), which is not available for other forms of cybercrime. Fraud was also the most common offence related to case disclosures by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) in 2021 (FINTRAC, 2021a).

Cyber-fraud leads to substantial financial and psychological harms

The financial harms associated with cyber-fraud are considerable and growing. According to the Government of Canada's anti-fraud reporting venue and central fraud data repository, the Canadian Anti-Fraud Centre, over 67,000 people and businesses in Canada were victims of fraud in 2020, collectively losing more than $104 million (CAFC, 2021b). That amount almost doubled the following year, with people losing close to $200 million from January to October 2021 (CAFC, 2021c). So-called romance-related frauds, often perpetrated online, caused the most financial losses for people in Canada in 2020 ($18.5 million) (CAFC, 2021b). The COVID-19 pandemic has provided a new avenue for those committing fraud; from March 2020 to May 2021, there were close to 20,000 victims and $7.4 million lost in Canada due to pandemic-related fraud (e.g., scams requesting payment for fraudulent medical advice) (Moreau, 2021a).

The harms of cyber-fraud go beyond financial losses. It is associated with emotional and psychological impacts on victims and survivors, including trauma, which in extreme cases has been a contributing factor in death by suicide (Cross *et al.*, 2016; Cross, 2017). Other harms documented from online fraud involve loss of sleep, ongoing fear, and concerns for one's physical safety (Cross *et al.*, 2016).

Considerable fraud-prevention efforts are implemented by financial institutions when they are affected

When financial losses due to fraud severely affect financial institutions, robust efforts to prevent further fraud tend to follow. For example, credit card fraud amounts to approximately $800 million in annual financial losses in Canada (Henry *et al.*, 2018; Simple Rate, 2021), but zero-liability protection policies make financial institutions reimburse unauthorized transactions to customers victimized by fraud (FCAC, 2019; CBA, 2022). This has incentivized financial institutions to invest heavily in fraud-prevention efforts. Between 2009 and 2019, Canada's six largest banks collectively invested $100 billion in technology, substantially improving their in-house cybersecurity (CBA, 2022).

3.3.2 The Effects of Cyber-Fraud on Certain Demographic Groups

Older adults are vulnerable to cyber-fraud, resulting in significant financial losses

Older adults in Canada are particularly vulnerable to cyber-fraud. Declining cognitive abilities among older adults, such as short-term memory and alertness, are correlated with greater susceptibility to online deception (Ebner *et al.*, 2020). Social isolation and economic insecurity may exacerbate their vulnerability (Cross, 2016; ESDC, 2019), as can low levels of digital literacy, which can make it challenging to effectively discern genuine from phishing emails (Grilli *et al.*, 2021).

However, phishing attacks have become increasingly sophisticated and deceptive, making them difficult to identify even with high levels of digital literacy (Alkhalil *et al.*, 2021). Cyber-fraud may also be tied to the abuse and exploitation of older adults (JUS, 2010), for which there are protections enshrined in privacy and human rights legislation (Box 3.5).

Box 3.5 Protections Against Exploitation of Older Adults

All provinces and territories in Canada have human rights legislation protecting against age-based discrimination (GC, 2021b). However, Quebec has a more expansive approach when defining and addressing the abuse of older adults (GC, 2021b). Quebec's Charter of Human Rights and Freedoms contains specific provisions for securing the right of older adults to be protected against all forms of exploitation (Gov. of QC, 1976), establishing a quasi-constitutional status (GC, 2021b). Exploitation — which can be financial, physical, or emotional — involves taking advantage of and inducing harms to a vulnerable person (Éducaloi, 2022). Quebec's human rights commission (Commission des droits de la personne et des droits de la jeunesse) has a dedicated team to investigate exploitation of older adults and help find appropriate supports, including requesting an emergency court order (CDPDJ, 2022; Éducaloi, 2022). Exploitation can be reported without the victim's consent (CDPDJ, 2022). Financial exploitation of older adults is the most-reported form of exploitation to the commission (CDPDJ, 2022), and fraud-related exploitation may include obtaining money from an older adult using force or threats (Éducaloi, 2022).

In 2015, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) was amended to allow organizations to contact a government institution, or a person's next of kin or authorized representative if:

i. "the organization has reasonable grounds to believe that the individual has been, is or may be the victim of financial abuse,

ii. the disclosure is made solely for purposes related to preventing or investigating the abuse, and

iii. it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse"

(GC, 2000a)

This amendment, however, has been criticized as being discriminatory against older adults and potentially exposing them to additional risks because, in many cases, financial abuse is perpetrated by the next of kin (Van Cauwenberghe, 2015).

The most common types of fraud experienced by adults in Canada aged 60 and older were extortion, service scams (including tech support scams), and phishing (ESDC, 2019). So-called romance-related fraud generated the greatest financial loss among older adults ($9 million, accounting for 25% of all losses to romance-related fraud). These numbers are likely an underestimate, since older adults are less likely to report fraud to the police, in part due to feelings of shame as well as "a perceived low impact of reporting, particularly when losses are low in value" (ESDC, 2019).

Scams and spoofing practices often target new immigrants in Canada

New immigrants to Canada are also more vulnerable to cyber-fraud than the general population (RCMP, 2019; IRCC, 2021a). Cyber-threat actors often pose as legitimate organizations (e.g., government agencies, banks) and set up fake websites and online ads (CAFC, 2021d). These sites and ads often claim to offer inexpensive immigration services or falsely guarantee jobs for new immigrants by requesting fees (Canadian Centre for Cyber Security, 2020a). More than 3,500 fake Government of Canada social media accounts, websites, and email servers were taken down in 2020 (Canadian Centre for Cyber Security, 2020a).

Another common type of cyber-fraud affecting new immigrants involves impersonating immigration officials online or via phone calls threatening to arrest or deport targets unless they pay a fee or give away personal information (IRCC, 2021b). These scams are sometimes facilitated by spoofing phone numbers,[5] a practice that is not illegal (CAFC, 2020; Daubs, 2022). While the CRTC has some rules on unsolicited telecommunications, regulatory and civil law tools to combat spoofing in Canada are more limited than in other countries, such as the United States (Daubs, 2022).

Youth are more likely than older adults to be defrauded on social media

Social media is used as a tool for scammers to reach people and commit fraud. In the United States, reported cyber-fraud increased in every age group in 2021, but those aged "18 to 39 were more than twice as likely as older adults to report losing money" to social media scams (FTC, 2022). While equivalent data are not available in Canada, there are high levels of social media use by young people in Canada, along with evidence that scammers are increasingly using social media to target different demographic groups, including youth (RCMP, 2018; Canadian Centre for Cyber Security, 2020b). In response, Facebook Messenger has introduced safety notices in chats attached to resources to help people identify suspicious activities, including scams (Facebook, 2020a).

5 Spoofing entails a caller deliberately manipulating information transmitted to a caller ID display in order to hide their identity.

3.4 Summary

To answer the Sponsor's question on how serious criminal activities and harmful behaviours have evolved to exploit advances in ICTs, the Panel focused on the exploitation, harassment, and abuse of people, violent extremist activity, the propagation of hate, and fraud. In particular, this chapter described how ICTs can increase the reach of cyber-threat actors, making it easier for them to recruit and communicate among other perpetrators as well as find and target victims. This creates numerous challenges for authorities that seek to prevent, counter, and investigate harmful activities using tools or approaches that may be maladapted to ever-evolving digital contexts.

Harmful acts take place on a spectrum of criminality and legality. Depending on the circumstances, some acts commonly considered reprehensible, such as cyber-bullying, online harassment, or the dissemination of deepfakes, may not be criminal or even illegal. However, the evidence demonstrates that these and other cyber-harms can lead to considerable physical, psychological, and financial impacts for the people targeted. At the same time, not everyone is equally at risk of experiencing harms online. Common targets of harmful acts and content online include women, youth, racialized and minoritized communities, and some professions such as journalism, highlighting the intersectional nature of this issue.

Addressing these harms requires a combination of legal and non-legal approaches informed by the experiences of victims and survivors. The Panel found that legal reforms can sometimes limit the dissemination of deepfakes and the non-consensual distribution of intimate content. The criminalization of all instances of cyber-bullying, however, is not advisable for a range of reasons, including the negative impact on youth, many of whom engage in cyber-bullying as a result of their own traumatic experiences. Alternative approaches to addressing cyber-harms include educational programs, community guidelines and content moderation programs on social media platforms, and banks' fraud-prevention measures. However, there are no easy or universal solutions to the problem of cyber-harms; any solutions presently available are vulnerable to workarounds or can become outdated due to the ever-evolving nature of ICTs.

The next chapter expands on these challenges by examining how specific digital tools and forums, including cryptocurrencies and online misinformation, complicate containment and enforcement efforts by helping to conceal, fund, and amplify harmful acts. The use of these tools has resulted in the private sector, including social media companies, taking on an increasingly active and self-regulated role in managing harmful acts and moderating harmful content.

4

Digital Enablers of Harms

Chapter Findings

- Crowdfunding sites, cryptocurrencies, and the Dark Web have little oversight, can be used to fund and conceal harmful acts online, and can make laws difficult to enforce.
- The Dark Web provides high levels of anonymity to users, which can be exploited to conceal crimes; law enforcement agencies are often unable to dismantle illegal activities taking place on the Dark Web, as malicious actors can adapt and move their operations swiftly.
- Cryptocurrencies expose multiple enforcement and regulatory challenges related to evolving technologies, including difficulties with tracing, insufficient capacity and training within law enforcement and the broader justice system, jurisdictional barriers, and the inability of some laws to be adapted.
- Misinformation can spread easily online and facilitate the creation or propagation of harmful content. Individuals may rely on misinformation to justify subsequent harms or crimes, both online and offline.
- Social media companies have taken some self-regulated actions to moderate harmful content on their platforms, including the removal of misinformation, but issues of transparency, accountability, and consistency persist. Some moderation methods can lead to the over-removal of legal content.

Advances in ICTs have had dramatic impacts on nearly all aspects of daily life, many of which were unforeseen or unexpected. New digital platforms and tools are regularly being brought to market, often without consideration of how they may be exploited for nefarious purposes. This chapter demonstrates how digital tools — such as financial instruments (e.g., cryptocurrencies, crowdfunding sites), the Dark Web, and social media platforms — can facilitate the financing, concealment, and spread of cyber-enabled harmful acts and content, including misinformation. While these tools are not unlawful, they have little oversight, are largely decentralized, and can be used to facilitate criminal or otherwise harmful behaviour, making it more difficult to detect, monitor, and combat harmful acts. These tools ultimately create challenges that may not always be best approached through law enforcement, but rather through some combination of platform self-regulation, digital literacy education, content redirection, and content blocking, among other things.

This chapter begins by describing financial tools that have been used to finance and facilitate a variety of criminal and harmful behaviours. Crowdfunding sites and cryptocurrencies are themselves legal but have emerged as ways to conceal the movement of large amounts of money. In general, regulatory gaps and limited technical resources in law enforcement have made these financial tools attractive to cyber-threat actors.

Next, several common tools for enhancing online anonymity are considered. The Deep Web, Dark Web, and virtual private network (VPN) services allow users to conceal certain kinds of information about themselves or about material being shared. Like other tools discussed in this chapter, they are not inherently illegal and have positive, beneficial uses. Yet, when used by cyber-threat actors, they can obscure important information, such as perpetrators' identities and physical location. In other cases, well-intending users of these tools may be opening channels for cyber-threat actors to cause harm.

A further section covers misinformation and the potential threats that may be associated with its spread. In recent years, misinformation, including visual misinformation (which can range from crude or simplistic to highly sophisticated), has grown increasingly prevalent in online discourse and has been linked to conspiracy beliefs that have inspired harmful and criminal activities. The Panel notes that, largely, these kinds of harm-enabling activities are carried out using services that invite user-generated content, such as social media platforms.

The chapter then deals with social media platforms in general. On one hand, social media platforms connect people around the world in ways that allow for free speech and critical discourse; on the other hand, increased connectivity has also allowed for the creation and sharing of criminal, extremist, and hateful content. Likewise, misinformation and misleading content are also readily shared over social media platforms. This section specifically deals with the ways in which these platforms try to address such harmful behaviours — much of which is through self-regulation, but also through state intervention.

At the conclusion of this chapter, the Panel shows that the capacity of different orders of government, law enforcement, and social media companies to enforce existing laws and policies is constrained, and how current content moderation efforts are ineffective. Alternatively, some preventative tactics are described, including digital literacy education and content redirection and blocking.

4.1 Financial Tools

4.1.1 Crowdfunding Sites

Crowdfunding enables money to be raised "by collecting small, individual contributions from a large pool of donors through online platforms," such as GoFundMe (BDC, 2022). Crowdfunding is used for various beneficial causes, as well as to sometimes finance criminal or otherwise harmful activities. For example, the truck convoy that converged in Ottawa in January 2022 (hereafter referred to as "the convoy"), and which included illegal blockades, was partly funded through crowdfunding donations from both within and outside Canada (SECU, 2022a.) In a statement to Parliament, GoFundMe — a major crowdfunding platform used by the convoy — explained that 88% of the funds raised for the convoy on its platform originated in Canada, with 86% of donors appearing to be from Canada (SECU, 2022b).

There are regulatory gaps and enforcement challenges with crowdfunding sites

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) monitors for transactions linked to groups involved with terrorism and alerts authorities to suspicious financial activities (FINTRAC, 2021b); however, the activities of many extremist groups are missed (Thompson, 2022; Tworek, 2022). Fundraising by extremist groups that violate crowdfunding platforms' terms of service is relatively common and is not a new practice (Tworek, 2022) but, unlike banks and other financial institutions, crowdfunding sites were not required to report suspicious transactions to FINTRAC until early 2022 (GC, 2022a). Barry MacKillop, Deputy Director of FINTRAC's intelligence unit, explained that, although crowdfunding platforms based in the United States were not subject to Canadian laws at the time of the convoy, "payment processors with a Canadian presence and Canadian banks that are used to transfer funds to or from these platforms were subject to the registration and reporting requirements" (SECU, 2022a).

The federal government — using the powers of the *Emergencies Act* — directed all online crowdfunding platforms (including those dealing in cryptocurrencies) to report to FINTRAC if they possessed funds owned by anyone involved in the convoy (FIN, 2022). Though these measures were temporary, the Government of Canada has announced it will introduce legislation to make the reporting requirements of crowdfunding companies clearer (GC, 2022a). This was confirmed in Canada's 2022 budget as part of wider efforts to strengthen anti-money-laundering and anti-terrorist financing legislative and enforcement tools (GC, 2022b).

There are concerns among some that the new rules are examples of government overreach (Durrani *et al.*, 2022) and that requiring companies outside Canada to report to FINTRAC will be difficult to enforce (Karadeglija, 2022). Questions exist about whether the government can actually exercise such authority given how the decentralized and anonymous nature of crowdfunding exchanges already challenges the enforcement of existing regulations (Swartz, 2021). This is compounded by capacity constraints within FINTRAC, the high volumes of data received, and the perception that there are limited repercussions if financial institutions do not comply with reporting requirements (Carvin *et al.*, 2021a).

4.1.2 Cryptocurrencies

Digital currencies are payment systems that allow for payment processes through electronic transactions (Frankenfield, 2022a). Digital currencies (which include debit, credit, and e-transfer exchanges done through traditional banks, as well as virtual currencies) represent a vast and rapidly changing ecosystem of products, only some of which are regulated. Some digital currencies are exchangeable for other currencies, including other types of digital currency or currency issued by a central bank, such as the Canadian dollar (i.e., fiat currency). Some are permanently linked to a specific platform (e.g., in-game currencies that typically cannot be directly redeemed or exchanged for other currencies), while some are rewards points (often redeemed for goods or cash-back offers). Still others, however, do not fit into any classification system (Frankenfield, 2022a).

Virtual currencies, which are often associated with cryptocurrencies, in-game currencies, and rewards points, are a subset of digital currencies that are not associated with or issued by a central bank. Cryptocurrency is a type of open virtual currency that, unlike many types of rewards points or some in-app currencies, can be exchanged for other digital or fiat currencies (Frankenfield, 2021). These are typically, but not always, decentralized currencies that are not controlled or managed by any one institution, and thus stand in contrast to central bank-issued currencies (Frankenfield, 2021). This section focuses on decentralized and open cryptocurrencies because of their growing use in various cyber-enabled crimes.

Cryptocurrencies are decentralized and facilitate user anonymity

Cryptocurrencies are novel financial products first introduced around 2008. More than 1,800 currency types had been created as of 2018, including Bitcoin, Ether, Monero, Ripple, and Litecoin (Kethineni & Cao, 2020). Unlike other payment systems (e.g., cash, credit), cryptocurrencies generally operate independently of a centralized authority (e.g., bank, government) that monitors transaction

legitimacy or the amount of currency in circulation (CRA, 2021). Instead, the system functions through validated public transaction records (Frankenfield, 2022b). For example, Bitcoin uses a combination of cryptography and blockchain technology to track and certify transactions among users (Berentsen & Schär, 2018). In brief, transactions are recorded in "blocks" that are then linked to a public ledger of transactions, which is verified and unalterable; encryption processes using a set of public and private "keys" further ensure a transaction's integrity (Berentsen & Schär, 2018).

Cryptocurrencies have been designed based on privacy and security principles, but different cryptocurrency types offer variable privacy and design features. Monero, for example, offers *stealth addresses,* which are one-time-use wallets created when a user initiates a transaction (Kanstrén, 2021). Other currencies pass transaction information through The Onion Router (Tor),[6] or otherwise do not record the identities or locations of senders. The level of privacy cryptocurrencies have also depends on individual user practices, which can be increased through tactics such as frequently switching pseudonyms or using IP-masking services (Baron *et al.*, 2015). The potential for anonymity, ability to evade taxation, lack of centralized authority, and growth of online dark markets have made cryptocurrencies attractive methods of payment for illegal goods or services; several of the biggest dark markets of the past decade (e.g., Silk Road, AlphaBay, Hansa) all accepted at least one type of cryptocurrency before they were shut down (Kethineni & Cao, 2020). Notably, after being denied service by major credit cards Visa, Mastercard, and Discover for its unsatisfactory moderation of child sexual abuse material (CSAM), Pornhub pivoted to accepting only cryptocurrencies (Goodwin, 2020) (Chapter 3).

Cryptocurrencies can be tools to launder money and finance crimes

As the market for cryptocurrencies grows, so too does the number of cryptocurrency exchanges. Many users choose to perform transactions on decentralized cryptocurrency exchanges (DEXs) in part due to their lower transaction fees, but also because it is easier to operate anonymously (Clark *et al.*, 2022; Khan & Ali Hakami, 2022). Public safety concerns about cryptocurrencies include their potential use as difficult-to-trace tools for laundering money, enabling ransom payments, and financing terrorism, along with other financial crimes (Kethineni & Cao, 2020; Davis, 2021) (Box 4.1). Notably, it has been argued that the ease of cryptocurrency transfers coupled with the difficulty of tracing

6 Anonymous encrypted browsers, such as The Onion Router, are not used exclusively on the Dark Web. These browsers are designed to protect the personal privacy of their users, and thus have multiple beneficial applications (Lukings & Lashkari, 2022b).

them has played a key role in the rise of large ransomware operations (Weaver, 2021). According to the Canadian Centre for Cyber Security (2022a), although "law enforcement has had some success in tracking and, in some cases, recovering stolen funds, cyber threat actors continue to refine and develop techniques for obscuring illicit financial transactions" and "cryptocurrency money laundering will almost certainly continue to facilitate the growth of cybercrime."

Box 4.1 Online Fundraising for Terrorist Activities

Online spaces can be used to "inspire, incite, coordinate, finance and plan acts of violence" (Canada Centre, 2018). Terrorist organizations such as Al-Qaeda, for example, share instructions on how to carry out violent acts online, including the use of weapons. Financial technologies (including cryptocurrencies) have played an important role in funding terrorism in recent years (Davis, 2021). It is not challenging to set up wide-ranging fundraising campaigns on social media to solicit donations, which, upon receipt, can be easily transferred internationally using cryptocurrency platforms and exchanges. Even if social media platforms ban fundraising efforts for terrorist activities, it is possible for fundraisers to contact prospective donors individually using encrypted messaging, which can make it challenging to track, monitor, or interdict such fundraising campaigns (Weimann, 2016; Davis, 2021). These activities can be even more difficult to trace if they migrate to the Dark Web, which has further facilitated coordination efforts among terrorist organizations (Weimann, 2016).

FINTRAC was created in 2000 to meet international anti-money-laundering standards, and was expanded to help identify terrorist financing schemes in 2001 (Carvin *et al.*, 2021a). FINTRAC collects, analyzes, and stores financial information from thousands of sources, including accountants, banking and financial services companies, casinos, and insurance companies. In cases with reasonable grounds to suspect illegal activity, information can be shared with appropriate law enforcement or security agencies (FINTRAC, 2021a). FINTRAC requires the cooperation of intermediaries — those facilitating the transfer and exchange of value — to report large or suspicious financial transfers. It also relies on self-reporting from financial institutions (FINTRAC, 2022), which complicates enforcement efforts given the anonymity of cryptocurrencies and their associated exchanges. In 2019, updated regulations for FINTRAC meant to address virtual

currency (including cryptocurrencies) were adopted. Under the updated regulations, for example, dealers of cryptocurrencies that serve Canadian customers are treated as money service businesses (MSBs), which are subject to FINTRAC's reporting requirements (GC, 2019b; Carvin *et al.*, 2021a) (Chapter 5).

Regulations for cryptocurrencies are difficult to enforce

Cryptocurrencies can share many qualities with traditional currencies and, in some cases, are exchanged like securities or investment products. In Canada, securities and investments are regulated through registration requirements for dealers, advisers, and fund managers; requirements specific to exchanges and marketplaces; and reporting and disclosure requirements (d'Anglejan-Chatillon *et al.*, 2021). With cryptocurrencies, it is not always clear whom to hold accountable for illegal operations, let alone how. DEXs, in particular, often operate with little oversight and have no central, trusted intermediary that performs trades; as such, all transactions are essentially person-to-person (Chainlink, 2022). This introduces several enforcement questions, such as which jurisdictions should be responsible for overseeing any single DEX's legal status, and who counts as a stakeholder in the DEX and is thus responsible for ensuring their DEX is abiding by regulations (GC, 2021c). The Canadian Securities Administrators (CSA) has issued guidelines on trading cryptocurrencies and on what regulations apply to crypto-asset trading platforms (CSA, 2020; CSA & IIROC, 2021). Regulation of securities falls under provincial and territorial jurisdiction and is relatively uniform across the country. However, derivatives based on virtual currencies are regulated by both the provincial/territorial and federal governments (d'Anglejan-Chatillon *et al.*, 2021).

Not all cryptocurrency exchanges are ready to comply with regulations, and some foreign exchanges may choose to leave the Canadian market (Sobowale, 2021). Notably, the CSA announced in August 2022 that members (securities regulators from each province and territory) will now expect crypto trading platforms to register with their principal regulator, and in the meantime, agree to comply with terms and conditions that address investor protection concerns (OSC, 2022). The announcement also states that CSA members may take action if a trading platform is not prepared to comply with this announcement. In the Panel's view, it is sometimes unclear which regulations best apply to cryptocurrencies, or whether stringent regulations should be applied if doing so causes cryptocurrency traders to leave Canadian markets.

A variety of regulatory approaches to cryptocurrencies exist in other jurisdictions. Australia's financial model treats virtual currencies as property (which is also true in Canada when cryptocurrencies are not being traded as securities) and allows exchanges to operate provided they are registered with the Australian Transaction Reports and Analysis Centre (AUSTRAC, 2018; Smith, 2021a).

However, not all countries are taking similar approaches. In the United States (as in Canada), virtual currencies can be considered securities, commodities, currencies, or property depending on whether a user is dealing with the Securities and Exchange Commission, Commodity Futures Trading Commission, Department of the Treasury, or Internal Revenue Service (Smith, 2021a). In the United Kingdom, most cryptocurrency exchanges are required to register with the Financial Conduct Authority (FCA) (Hammond & Ehret, 2021). Additionally, customer due diligence (or "know your customer") and anti-money-laundering regulations, as well as regulations designed to combat the financing of terrorism, have been created by the FCA. As cryptocurrencies are not legal tender in the United Kingdom, taxes are derived from the gains and losses associated with their use, which is limited by a ban on the trading of cryptocurrency derivatives. In the European Union, taxation laws and regulations vary considerably across member states (Hammond & Ehret, 2021).

Some cryptocurrency exchanges, either hoping to supplement or get ahead of government regulation, are opting to self-regulate. On February 7, 2022, a group of 16 exchanges from around the world, convened by the risk-monitoring software company Solidus Labs, announced the launch of the Crypto Market Integrity Coalition (Lang, 2022). The stated goal of the coalition is to "advance the integrity and efficient functioning of digital asset markets" (CMIC, 2022). It aims to uphold market integrity and efficiency regardless of regulatory requirements, and plans to do so by regularly monitoring, detecting, and eliminating unfair market practices (CMIC, 2022). As of December 2022, the coalition was seeking other cryptocurrency trading platforms to sign a "Public and Unequivocal Pledge," but has not made clear any other plans.

Despite efforts to regulate the cryptocurrency space and apply existing regulations, it has been challenging for law enforcement agencies to enforce the legal *use* of cryptocurrencies. Many commonly used cryptocurrencies are theoretically traceable by experts and government agencies, but the small supply of expertise, high cost, and infrastructure required to track transactions and enforce regulations has inspired the Royal Canadian Mounted Police (RCMP) to expand its cryptocurrency program by training more officers to aid in investigations (Northcott, 2022). At the same time, advances that reduce traceability include using DEXs and privacy-enhanced coins, creating convoluted transaction paths by converting illicit funds into different cryptocurrencies or using *tumbler* services that essentially scramble the transaction path for a small fee, are also being adopted (Clark *et al.*, 2022; Europol, 2022; Freeman Law, 2022). In the experience of Panel members, these advanced techniques, in some cases, increase the difficulty of tracing cryptocurrency transactions to a level beyond the ability or capacity of the vast majority of law enforcement agencies.

Cryptocurrency users can be targets of theft and fraud

Between October 2020 and May 2021, the U.S. Federal Trade Commission (FTC) reported over US$80 million in losses due to cryptocurrency investment scams (Fletcher, 2021). Classic phishing, fraud, and extortion-based tactics occur where victims are compelled to transfer cryptocurrency to malicious actors, with the transferred assets often not being insured by an intermediary or governing body (which a traditional online currency might be); this leaves victims with few options to regain their stolen assets (GC, 2021d; AARP, 2022). Cryptocurrency exchanges can also fall victim to theft or bankruptcy (Lane, 2022). Often, when users buy cryptocurrency through an exchange, their assets are held in the exchange's own wallets, whose private keys are known only by that exchange. If a cyber-threat actor compromises the security of an exchange, they may be able to obtain the information required to take control of that exchange's hot wallets (wallets that are actively connected to the network) and thus their customers' assets. In these cases, or in the case of failure for commercial reasons, users have limited options to regain their stolen or lost assets (e.g., AscendEX, BitMart, and Liquid) (Lane, 2022).

A market for stock exchange-style securities based on the value of virtual currencies has also emerged, forcing governments worldwide to consider how this new asset trading type could be regulated (CRA, 2021). As with investments in other volatile markets, the value of the virtual currency being traded can vary widely. Additionally, schemes have been used to affect the value of cryptocurrencies in order to gain an advantage over other traders. One report by Bitwise suggested that as many as 95% of reported Bitcoin trading volume is fake and/or represents non-economic trading, meant to imply the asset is highly liquid (a scheme known as "wash trading") (Bitwise Asset Management, 2019); several other studies vary on the exact percentage, but also find that most reported Bitcoin trading volume is associated with wash trading (Le Pennec *et al.*, 2021). Since these exchanges tend to be unregulated and decentralized, determining whether a source of pricing or exchange data is reliable is no trivial task and an active area of financial analysis research (Vidal-Tomás, 2022).

4.2 Tools for Online Anonymity

4.2.1 The Deep Web and Dark Web

The Dark Web is one part of the Deep Web

Search engines such as Google only scratch the surface of the content contained on the internet (Figure 4.1). The *Deep Web* refers to any part of the internet that is unindexed (i.e., not catalogued by traditional search engines), and accessing it may

require passwords, encryption, or specialized software (Weimann, 2016; Sheils, 2021). Examples of content on the Deep Web include online banking, personal email accounts, user databases, and members-only sites (Lukings & Lashkari, 2022b). The *Dark Web* is a subset of the Deep Web, and can only be accessed through the use of specialized browsers, such as Tor (Weimann, 2016; Chertoff, 2017; Lukings & Lashkari, 2022b). The level of user anonymity is higher on the Dark Web than on the indexed internet (i.e., Open Web) or Deep Web. When using services such as Tor, a person is generally protected from surveillance and identification by potential observers through multiple layers of encryption (Hatta, 2020).

The anonymity and privacy of the Deep Web have made it an important tool for civil advocates such as journalists, activists, and whistleblowers, who may be working in hostile environments; however, it also creates an alluring environment for criminal activities — especially the Dark Web, which can conceal cyber-threat actors (Kalpakis *et al.*, 2016; Lukings & Lashkari, 2022b). For example, one common use of the Dark Web is accessing *dark markets*, which are platforms for selling and buying illegal goods and services, such as CSAM, illicit drugs, counterfeit products, or weapons (Lukings & Lashkari, 2022b). Another common use is to anonymously share links to CSAM (which is itself not hosted on the Dark Web, but rather the Open or Deep Web) (C3P, 2021). The anonymity also makes regulations difficult or nearly impossible to enforce on the Deep Web and Dark Web.

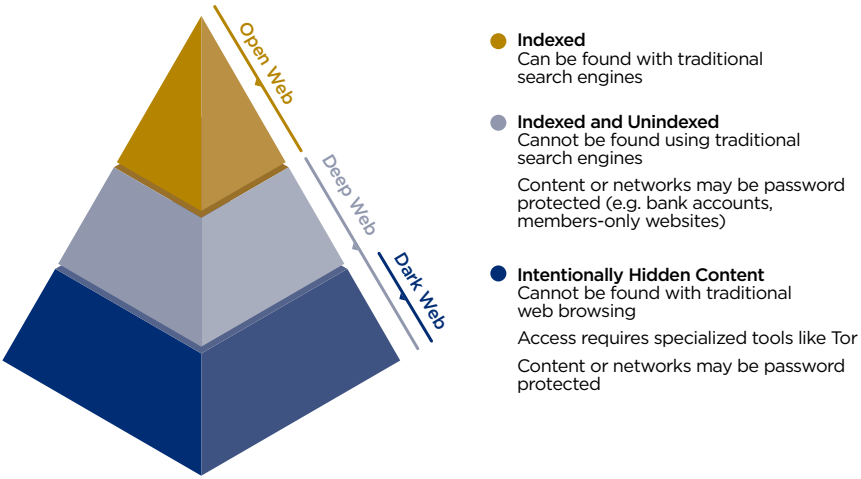


Figure 4.1 Layers of the Internet

The internet can be divided into three parts: the Open Web, which is accessible by traditional web browsers and indexed by search engines; the Deep Web, which is often password-protected; and the Dark Web, which is intentionally hidden. The Dark Web is a subset of the Deep Web.

Determining the amount and types of content on the Dark Web is difficult. At the end of August 2022, there were approximately 2.8 million active Tor users around the world (The Tor Project, 2022), but this does not provide context on what individuals use the service for. Various studies have analyzed sections of content on the Dark Web, but detailed analyses are hard to conduct due to its size and dynamic nature (Monk *et al.*, 2018). Thanks to the high level of anonymity on the Dark Web, cyber-enabled crimes become more difficult to prevent, detect, and enforce (Kalpakis *et al.*, 2016; Lukings & Lashkari, 2022b). Challenges are magnified by jurisdictional complexities related to where a user, server, and crime are situated; this often stymies law enforcement investigations involving these digital spaces (Lukings & Lashkari, 2022b).

Dark markets commonly rely on cryptocurrencies (Patil, 2019), whose anonymity and privacy have made them popular payment methods for many malicious actors, including some terrorist organizations; this has prompted some experts to express concern that virtual currencies will eventually become "criminal currencies" (Kethineni & Cao, 2020). Multiple investigations have shut down dark markets hosted or operated by criminals based in Canada who were involved in the sale of illegal drugs through the Dark Web (Patil, 2019; RCMP, 2020b). AlphaBay, one of the largest dark markets until it was shut down after a global operation in 2017, was created and run by a Canadian citizen (FBI, 2017). However, special police operations to raid dark markets have not had long-term success in decreasing the number of illicit drug dealers, who can adapt their tactics quickly and sell their products elsewhere (Décary-Hétu & Giommoni, 2017).

4.2.2 Virtual Private Networks (VPNs)

VPNs are useful tools when used appropriately, but can also leave users susceptible to different security threats

In the last several years, VPN use by individuals and corporations has increased (Vigderman & Turner, 2022). Via one of several protocols (all of which have a range of privacy and security features), a VPN lets users create a virtual point-to-point connection over the internet to a remote network or IP address — for example, a user in Montréal can make it appear as if they and their device are located in Glasgow. However, not all VPNs offer the same privacy, security, or encryption features; in some cases, the use of a VPN may put a user's privacy and security at risk (Dinha, 2021).

Despite sharing an acronym, the VPNs used by companies serve different purposes and present different risks than the VPNs individuals may use to connect to the internet (Dinha, 2021). A company VPN is typically used to securely connect a remote user to the organization's internal network, which is useful for those who

work remotely and who must access secure company data over untrusted networks. The security of this type of VPN depends on the system being regularly updated to protect against the malicious entities that target it (Palmer, 2021).

Consumer VPNs connect individuals to the internet and may be used for a variety of reasons. One source suggested that avoiding identity theft and securing personal data are two of the more common uses of consumer VPNs, while other users may wish to bypass content restrictions imposed by their communities by obscuring their own IP address (e.g., to access another country's Netflix catalogue or public broadcasting service) (Vigderman & Turner, 2022). VPNs can help with these tasks, but they can also open users up to new risks (Dinha, 2021). Many VPN services are offered online in free and paid form, but there is no guarantee that they provide the privacy, security, and anonymity promised, or that the provider itself will not track or otherwise compromise the user's data or security. As such, it is important for potential VPN users to understand how these tools work and who operates them, and people should only use VPN tools from trusted providers.

4.3 Misinformation

4.3.1 Online Spread of Misinformation

Spreading misinformation is not illegal but can lead to harm

Misinformation is broadly defined as information that is false or misleading (Heer *et al.*, 2021). *Disinformation*, in turn, is a "coordinated or deliberate effort to knowingly circulate misinformation in order to gain money, power, or reputation" (Swire-Thompson & Lazer, 2020). A related concept is *mal-information*, which is real information used to mislead (often through exaggeration) and inflict harm (UNESCO, 2018; Canadian Centre for Cyber Security, 2022b). The Panel uses the term *misinformation* to describe all three in this report, because it can be difficult to determine intent, and because the distinction, ultimately, does not affect the potential impact.

While the spread of online misinformation in and of itself is not a criminal act and usually lies outside the current mandate of law enforcement,[7] it can lead to substantial harms and support or encourage crime (Europol, 2020a); some of the threats and harms that can result are explored in Section 4.4. As demonstrated in this section, misinformation can help motivate hateful and violent acts, and it can be difficult to contain. Notably, this section focuses on ICTs and platforms that rely on user-generated content, which suggests that misinformation is a complex,

7 The Canadian Security Intelligence Service (CSIS) is mandated to investigate and identify disinformation campaigns, often perpetrated by foreign actors, that have national security implications, including influencing Canadian democratic processes (CSIS, 2021a).

multi-headed issue with no single ideological cause or method of transmission. Combatting misinformation online requires a holistic approach that goes beyond content alone (Tworek, 2020).

ICTs can facilitate the spread of misinformation

Misinformation has historically spread through different forums and media for political and economic reasons; it has long been used as a tool of warfare, to influence economic outcomes, and to erode trust in institutions (Rid, 2020). ICTs can facilitate the rapid spread of information on an even larger scale than was previously possible using print, radio, or television distribution channels, making misinformation harder to control than in previous generations (Rid, 2020). Moreover, given the speed and distance it can cover, contemporary misinformation can spread rapidly, on larger scales, and across broader geographic regions. An analysis by Shao *et al.* (2018) looked at 14 million messages on Twitter and found that social bots — software-controlled profiles on social media that can be used to communicate useful information — also play a disproportionate role in spreading misinformation, especially early on, before content goes viral. Evidence suggests that false information online spreads faster and more broadly than truthful information, and misinformation about politics spreads faster than other types of misinformation (Vosoughi *et al.*, 2018).

As in other countries, people in Canada are living in a polarized society (Owen *et al.*, 2019). Recent evidence shows that ICTs do not inherently cause polarization, however. Polarization online can be driven by external (offline) events — such as the decline of perceived legitimacy of government institutions — that are unrelated to activity occurring on online platforms (Benkler *et al.*, 2018; Owen *et al.*, 2019; Bennett & Livingston, 2020; Waller & Anderson, 2021). At the same time, misinformation circulated online impacts people's beliefs. For example, a survey of 1,000 people in Quebec found that more than 20% of participants believed or agreed with objectively false conspiracy theories or misinformation circulated on the internet (Langlois & Sauvageau, 2021). The same study also found young people were significantly more likely to believe these false ideas.

The design of many social media platforms can help amplify particular forms of content. The Canadian Centre for Cyber Security (2022a) states that social media algorithms have almost certainly contributed to the spread of misinformation. To generate more engagement among users, Facebook's algorithm systematically favours (and amplifies) emotional or provocative content, which is more likely to contain misinformation (Merrill & Oremus, 2021). Contemporary online platforms have significantly displaced traditional media sources, which typically involve some form of editorial oversight to evaluate the veracity of information and

determine what should be shared (Trudel, 2021). Online platforms have deprioritized editorial functions in favour of automated ones intended to incite emotional responses to information.

Misinformation can cause direct and indirect harms, including instigating hate and facilitating fraud

In Canada, the proliferation of misinformation online has contributed to a rise in discrimination, marginalization, and hate (Tenove *et al.*, 2018; Heer *et al.*, 2021). For example, false or misleading information on social media linking the Muslim community to COVID-19 outbreaks has contributed to Islamophobia (Al-Qazzaz, 2020). Similarly, reported incidents of anti-Asian racism (including online) rose in 2020 and 2021 (Macguire, 2020; Kong *et al.*, 2021), which may be linked to misinformation on social media platforms about the origins and spread of COVID-19 (Section 3.2.2). Misinformation is also associated with discrimination and prejudice. Experiments have shown that exposure to conspiracy theories about Jewish people and immigrants to the United Kingdom exacerbated prejudice toward these groups (Jolley *et al.*, 2020). Misinformation about particular communities or identities can be circulated online with the intent to discredit or denigrate them (Tenove & Tworek, 2019); as discussed in Section 3.2.2, groups with hateful ideologies use ICTs to disseminate their messages and find supporters (Tenove *et al.*, 2018).

In some cases, misinformation can be used to support or motivate cyber-enabled crime. The COVID-19 pandemic, for example, created opportunities for cyber threat actors to exploit the increased vulnerability of users for their own gains (OECD, 2020a). The spread of misinformation about so-called cures for COVID-19 has been used to help sell unregulated and possibly harmful products to people online, including through the Dark Web (Europol, 2020a; OECD, 2020b). Misinformation has also been linked to cybercrime by making phishing attacks more effective and increasingly facilitating hybrid threats (which "combine conventional and unconventional, military and non-military activities [...] to achieve political aims") (Europol, 2020b).

Misinformation can affect democratic processes and freedom of expression

Canada's *Elections Modernization Act* addresses misinformation and foreign interference in elections by prohibiting foreign entities and individuals from buying advertisements during an election period, and by requiring online platforms to publish a registry of partisan advertising conducted during an election (GC, 2018a). CSIS, however, has warned that people in Canada are often

targeted by online misinformation campaigns from various cyber-threat actors, including those sponsored by foreign states, which has national security implications (CSIS, 2018, 2021b). Such misinformation campaigns on social media, including web brigades, are often intended to increase polarization, and undermine trust in different orders of government, institutions, and democratic processes (CSIS, 2021b). For example, a report exploring misinformation spread during Canada's 2021 federal election found that different groups growing more distrustful of government experts and mainstream media have begun to coalesce, forming a "big tent" community of misinformation that further exposes members to news and ideas that tend to be highly ideologically motivated (Bridgman *et al.*, 2022). At the same time, research suggests false rumours (i.e., misinformation) are more likely to emerge and re-emerge multiple times on Twitter compared to true rumours (i.e., facts) (Shin *et al.*, 2018). Similarly, the infusion of a large volume of misinformation can disempower people by negatively impacting their ability to search, receive, and share truthful information, and to form opinions and beliefs autonomously (Khan, 2021).

4.3.2 Conspiracy Beliefs

Conspiracy theories constitute one type of misinformation and are often politically motivated. Such theories often seek to "explain events or practices in terms of actors secretly abusing their power to accomplish their [own] goals" (Craft *et al.*, 2017), and they can emerge in response to a range of social and economic factors, including distrust in institutions, resentment of elites rooted in rising inequality, and racism (Tworek, 2020).

Social media enables conspiracy ideation

The importance of social media platforms when it comes to the spread of conspiracy theories is elevated because they are often used as a source of news. For example, 24% of people in Canada report they use Facebook as a news source and 24% reported using YouTube for the same purpose (Andrey *et al.*, 2021b). Social media users in Canada also show interest in political discourse; one survey found that 33% of people in Canada use social media platforms at least once a week to share news or political posts, while 30% comment on news or political posts with similar frequency (Andrey *et al.*, 2021b).

Using social media for news is positively correlated with beliefs in conspiracy theories and misinformation (Enders *et al.*, 2021), even when controlling for other factors, such as use of news media, partisanship, age, and education (Stecula & Pickup, 2021). The social media users most likely to spread misinformation are those who most access polarizing content related to conspiracy ideation

(Bessi *et al.*, 2016). Not all platforms have the same effect, however; some U.S. studies published in 2021 suggested that, when individuals used Facebook or YouTube for news, they were more likely to adopt conspiracy beliefs than those who principally used Twitter to obtain their news (Stecula & Pickup, 2021; Theocharis *et al.*, 2021).

Conspiracy beliefs can motivate criminal acts, including violence

Studies have found positive correlations between beliefs in conspiracy theories and criminal behaviours and intentions (Uscinski & Parent, 2014; Jolley *et al.*, 2019; Rottweiler & Gill, 2020). Experimental evidence suggests that being exposed to conspiracy-related material plays a role in increasing intentions to commit common crime (e.g., running red lights, using cash to avoid paying tax) in the future (Jolley *et al.*, 2019). People with especially strong conspiratorial predispositions are more likely to be inclined to violent actions (Uscinski & Parent, 2014; Rottweiler & Gill, 2020). As demonstrated in subsequent sections of this chapter, people may rely on misinformation — which facilitates radicalization and extremism — to justify offline violence and other harms (including vandalism), which may lead to social unrest. As with other forms of online harassment and harm, certain public-facing professions may be targeted more than others (Section 3.1.2).

The link between conspiracy theories and criminal behaviour has been observed in the context of the COVID-19 pandemic. For instance, false COVID-19 claims that radio waves emitted by 5G towers make people more vulnerable to COVID-19 contributed to anger against governments and even violent responses (Devlin, 2020; Jolley & Paterson, 2020). In the Canadian context, Global News obtained a confidential CSIS report in 2020 warning about conspiracy theories linking COVID-19 to 5G technology, expressing concern that "ideologically motivated violent extremists" may engage in acts of arson and vandalism against 5G infrastructure (Bell, 2020). Police investigated the potential role conspiracy theories may have played following the arrest of two people in Quebec for setting fire to several cell towers, none of which carried 5G technology (Bellemare *et al.*, 2020). Similar attacks occurred elsewhere in the world (Cerulus, 2020; OECD, 2020b), which had the potential to impair the functionality of emergency service systems (Devlin, 2020).

Entrenched beliefs in conspiracy theories are at the core of some violent extremist movements

Conspiracy theories and violent extremism are increasingly intertwined (SECU, 2022a). QAnon, one of the most well-documented examples of political misinformation motivating violence (Winter, 2019; Garry *et al.*, 2021), is a set of conspiracy theories falsely claiming that "a group of Satan-worshipping elites who run a child sex ring" are attempting to control American politics and media (Ipsos & NPR, 2020). The movement originated and proliferated online, and social media facilitated the dissemination of QAnon-related misinformation (Garry *et al.*, 2021; Roose, 2021; Lin *et al.*, 2022). Its members are highly active online; on Twitter, for example, QAnon-related hashtags and phrases were used over 20 million times between January and September 2020 (BBC News, 2021). Some of its adherents have taken action offline, such as participating in the violent and deadly attack on the U.S. Capitol in January 2021 (Garry *et al.*, 2021; Roose, 2021), which was mostly planned online (Frenkel, 2021). It has been reported that other QAnon supporters have been charged with violent crimes, including kidnapping and assassination plots (Roose, 2021).

Though some social networks banned QAnon content from their platforms, citing the risk of offline harm (Roose, 2021), the movement's conspiracy theories continue to circulate. The Federal Bureau of Investigation (FBI) has warned that conspiracy theories are a new domestic terrorism threat in the United States (Winter, 2019). Warnings of rising violence from domestic extremist groups, including those motivated by conspiracy theories, have also been issued by the U.S. Department of Homeland Security (DHS, 2021).

While QAnon theories primarily focus on the United States, Canada is not immune to public safety concerns rooted in such misinformation (Box 4.2). A social media analysis found that Canada is the third-most-active country driving QAnon content on Twitter (Gallagher *et al.*, 2020). Exposure to U.S.-based Twitter accounts is associated with an increased likelihood of posting misinformation on Canadian-based accounts (Bridgman *et al.*, 2021). An online environmental scan of right-wing extremism found that right-wing extremists in Canada often discuss unfounded conspiracy theories and misinformation about U.S. politics more frequently than they do Canadian politics (Hart *et al.*, 2021). The same study found that Canada was the third-most-mentioned country among online right-wing extremists in the United States (Hart *et al.*, 2021).

Box 4.2. Conspiracy Theories Linked to Public Safety in Canada

Rideau Hall incident: On July 2020, an armed man was arrested after ramming a pickup truck through the pedestrian gate of Rideau Hall in Ottawa, home to the Prime Minister of Canada and the Governor General — neither of whom were present at the time of the incident (ONCJ, 2021). The suspect was subsequently charged with 22 crimes, including misusing prohibited weapons and uttering threats (ONCJ, 2021). While the RCMP did not comment on the suspect's specific motive, journalists found posts about QAnon and other false conspiracy theories on his social media accounts, including some posted shortly before the incident (Boutilier & Ling, 2020).

The convoy: The convoy that converged in Ottawa in January 2022 led to massive disruptions in the city, over 200 arrests, and the first-ever use of the *Emergencies Act* in Canada (Fraser, 2022; Tunney, 2022). The convoy was a complex and multifaceted phenomenon; while many in the convoy protested vaccine mandates, substantial elements of the movement more generally coalesced around conspiracy theories and violent anti-government ideology, identified as a national security threat by CSIS (DEDC, 2022). Some of the convoy's leaders and participants supported QAnon and falsely claimed that the World Economic Forum intends to impose totalitarianism (Ling, 2022). Partly motivated by these grievances and conspiracy theories, convoy organizers rallied supporters to raise funds on social media, and ultimately propelled a movement that continues to proliferate online (Ling, 2022).

4.3.3 Visual Misinformation

Visual misinformation comes in many forms, with varying levels of sophistication

Visuals are effective tools for framing and emphasizing specific issues, which is reflected by their prevalence in news coverage and online media (Powell *et al.*, 2015). The varied ways in which visual misinformation can be created or communicated can make it challenging to assess how it affects viewers, especially when received over social media (Powell *et al.*, 2015; Hameleers *et al.*, 2020; Brennen *et al.*, 2021). Digital image manipulation techniques have become increasingly accessible (Paris & Donovan, 2019). Some use deepfake technology (Section 3.1), where full image synthesis techniques can create entirely fictional yet highly realistic images (Khoo *et al.*, 2021). Notably, fake social media profiles with synthetic photographs of non-existing individuals have been used to

facilitate fraud and misinformation campaigns (Ajder *et al.*, 2019; Carlini & Farid, 2020). Visual manipulation can also be done using rudimentary editing (e.g., cut-and-paste) to share information out of context or in intentionally deceptive ways (Paris & Donovan, 2019; Brennen *et al.*, 2021; Khoo *et al.*, 2021).

Visual misinformation is more difficult to combat than text-based misinformation

Analyzing visual misinformation requires researchers or organizations to collect, store, and analyze large amounts of data to train automated detection systems (Brennen *et al.*, 2021). Likewise, visual content propagates further and faster than online moderation teams and researchers can find and track it using existing tools (Paris & Donovan, 2019). While techniques to identify manipulated media are improving (Rao *et al.*, 2021), current research and interventions are largely reactionary and address existing manipulation techniques (Paris & Donovan, 2019; Khoo *et al.*, 2021). Just as text-based information can be misleading depending on how it is interpreted, classifying visual media as "real" or "fake" can present similar challenges, on the basis that public interpretation of an image can vary depending on a range of factors, including paired text (Matthes *et al.*, 2021; von Sikorski, 2021). For example, when real, unaltered visuals are shared without context, or in combination with misleading descriptions, they can go viral and provoke fear or public outrage (Paris & Donovan, 2019; Dan *et al.*, 2021).

While fact checking can be used to explain away some visual misinformation, the process can be resource-intensive when specialized expertise is required to determine if an image has been manipulated (Brennen *et al.*, 2021; Khoo *et al.*, 2021). Total visual deception is not necessary for a misinformation campaign to confuse audiences, evoke an emotional response, or sow distrust in legitimate news; in other words, visuals can generate strong emotional responses or uncertainty in viewers even if they are aware that the information they see is inaccurate (Vaccari & Chadwick, 2020; Dan *et al.*, 2021). Nonetheless, while there are clear linkages between seeing visual misinformation and having emotional reactions, less is known about how visual information is created or the extent to which it is used to inspire people to act offline (Dan *et al.*, 2021).

Even though the technologies used to create, propagate, and identify visual misinformation have improved over the past few years, there has not been a corresponding development and adoption of social, political, and economic practices to help address this kind of misinformation (Paris & Donovan, 2019; Dan *et al.*, 2021). The same social media platforms that rely on users to create and share content struggle to moderate what has been produced (Section 4.4). Indeed, given existing technical tools and regulatory attempts, it is often unclear who can, or should, be held accountable when problematic content is generated, shared, or re-shared on the platforms.

4.4 Social Media Platforms

4.4.1 Criminal Content

Criminal content on social media platforms is on the rise

As noted in the previous chapter, many cyber-enabled crimes or harmful behaviours are carried out over largely self-regulated social media platforms. For example, a survey of 38 police forces from England and Wales revealed that, during the first three months of COVID-19 lockdowns, communication for over 50% of child-grooming crimes happened over Meta-owned apps such as Instagram, Facebook, and WhatsApp, while 20% happened over Snapchat (NSPCC, 2020). This section provides an overview of various self-regulating actions that social media companies have taken to moderate, remove, and otherwise combat harmful content on their platforms, including extremist and hateful content and misinformation. While there is evidence of successful interventions in specific instances, as well as promising and emerging approaches being rolled out, persistent issues of trust (Box 4.3), transparency, accountability, and consistency have made content moderation attempts inadequate to date. In particular, the way platforms decide to respond to public pressure and their decisions around self-regulation can lead to an inconsistent and shifting landscape of what is and is not allowed across social media platforms (Cusumano *et al.*, 2021; Ghosh, 2021a) (Box 4.4).

Box 4.3 Low Levels of Public Trust in Social Media Companies

Despite the popularity of social media platforms as aggregators of news and information sharing, there is low trust in the ability of such companies to address misinformation. Survey results suggest that people in Canada "do not trust social media platforms to act in the public's best interest." Trust in social media platforms (e.g., Facebook, TikTok, WhatsApp) is lower than in oil companies (Imperial Oil, Shell Canada), big technology companies (Google, Apple), and telecommunications providers (Bell Canada). Survey results suggest that efforts made by social media platforms to combat misinformation (e.g., enhanced fact checking) did not have a substantial effect on how the Canadian public perceived social media companies between 2019 and 2021.

(Andrey *et al.*, 2021b)

4.4.2 Extremist Content

Social media platforms have taken actions to remove extremist content, with mixed results

Social media companies have taken steps to combat extremist content with variable effects. Meta, for example, bans groups on Facebook that "proclaim a hateful and violent mission" and removes content that "represents, praises or supports them" (Facebook Canada, 2021). Similarly, approximately half of YouTube channels and private Facebook groups with this content in 2019 became inactive in 2020 (Hart *et al.*, 2021). However, new channels and pages with right-wing extremist content often quickly replace the old, which currently impairs the ability to significantly reduce these kinds of channels and pages in the long term (Hart *et al.*, 2021). With the exception of YouTube, where researchers observed a notable decrease in the volume of right-wing extremist content, more right-wing extremist activity was detected on social media platforms in 2020 than in 2019 (Hart *et al.*, 2021). As the industry matures, it is increasingly apparent that different methodologies may be more effective to address various content types. This view was observed in a survey of relevant employees of social media and messaging app companies, which showed that, while automated content scanning is seen as relatively effective in detecting known CSAM, it is less effective for detecting extremist or terrorism-related content (Pfefferkorn, 2022).

Box 4.4 Financial Incentives and the Design of Social Media Platforms

Social media companies are some of the most profitable companies in the world, and yet, their business models largely depend on providing free services to their users. A 1973 short film entitled "Television Delivers People," by artists Richard Serra and Carlota Fay Schoolman, suggested that, if a service (e.g., television) is free, the viewer must then be the product. This idea has been used to describe the business model many social media companies follow: providing a free service to the public, whose attention is then delivered to advertisers for profit (McFarlane, 2021). Therefore, any decision a social media company makes that could influence user engagement, such as content moderation (e.g., increasing/decreasing the visibility of posts, changing the algorithms used to display content and advertisements, blocking/banning users), has the potential to affect profitability (Grygiel & Brown, 2019).

(Continues)

(Continued)

In other words, content moderation decisions are about more than respecting open discourse and the safety of users; they are also financial decisions — a consequence of the very design of many of these platforms. For many companies, content moderation is done internally or outsourced, requiring company resources either way. Meanwhile, the incentives for diverting resources into content moderation can be minimal and minimally effective, leading to calls for better self-regulation and legislative reform (Cusumano *et al.*, 2021; Ghosh, 2021a). Moreover, the ways users engage with online platforms are subject to design choices made by the platforms themselves. Users are presented with online communities and services built on sociotechnical affordances — such as reposting, "liking," or commenting directly on posts — that are defined by the relationship among user action, platform, and social context, which can influence the behaviour and retention of users on any platform (Leonardi & Vaast, 2016). For example, Twitter allows users to "like" posts (which may increase the frequency those posts are shown to others) but does not offer the option to "dislike" posts. This design choice could significantly affect what users choose to post, what they get to see, and whether they will continue to use the platform, all of which impacts the platform's marketability to advertisers.

Social media companies have adapted their tactics to address violent extremist content. Meta, as an example, continually updates its content moderation policies in response to guidance from experts and other parties. As of 2020, Holocaust denial content is subject to removal, and Meta expanded its Dangerous Individuals and Organizations policy to include those that do not directly incite violence but nevertheless pose a risk to public safety because they celebrate violent acts (Facebook Canada, 2021). Action is taken against individuals on this list; some have been removed from Facebook altogether (Facebook Canada, 2021). It appears, however, that decisions related to public safety are made *ad hoc*, leading civil society groups to raise concerns about how and why organizations or individuals are included in this list, with some calling for Meta to adopt a more systematic method to remove all content under this category (Horwitz & Scheck, 2021). The individuals responsible for actually carrying out moderation reviews for large platform companies often operate in poor working conditions and experience psychological harms due to the nature of their work, which requires them to view and remove harmful and offensive material, including terrorist content, from the respective companies' platforms (Box 4.5).

Box 4.5 Poor Working Conditions of Content Moderators

Social media platforms use artificial intelligence (AI) for some content moderation, but they also rely on human moderators who decide whether illegal and/or harmful content (e.g., CSAM, violent content) needs to be removed (Dwoskin *et al.*, 2019; Roberts, 2019; Llansó, 2020). A large number of content moderation jobs are outsourced to third-party contractors around the world, often outside North America, where there have been reports of exploitative labour practices, inadequate compensation, and little support to address the psychological impacts resulting from workers' ongoing exposure to harmful content (Dwoskin *et al.*, 2019; Perrigo, 2022). The same claims have been made related to third-party content moderators within North America, as well (Newton, 2019).

Social media companies have launched some coordinated, self-regulated efforts. For example, the Global Internet Forum to Counter Terrorism (GIFCT) was established as a collaboration among Microsoft, YouTube, Facebook, and Twitter in 2017, and later developed into a non-governmental organization (GIFCT, 2020). GIFCT is a membership-based organization for technology companies that coordinates the sharing of information, research, and strategies among members to combat the spread of online terrorist and extremist violent content. Members have access to joint initiatives, such as a content identification platform, URL sharing, and a shared content incident protocol. GIFCT also funds research on terrorism and technology, and hosts training sessions in partnership with other organizations (e.g., Tech Against Terrorism) (GIFCT, 2020). However, some legal experts have raised accountability concerns, including critiques that GIFCT lacks adequate oversight and transparency; there are no processes for auditing or challenging GIFCT decisions (Douek, 2020).

The fact that larger social media platforms remove content that violates their community standards is likely a primary reason why many extremist groups are highly active on "fringe" platforms (Hart *et al.*, 2021). Preferred fringe platforms include Gab, Telegram, BitChute, and Odysee, all of which have less stringent content moderation than mainstream platforms (Hart *et al.*, 2021); audio applications, such as Clubhouse, allow users to communicate in audio chatrooms with large audiences (Dwoskin *et al.*, 2021a). Telegram, a Dubai-based social media app used notably by pro-democracy protesters in Hong Kong and by Islamic extremists, increased its U.S. user base around the January 6th Capitol insurrection (Molla, 2021). Fringe platforms play a disproportionate role in incubating and amplifying groups designated as

terrorist organizations in Canada (Hart *et al.*, 2021). Much less is known about moderation actions taken by smaller social media sites, highlighting the importance of providing support to develop companies' capacity to address the promotion and circulation of extremist content as well as fund research to study smaller and emerging networks (Canada Centre, 2018; SECU, 2022a).

4.4.3 Hateful Content

The ways in which social media platforms moderate hateful content raise concerns

Corporate, instead of state, actors are principally responsible for detecting and controlling online hate speech (Ullmann & Tomalin, 2020). Most major social networking companies, such as Meta, Google, and Twitter, have their own definitions, user guidelines, and corporate policies with respect to hate speech. As currently designed and implemented, these guidelines and policies tend to be reactive, insofar as companies typically only respond to hate messages after they have been posted and reported by users (Ullmann & Tomalin, 2020). While automated content removal tools exist, there are technical challenges to their implementation that need to be overcome. For example, because there are biases and little social context within the data used to train AI hate speech moderation systems, content posted by members of marginalized communities is more likely to be labelled as offensive, potentially leading to the over-removal of harmless content (Sap *et al.*, 2019; Dias Oliva *et al.*, 2021). This is likely one reason why most companies currently tend to rely on human moderators to assess most of the reported content and to decide whether said content meets the threshold for removal (Ullmann & Tomalin, 2020).

Further complicating the moderation of online hate is the fact that full transparency of social media platforms' practices has been elusive. According to Frances Haugen, a former Meta employee and whistleblower, "almost no one outside of Facebook knows what happens inside Facebook. The company's leadership keeps vital information from the public, the U.S. government, its shareholders and governments around the world" (Haugen, 2021). With respect to monitoring online hate, internal documents from Meta revealed a leadership hesitant to implement forceful actions to address online hate content in the name of so-called "neutral" or "race-blind" stances (Dwoskin *et al.*, 2021b). Furthermore, records indicate that algorithms implemented in 2015 to identify and remove hate speech consistently failed to remove content that put the site's most-targeted groups (Black, Muslim, LGBTIQ+, and Jewish people) at risk. Meta's policies may affect who uses its services, as suggested by the number of Black

users leaving Facebook, potentially in part out of concerns for their safety and well-being (Dwoskin *et al.*, 2021b).

Data collection or surveillance practices can also deter online use or cause people to self-censor or self-regulate their own right of free expression, causing a chilling effect (Solove, 2006). These surveillance practices may be used by law enforcement or companies themselves. For example, most major online platforms, including Facebook, YouTube, Twitter, and Google, use "notice and take-down" systems that allow individual users to report illegal or objectionable content (Keller, 2021). Due to the massive number of take-down requests received, companies may either process removal requests without valid legal reason, or investigate but err in their final judgment — ultimately removing legal content (Keller, 2021). Either way, the result may be the over-removal of online content and the potential to create hesitancy among users to post freely and fully exercise their freedom of expression.

4.4.4 Misinformation and Misleading Content

Tactics by social media platforms to remove misinformation have had limited success

Most social media platforms have taken some steps to combat misinformation. These actions often strive to balance freedom of speech with protection from harms (e.g., Facebook Oversight Board, 2019), but have had limited success and raised multiple concerns. Social media platforms have developed policies that dictate what qualifies as misinformation and have demonstrated some ability to slow its proliferation. For example, in the aftermath of the attack on the U.S. Capitol in January 2021, Facebook removed posts, groups, and users promoting QAnon conspiracies based on its Coordinating Harm and Promoting Crime policy (Booker, 2021). Similarly, Twitter cited the need to take "strong enforcement action on behavior that has the potential to lead to offline harm;" the platform suspended more than 70,000 accounts sharing QAnon content in less than a week (Twitter, 2021a).

In January 2019, YouTube announced its intention to curb the spread of videos "that could misinform users in harmful ways" (YouTube, 2019). A study examining 8 million YouTube recommendations over a 15-month period found the platform was able to reduce video recommendations for conspiracy theories through its algorithm (Faddoul *et al.*, 2020). While the intervention nearly eliminated some conspiracy theories from its recommendations, particularly those surrounding highly publicized topics, others were barely impacted (Faddoul *et al.*, 2020).

Some social media companies have used external groups to help deal with misinformation. Meta and TikTok have formed partnerships with third-party

fact-checking companies to fight misinformation (Facebook, 2020b; Ardill, 2021). For example, for false claims that do not violate Facebook Community Standards, independent fact-checking partners identify, review, and rate viral misinformation; claims that do violate Facebook Community Standards, such as incitements to violence, are often removed by Meta itself (Facebook Canada, 2021). If a fact-checker deems a piece of content false, Facebook reduces its distribution, notifies users who try to share the content (or previously shared it), and puts warning labels with links to a fact-checker's article disproving the false claim (except in specific cases where it will be removed, as explained below). Meta also uses automation, such as AI, to detect and remove fake accounts (Facebook Canada, 2021), but evidence shows that machine-based fact checking needs to be complemented by human fact-checkers to avoid the over-removal of non-harmful content (OECD, 2020b).

Evidence indicates that fact checking alone is not a silver bullet (Tenove & Tworek, 2019). One experiment-based study found that attaching warnings to the headlines of news identified as false by third-party fact-checkers does "lead to a modest reduction in the perceived accuracy of false headlines" (Pennycook *et al.*, 2020). However, false headlines that were not flagged were perceived as "validated" and more accurate than a control, and thus given more consideration for sharing on social media. Subsequent research suggests that one way of improving the quality of shared content may involve nudging users to pay attention to accuracy (e.g., by sending them a message on Twitter asking their opinion about the accuracy of a headline) (Pennycook *et al.*, 2021). In addition to fact checking, some social media platforms have sought advice and guidance from advisory groups or independent review committees on policy development and implementation surrounding content moderation (Box 4.6).

Box 4.6 The Oversight Board for Meta

A notable example of an independent review group for online content is the Oversight Board established by Meta. It is composed of experts from around the world who review select cases related to content moderation decisions by Meta, then provide binding decisions that "Facebook will implement [promptly], unless implementation [...] could violate the law" (Facebook Oversight Board, 2019). This board is intended to serve as a kind of tribunal for judgments, though there have been criticisms related to its structure and composition, whether it can truly be independent from Meta, and whether it can adequately deal with the scale and diversity of Facebook content (Klonick, 2020).

(Continues)

(Continued)

An example of the board's work includes reviewing then-President Donald Trump's comments on Facebook and Instagram during the January 6th riots at the U.S. Capitol and Meta's subsequent decision to remove the comments and suspend the President's account (Facebook Oversight Board, 2021). The board upheld Meta's decision to block access to the account but ruled that "indefinite suspension" was not appropriate and stated that Meta should be transparent about "the rules that it uses when it imposes account-level sanctions against influential users," impose (and explain) time-limited suspensions, and evaluate whether the risk "recede[s] before the suspension ends," among other recommendations (Facebook Oversight Board, 2021).

Content removal policies are inconsistent across platforms, and moderation is under-resourced

Some experts have argued that the actions taken by social media companies to date have been insufficient to curb the spread of large volumes of misinformation (Bellemare & Ho, 2020). As in the case of hate speech, a common critique is that companies' measures tend to be reactive, and are inconsistent across platforms (Heer *et al.*, 2021). Each platform decides what qualifies as misinformation and determines the appropriate intervention. Meta, for example, generally allows political misinformation but, in the past, has de-emphasized it in Facebook news feeds, removed misinformation related to COVID-19 if it "could lead to imminent physical harm" (Facebook, 2020b), and banned misinformation related to voting (e.g., posting false voting hours) (Leinwand, 2018). Twitter, meanwhile, has used a graded scale of options that range from labelling a tweet as misleading or sensitive to removing tweets and even potentially suspending the associated account (Twitter, 2021b). In other words, content that spreads on one platform might be shadow banned (a method of blocking a user from a platform without their knowledge, usually by making their posts invisible to other users) on another, or lead to account termination on yet other platforms. As a result, users lack predictability and, since policies can be quickly updated, regulators and researchers may find it challenging to compare companies' policies directly and systematically.

The language of misinformation impacts the likelihood it will be detected. There are too few human moderators with the necessary language skills and local cultural context to identify and remove harmful and false Facebook content from users in several developing countries; while AI systems can help, they do not work effectively against many of the languages used by Facebook users (Culliford & Heath, 2021; Scheck *et al.*, 2021). Over 90% of monthly Facebook users are outside

the United States and Canada; yet, out of the 3.2 million hours devoted to removing or labelling false content in 2020, Meta employees and contractors only spent 13% of that time on non-American content (Scheck *et al.*, 2021). The limited language capacity of moderators may affect Canada given that 12% of people in the country primarily speak a language other than English or French at home (StatCan, 2018), and newcomers have been targeted by online misinformation campaigns in non-official languages (Edmonds & Flahault, 2021).

Encryption and lack of transparency are ongoing challenges for social media companies

Platforms that encrypt messages, such as WhatsApp, can have a more difficult time monitoring for misinformation because they cannot read personal messages (Gupta & Taneja, 2018). However, one study shows that social media platforms and messaging apps tend to rely on user-driven abuse-reporting tools to combat misinformation, as well as metadata such as account usernames, frequency or volume of account actions, and previous reports of abuse, rather than accessing content sent among users, encrypted or not (Pfefferkorn, 2022). Some researchers have raised questions about measures adopted by social media companies; for example, messaging services are not particularly transparent — and thus understandable to users — and the efficacy of measures adopted are often unclear (Heer *et al.*, 2021). Granting independent researchers' greater access to social media companies' data would allow for an independent evaluation of companies' claims, although policies will also be needed to ensure the privacy or security of social media companies' user base and platforms (Tenove & Tworek, 2019).

Big social media platforms can reduce the spread of misinformation, but not eliminate it

Efforts by social media companies to impede the spread of conspiracy theories and other types of misinformation may have unintended consequences. While there is some disagreement about whether banning accounts from mainstream sites is effective in the long term, evidence points to noteworthy trade-offs when using such tactics. In particular, measures to remove misinformation and other types of harmful online content can force the individuals producing such content to move to fringe websites and platforms. After the attack on the U.S. Capitol in January 2021, Facebook, Twitter, and YouTube banned thousands of accounts promoting QAnon, but the conspiracy theory persisted because adherents migrated to sites such as Gab and Telegram (Bond, 2021).

It is harder to control the spread of conspiracy theories among fringe sites, and, once there, individuals may be exposed to even more extremist content and potentially further radicalized (Bond, 2021) (Section 3.2). At the same time,

removing accounts with a prominent social media presence and a large following has been shown to dramatically reduce the spread of misinformation on social media within days (Ghosh, 2021b). Building on these trade-offs, one study found that two communities banned from Reddit that migrated to fringe sites resulted in an overall reduction of posts, active users, and new users, though the users who remained tended to generate content exhibiting increased levels of toxicity and radicalization (Horta Ribeiro *et al.*, 2021).

4.5 Preventative Tactics

4.5.1 Digital Literacy Education

A range of promising programs seek to increase digital literacy

In addition to actions taken by social media companies (Section 4.4) and regulatory tools (Chapter 5), teaching digital, media, and information literacy skills can empower people to more critically assess online information, identify hateful content and misinformation, seek credible sources of information, and reduce the risk of becoming a victim of cyber-enabled crimes (OECD, 2020b; OPC, 2022). The Government of Canada has funded 50 literacy initiatives led by universities and non-governmental organizations to address online misinformation (De Coninck *et al.*, 2021). The Organisation for Economic Co-operation and Development (OECD, 2020b) notes that robust partnerships among social media platforms, governments, news media, and educators are critical for the success of these initiatives.

Educational tools to improve digital literacy can be effective. One study found that digital media literacy interventions among a nationally representative sample of Americans improved discernment between truthful and false news headlines by 27% (Guess *et al.*, 2020). Research has also shown that information literacy — the ability to navigate and find information online that is verified and reliable — can significantly increase the likelihood of identifying false news stories, while digital or media literacy alone do not (Jones-Jang *et al.*, 2021). In Canada, one of the educational initiatives that have been shown to be effective is CIVIX's CTRL-F: Find the Facts program. The program teaches youth how to evaluate online information with the same lateral reading techniques used by fact-checkers (CIVIX Canada, 2022). These techniques entail conducting simple web searches to locate key context about the sources and claims to be evaluated instead of focusing on analyzing the source of information itself. A study of over 2,000 students in grades 7–12, conducted by independent evaluators, found that students who took the program were more than three times more likely to read laterally than a control group (Pavlounis *et al.*, 2022). The ability of CTRL-F

students to accurately assess the reliability of sources and claims increased from 47% to 75% after completing the program (Pavlounis *et al.*, 2022).

Other initiatives are also aimed at youth. MediaSmarts (formerly the Media Awareness Network) is a Canadian organization that has focused on teaching media and digital literacy since 1996, both within Canada and globally (Titley *et al.*, 2014). Key to digital literacy is creating an awareness among young users that the internet has no gatekeepers and that, as a result, inaccurate information is as widely available as accurate information. Digital media literacy aims to teach skills that allow young people to distinguish the quality and verifiability of online material, to think critically about sources and messaging, and to recognize red flags associated with sources that try to manipulate or provide biased information. In addition, media literacy can be helpful in teaching effective methods for countering hate speech online without escalating it, as well as reporting harmful, abusive, or hateful content (MediaSmarts, n.d.).

In order to promote digital literacy, the Office of the Privacy Commissioner of Canada (OPC) has created educational resources for youth, including a graphic novel, with the objective of helping them reduce privacy risks (OPC, 2022). The OPC's approach is to empower youth with "the skills to critically evaluate situations on their own," rather than imposing rules or digital tools to block access to content (OPC, 2022).

4.5.2 Content Redirection and Blocking

Digital tools can be used to redirect people at risk of engaging in criminal activities

Digital tools that monitor searches have been used to attempt to stop users from accessing illegal or harmful material. For example, a pop-up warning message might appear when someone types identified CSAM keywords into their search engine (Edwards *et al.*, 2021). In clearly stated warnings, users are informed that viewing CSAM is illegal. As search terms increase in seriousness, so do the pop-up warnings. These messages are meant to destroy a user's sense of security and anonymity, and — especially among early offenders — deter and influence their behaviour (Edwards *et al.*, 2021). While these warnings are a cost-effective option, more research is needed to determine their impact on deterrence (Prichard *et al.*, 2022). The Canada Centre for Community Engagement and Prevention of Violence, which leads the federal government's anti-radicalization work (PS, 2019b), has also developed tools to redirect users based on their search histories (Box 4.7).

Box 4.7 Canada Redirect: Targeted Counter-Content Campaigns

Canada Redirect was launched by Moonshot (a tech start-up) in 2019, with funding from the Community Resilience Fund and in collaboration with the Canada Centre for Community Engagement and Prevention of Violence. Focusing on ISIS, Al-Qaeda, and far-right content that incites violence and promotes conspiracy theories, Canada Redirect targeted people prone to extremist messaging based on their Google searches, and "redirected thousands of them to videos that undermined relevant themes or content specific to each search." The videos offered "contextual, credible and safe content that challenged extremist beliefs." For example, videos attempted to elicit viewers' emotions and empathy, emphasized the toxic culture within extremist groups, and highlighted the importance of dialogue and diversity in Canada.

The project implemented localized campaigns, allowing Moonshot to collect neighbourhood-level data on extremist search activity, pilot-test messaging, and explore the feasibility of providing at-risk users with healthy content and access to community services. Between February 2019 and March 2020, 171,382 keyword searches related to extremist content were captured by Moonshot in Canada, in English, French, and Arabic. There were 2,583 clicks on the tailored content alternative, and 3,960 video views. Users seeking information on violent right-wing extremist content were more likely to engage with Moonshot's alternative content.

(Moonshot CVE, 2021)

As noted in Section 4.4, social media platforms have also begun introducing warnings to users, with the goal of limiting the spread of misinformation. For example, when Twitter users attempt to share an article they have not read, a warning encourages them to read the article before sharing (Vincent, 2020; Ghaffary, 2021). The goal of these nudges is to prompt users to consider what they share (Vincent, 2020; Ghaffary, 2021).

Content blocking and quarantine can stop users from accessing illegal or harmful content

Cleanfeed technology refers to various ISP-level content-filtering systems. It was developed in the United Kingdom in 2003, implemented in 2004, and adopted in Canada in 2006 (Brighton, 2004; Cybertip.ca, 2022a). At launch, the goal of Cleanfeed Canada was to block access to foreign websites hosting CSAM. An initial list of blocked websites was provided by Cybertip.ca (Canada's designated

regulator administered by C3P — the Canadian Centre for Child Protection) which is then forwarded to participating ISPs (Cybertip.ca, 2022a). The participation of ISPs is voluntary and it is worth noting they have no input into or knowledge about which websites are on the list (Cybertip.ca, 2022a). The list is maintained by Project Arachnid via its Shield API tool (Project Arachnid, 2022). The adoption of Cleanfeed was proposed in Australia in 2008, but loud opposition on the grounds of censorship and freedom of speech resulted in the initiative being cancelled quietly by 2010 (Liebhardt, 2008). Although Cleanfeed Canada may be considered a form of censorship by some, accessing CSAM is illegal, which Geist (2021a) argues distinguishes this initiative from the censoring of materials considered to be free speech.

Quarantines have been proposed as a simple mechanism to protect users from being exposed to online hate. This alternative approach to human content moderation would rely on automated detection systems similar to those already used to prevent malicious software or emails. A quarantine process for online hate would hold questionable messages in limbo, marked as neither permitted nor prohibited (Ullmann & Tomalin, 2020). Recipients or moderators of the messages would be alerted to the presence of quarantine items and have the opportunity to view the message or immediately delete it — giving recipients a choice in their own level of protection. In this scenario, senders write what they wish, but recipients decide what to view. According to Ullmann and Tomalin (2020), quarantines may act as an appropriate middle ground between combatting online hate and protecting the right to free speech.

4.6 Summary

To answer the Sponsor's question about the challenges created by ICT advances when it comes to preventing, investigating, and prosecuting online harms, the Panel focused this chapter on emerging online platforms, such as crowdfunding sites, cryptocurrency exchanges, the Dark Web, VPNs, and social media, which can all be exploited to amplify harms, including serious crimes. These enabling tools are not illegal; however, they can facilitate the financing, concealment, and spread of harmful content. Cryptocurrencies, for instance, are largely decentralized and can be used to anonymously pay for illegal transactions across jurisdictions and launder money.

The Panel found that law enforcement agencies face significant challenges in trying to trace some cryptocurrency exchanges, hampering criminal investigations. Similarly, the anonymity provided by the Dark Web and data-obscuring technologies such as VPNs can protect people engaged in positive online activity (e.g., journalists) as well as those who mean harm (e.g., people

dealing in illicit sales or sharing CSAM). The Panel found that these tools can impede the detection and investigation of criminal activity and put well-intentioned users at risk when used improperly.

While some practices have been implemented with the goal of enhancing the overall health of the online ecosystem, the Panel found their impact remains limited, since harmful content continues to proliferate and online tools continue to be used to facilitate illegal activities. Misinformation can spread online more rapidly than ever before; while not criminal, it has been shown to motivate offline crimes and is increasingly linked to extremism and hate. Social media companies have taken some self-regulated actions to moderate harmful content on their platforms, including the removal of misinformation, but issues of transparency, accountability, and consistency persist. The Panel also found that some moderation tactics have unintended effects, such as the over-removal of benign content.

Moving beyond the challenges of self-regulation explored in this chapter, Chapter 5 will focus on a range of regulatory tools that different orders of government in Canada and abroad are using, or considering, to govern digital spaces and counter online harms in light of ever-evolving ICTs.

5

Regulatory Context and Tools

Chapter Findings

- The speed of technological change creates challenges for the interpretation and enforcement of law, and most of the laws in Canada that currently apply to cyber-enabled crime were originally developed for offline offences.
- State governance of digital spaces tries to accommodate the protection of users from cyber-enabled crimes and constitutional rights and freedoms, such as freedoms of expression and privacy.
- State governance of digital spaces tries to deter individuals from engaging in criminal activities and, when someone is harmed by a cyber-enabled crime, seeks to facilitate investigations and prosecution without unduly infringing upon Charter rights.
- Governments in Canada and other countries are exploring and applying a range of regulatory approaches to address cyber-enabled crime and cyber-harm. Differences in legal systems and legal cultures need to be considered when assessing the extent to which foreign approaches are appropriate for a Canadian context.
- Governance of digital spaces is not limited to state-sanctioned tools and rules. A variety of approaches and instruments (e.g., corporate self-governance policies, user codes of conduct) can be considered in the creation of a responsive governance system.

Information and communication technologies (ICTs) are regularly used to facilitate criminal or harmful behaviours. In response, the Canadian government, like foreign governments, has intensified efforts to enhance the safety of the online ecosystem. Cyber-enabled harms may, at least partially, be mitigated or prevented by adopting a range of legal instruments, such as laws, regulations, and policies. However, important questions remain about the effectiveness of state-sanctioned legal responses and their ability to accommodate both the protection of users from cyber-enabled harms and their constitutional rights and freedoms, such as freedom of expression or privacy. In this chapter, the Panel assesses a number of domestic, foreign, and international instruments, with the aim of outlining different approaches to addressing cyber-enabled harms while simultaneously flagging limitations associated with some approaches.

This chapter begins by turning to Canada's existing laws and policies, in order to summarize what instruments currently exist to address or prevent cyber-enabled

harms, including criminal offences. It then examines policies and laws that other jurisdictions have proposed or adopted, some of which might address gaps in Canada's regulatory regimes or present options for strengthening existing policies. In particular, the Panel considers select enacted or proposed legislation in Australia, Germany, New Zealand, the United Kingdom, and the United States, as well as the European Union. These jurisdictions are chosen based on their link to Canada via close international cooperation (e.g., G7, Five Eyes), shared sociopolitical similarities, and/or because they have introduced or enacted policies and legislation that appear to influence the domestic regulatory landscape.

After examining different foreign responses to cyber-enabled harmful activities, the Panel unpacks the efficacy of international collaboration among Canada's allies. In doing so, it finds that reliance on the private sector is an important element of international governance, and that international proposals may have a chilling effect on the right to freedom of expression or undermine the right to privacy.

The chapter concludes by discussing the range of proposed policies and legislative reforms brought forward by the Government of Canada, in order to highlight its overly broad reach and potential interference with constitutional rights. As an outcome, the Panel finds that one of the main challenges of state governance of digital spaces is enhancing the health of the online ecosystem while simultaneously respecting constitutional rights and freedoms.

5.1 Select Laws and Policies in Canada

The ability of public safety organizations to protect people from cyber-enabled harms is, in part, predicated on the laws and policies these organizations are responsible for administering. When law reform regularly trails technological development, public safety bodies, such as law enforcement or regulatory agencies, may be stymied in their abilities to mitigate certain kinds of criminal or harmful behaviours.

In this section, the Panel discusses the regulatory regime for digital public safety through the lens of Canadian law and policies, in order to make clear that several common types of legal challenges arise from technological change, such as: (i) the need for laws to constrain or boost the development of technology; (ii) ambiguity in the application of legal rules; (iii) the scope of existing legal rules; and (iv) the "obsolescence of existing legal rules" (Bennett Moses, 2007). Specifically, the Panel looks at elements of Canada's *Criminal Code*, the civil law of Quebec, the common law and statutory torts, privacy legislation, defamation law, money-laundering laws, and anti-spam legislation, with the effect of identifying legal gaps and challenges.

5.1.1 The Distribution of Legislative Powers in Canada's Federal System of Government

The distribution of legislative powers among different orders of government — from federal to municipal — is central to any federal system, including Canada (Brideau & Brosseau, 2019). Thus, some issues examined in this report fall under federal jurisdiction, while others are regulated by provinces or territories, or by a combination of laws and regulations among different orders of government.

Section 91 of the *Constitution Act*, *1867* establishes exclusive jurisdiction of the Parliament of Canada over criminal law (Brideau & Brosseau, 2019). As such, criminal offences are established at the federal level and are consistent across the country. Section 92(14) of the *Constitution Act*, *1867*, however, gives provinces jurisdiction over the administration of justice; this means that the enforcement of the *Criminal Code* — for example, "conducting investigations, laying charges, and undertaking prosecutions" — generally falls under provincial jurisdiction (Brideau & Brosseau, 2019). As a result, the enforcement of offences is inconsistent across the country and reflects regional trends and challenges. For example, the procedure for laying charges and the median length of cases (calculated from the date of the first court appearance until the date of the final decision) vary across Canada (JUS, 2012; LCJC, 2017).

The Parliament of Canada has a constitutional mandate to legislate trade and commerce under Section 91(2) of the *Constitution Act*, *1867*, while provincial governments have jurisdiction over property and civil rights under Section 92(13) (Nisker, 2006). Despite different constitutional mandates, federal and provincial legislators often adopt legislation on similar issues (Section 5.1.4). Finally, tort law and civil law contain important privacy protections and liability frameworks. However, because these areas of law fall under provincial jurisdiction, there are discrepancies in remedies available to victims and survivors of cyber-enabled harms across the country (Section 5.1.3).

5.1.2 The Criminal Code

Looking at Canada's *Criminal Code*, it is apparent that most activities discussed in Chapter 3 constitute potential criminal offences. For example, in the category of exploitation, harassment, and abuse, the non-consensual distribution of intimate images is an offence under Section 162.1 (1) of the *Criminal Code* (Box 5.1), while cyber-harassment and cyber-stalking are offences under Section 264.

Similarly, some forms of abusive content are addressed under Sections 318 and 319 of the *Criminal Code*, making it an offence to advocate genocide, incite hatred against an "identifiable group" that is "likely to lead to a breach of the peace," and communicate statements that "willfully promote hatred against an identifiable group" in a public place (GC, 1985).

Box 5.1 The Non-Consensual Distribution of Intimate Content

From November 2009 to February 2012, Aydin Coban, a 35-year-old internet sextortionist residing in the Netherlands, "cruelly and relentlessly victimized" a Canadian teenager, Amanda Todd, who was 12 years old when the abuse began (BCSC, 2022). Over the course of more than two years, he used 22 aliases on different social media platforms to lure Ms. Todd or extort her into performing explicit live-cam shows by threatening to distribute intimate content already in his possession. Eventually, when Ms. Todd refused to comply with his demands, Mr. Coban kept his promise and distributed the illicit materials (BCSC, 2022). Although the harassment was reported to the RCMP, law enforcement at the time was unable to track down the sextortionist (Little, 2022). In 2012, Ms. Todd died by suicide.

An extensive investigation was launched only after her death, and it took several years to bring the perpetrator to justice (CIGI, 2021). In 2022, the Supreme Court of British Columbia found Aydin Coban guilty on multiple charges, including possession of child pornography, extortion, criminal harassment, and luring a child. He was sentenced to 13 years in prison. According to the court, his criminal acts caused "profound emotional and psychological harm" to Amanda Todd and "unquestionably contributed to her eventual death by suicide" (BCSC, 2022).

In 2015, partly in response to the public outcry over this case, the federal government amended the *Criminal Code* by criminalizing the non-consensual distribution of intimate images and providing several legal avenues to protect victims and survivors (GC, 1985; Macaulay, 2021). Among other things, a convicted offender may be prohibited from "using the Internet or other digital network, unless [they do] so in accordance with conditions set by the court" (GC, 1985).

Criminal law does not always fully engage with experiences of women and girls who are victims and survivors of technology-facilitated violence

Research conducted by Bailey and Mathen (2019) identified 410 reported criminal cases in Canada involving technology-facilitated violence (e.g., voyeurism, extortion) against women and girls as of January 2019. The vast majority (91%) of accused persons in these cases were male. Analysis of these cases found that judicial responses did not always fully engage with the experiences of victims and survivors due to two constraints (Bailey & Mathen, 2019). The first is its tendency to put the responsibility on women to avoid both sexual and physical violence (also known as the *responsibilization* of women for their attacks) (Grant, 2015). Criminal law's ability to recognize survivors' and victims' experiences can depend on whether the courts consider a victim or survivor "worthy" of protection (Bailey & Mathen, 2019). In some cases, courts were more likely to characterize sexual violence against girls as a public harm than violence against women. Further, some judicial analysis focused on victims or survivors who were seen as "innocent" or "good." This means that, for some women, the inability to be perceived as a "good victim" can lead to transferring responsibility for violence onto victims and survivors themselves (Bailey & Mathen, 2019).

The second constraint on criminal law's ability to fully engage with the experiences of victims and survivors is linked to narrow interpretations of *harm* and *violence* by courts (Narrative 3). Criminal law does not always recognize that online and offline worlds form a continuum, where fragmented and seemingly innocuous online comments and posts can be perceived as threatening by victims (Bailey & Mathen, 2019). When the criminal justice system does not fully see the connection between online speech and its offline effects, victims and survivors of crimes may be unable to achieve justice.

Narrative 3 *R. v. Corby*

In 2012, the Provincial Court of British Columbia rendered a decision in *R. v. Corby* (BCPC, 2012). In this case, the accused, Wayne Corby, was charged with the criminal harassment of Mihaela Michelle Bogdan under Section 264(1) of the *Criminal Code*. According to the prosecution, Mr. Corby engaged in conduct that caused Ms. Bogdan to reasonably fear for her safety after the couple's separation. After following Ms. Bogdan across the country, Mr. Corby wanted her to know he was nearby and made several posts on his Facebook page that included photos of places she regularly visited (e.g., place of work, gym, coffee shop), along with comments expressing longing for her ("I miss you, Michelle, very much"), and a link to The Police song "Every Breath You Take," which describes constant surveillance (BCPC, 2012).

Although Mr. Corby was eventually convicted of uttering a threat, some critics have argued that the court's analysis underestimated the integration of online and offline worlds by treating a host of Mr. Corby's behaviours and related events as isolated occurrences (Bailey & Mathen, 2019). According to the court, the posts were benign. While "some of the images had a special meaning or significance to [the complainant]," they were not aimed at her and were posted "for any Facebook user to view" (BCPC, 2012).

According to Bailey and Mathen (2019), criminal law should not be the exclusive, or even the primary, response to technology-facilitated violence against women and girls. In many cases, victims and survivors have well-founded reasons to choose alternative options (Section 3.1.2). Eliminating technology-facilitated violence requires resources that exceed "the capacity of a reactive and punitive" criminal justice system (Bailey & Mathen, 2019).

5.1.3 Common Law and Statutory Torts

Tort law is an area of private law concerned with compensating those injured by the wrongdoings of others. Torts should not be confused with crimes, which are wrongs against the state or public order that are prosecuted and punishable by the state (Beswick, 2022). A tort can be defined as "an act or omission that gives rise to injury or harm to another and amounts to a civil wrong for which courts impose liability" (LII, n.d.). Actions under tort law are usually brought by private parties seeking redress.

While the purpose of criminal liability is to enforce public justice, tort law's main function is to compensate the victim. Thus, the primary remedy of tort law is the awarding of monetary damages to the plaintiff (LII, n.d.). In addition to compensating the victim, tort law can "mediate social behaviour and protect fundamental rights" (Laidlaw, 2021a). In the context of disruptive technology, tort law can acknowledge privacy risks and define reasonable behaviour (Laidlaw, 2021a). Although tort law is primarily established by judges, some is outlined in statutes (Laidlaw, 2021a; Beswick, 2022).

Some of the harmful activities reviewed in this report may be liable under criminal or tort law. For example, the non-consensual distribution of intimate images is a tort as well as a criminal offence. Moreover, some legal scholars suggest that "threatening to distribute a person's intimate image in order to compel them [to] do something constitutes the tort of intimidation" (Dunn & Petricone-Westwood, 2018). Although redress is established under both criminal and tort law, access to justice for victims and survivors of cyber-enabled crimes remains a problem. Canada's criminal justice system experiences serious backlogs and delays (LCJC, 2017). Similarly, litigating cases in civil courts is onerous and rarely delivers desired results for victims and survivors (Laidlaw, 2021a). In many cases, victims do not know the identity of abusers hiding behind anonymous user accounts. Sometimes, the anonymity of alleged abusers prevents plaintiffs from proceeding with tort claims (Balkin, 2009; Citron, 2009; Zimmer, 2022). As a result, although public and private remedies are both provided by law, their effectiveness is limited, at best.

Opportunities for protecting privacy through tort law vary across provinces

British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador have introduced statutory causes of action in tort for privacy invasions (Laidlaw, 2021a). Several provinces — Alberta, Saskatchewan, Manitoba, Nova Scotia, Newfoundland and Labrador, New Brunswick, and Prince Edward Island — have also passed specific legislation creating the tort of non-consensual disclosure of intimate images (Gov. of NS, 2022). Although non-consensual disclosure of intimate images is a criminal offence, tort law aims to provide a more effective mechanism for victims to ensure the removal of content from the internet or the de-indexing of search engine results (Zimmer, 2022).

In *Jones v. Tsige*, the Court of Appeal for Ontario recognized a common law tort of intrusion upon seclusion (ONCA, 2012).[8] In this case, Ms. Jones (the plaintiff) brought a tort action against Ms. Tsige (the defendant) when she found out Ms.

8 This tort includes "physical intrusions into private places as well as listening or looking, with or without mechanical aids, into the plaintiff's private affairs" (ONCA, 2012).

Tsige had accessed her personal bank account information 174 times over the course of four years. Although Ms. Tsige never used Ms. Jones's bank account information or disclosed it to third parties, the Court of Appeal for Ontario held that the defendant intentionally intruded upon the plaintiff's privacy and recognized a common law tort of intrusion upon seclusion (ONCA, 2012).

This tort has been recognized in Nova Scotia (Laidlaw, 2021a) and paved the way for the judicial recognition of another privacy tort called "the public disclosure of private facts" in Ontario and Alberta (Mizrahi, 2018; Thiessen *et al.*, 2021). This tort provides that "[one] who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public" (ONSC, 2016). As a remedy, the defendant may be ordered to make best efforts to return all images of the plaintiff, remove any images posted online, and pay general damages, punitive damages, and aggravated damages for breach of confidence and mental distress (ONSC, 2016).

In *Caplan v. Atas*, the Ontario Superior Court of Justice acknowledged that existing torts failed to properly address the distinctive and malicious intent of perpetrators of internet harassment, or to compensate victims and survivors; as a result, it recognized a tort of internet harassment (ONSC, 2021). In particular, the Court found that the perpetrator in this case went beyond causing reputational damage and instead aimed to inflict "fear, anxiety, and misery" through systematic and serial online publications of defamatory material (Koczerginski, 2021). The Court granted a permanent injunction against Ms. Atas, vested title to the defamatory posts in the plaintiffs, and indicated it would issue ancillary orders to enable the plaintiffs to take down the content (ONSC, 2021).

Moreover, in *Yenovkian v. Gulian*, the Ontario Superior Court of Justice recognized the tort of "publicity placing a person in a false light" (ONSC, 2019). Unlike existing defamation law, this privacy tort protects an individual's right to determine their public image. The tort is "established where a person is portrayed in a false light publicly, the false portrayal would be highly offensive to a reasonable person, and the wrongdoer knew the portrayal was false" (Cumbo-Steinmetz *et al.*, 2020). In this case, the defendant engaged in an abusive cyber-bullying campaign against the plaintiff and her family, disseminating online materials containing false information (ONSC, 2019). The Court found that the defendant portrayed the plaintiff in a false light and that his behaviour caused serious harm, including a "visible and provable illness" and concerns about how strangers might mistreat the plaintiff based on the information spread online (ONSC, 2019). The court ordered the defendant to pay $300,000 in damages.

Torts that exist in Canada are often based on an outdated notion of privacy

The aforementioned torts, however, are limited in scope (Mizrahi, 2018; Laidlaw, 2021a). For instance, these torts are based on an outdated notion that privacy is "what happens when we are secluded or alone, that privacy only protects deviant or intimate behaviour, and that context does not matter" (Laidlaw, 2021a). In a digital age, privacy interests are almost always in play because people must constantly participate in the data-driven economy. Yet, depending on the circumstance, some digital privacy invasions, such as deepfakes, as well as amplification through search engines, "would likely not be actionable as a privacy tort" (Laidlaw, 2021a). Tort law's outdated framings of privacy, thus, do not necessarily account for contemporary harms in the interconnected world.

Legal scholars and practitioners suggest that some additional torts may be applicable to cyber-enabled crimes and harms (Dunn & Petricone-Westwood, 2018). For example, the non-consensual distribution of intimate images may give rise to the torts of appropriation of personality, breach of confidence, breach of fiduciary duty, and others. However, the potential of torts suggested by scholars to protect privacy is still an emerging area of civil law, because most reported cases involving the non-consensual distribution of intimate images have been prosecuted under criminal law (Dunn & Petricone-Westwood, 2018). Further studies, along with assessments of trial cases, may be needed to substantiate the utility of applying these torts to cyber-enabled harms.

5.1.4 Relevant Privacy Legislation

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) requires private sector organizations to obtain consent before collecting, using, or disclosing personal information

When people in Canada experience a privacy-related harm, they may turn to federal law in the hopes of addressing the issue at hand. Canada's federal privacy legislation, PIPEDA, applies to private sector organizations that "collect, use, or disclose personal information in the course of a commercial activity" (OPC, 2019c; Schwartz *et al.*, 2021). Under PIPEDA, personal information includes any factual or subjective information about an identifiable individual, including their name, ethnic origin, age, ID numbers, income, opinions, evaluations, employee files, and financial and medical records (OPC, 2019c). PIPEDA prohibits organizations from collecting, disclosing, or using personal information without consent (except in certain circumstances) and establishes a reporting-based regime for privacy breaches (The eQuality Project, n.d.) (Box 5.2).

Box 5.2 Data Breaches and PIPEDA

One reason why individuals might turn to PIPEDA is to determine what recourse they may have in the case of a data breach. Any company falling under the scope of the statute must disclose privacy breaches to both the Office of the Privacy Commissioner of Canada (OPC) and the affected individual. Breaches must be reported when there is a "real risk of significant harm to an individual" (GC, 2000a). Section 10.1(7) of PIPEDA stipulates that "significant harm" includes, among other things, humiliation, damage to reputation or relationships, and identity theft. Under Section 10.1(4), the notification to the affected individual shall 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" (GC, 2000a).

Compliance with PIPEDA is overseen by the OPC, which may, on its own initiative, investigate complaints submitted by individuals regarding the information management practices of private companies in any province that has not adopted substantially similar privacy legislation (OPC, 2017a; Mizrahi, 2018). As of June 2022, British Columbia, Alberta, and Quebec have passed privacy statutes that are "substantially similar" to PIPEDA, which means their own provincial laws often apply instead of PIPEDA (OPC, 2016a; Schwartz *et al.*, 2021). The OPC frequently deals with complaints related to impersonation and non-consensual distribution of intimate images (OPC, 2016b). To date, it has investigated cases about the operation of online dating websites and services, websites that re-post court and tribunal decisions, and many so-called *revenge* and *shaming* websites, among others (OPC, 2016b).

PIPEDA is limited by enforcement challenges

As noted in Chapter 2, PIPEDA is meant to regulate the relationship between businesses and individuals rather than protect privacy as a human right.[9] Although it is focused on ensuring that identifiable individuals' personal information is adequately protected, the actual application of PIPEDA to some cyber-harms and cyber-enabled crimes can be unclear. For example, deepfake videos may not breach privacy legislation because they are not exposing victims' and survivors' real life (McMillan, 2018). Moreover, if an individual uses

9 The Privacy Commissioner of Canada, however, has argued that PIPEDA should approach privacy through a human rights lens (OPC, 2021b).

someone's personal videos to produce a deepfake video for non-commercial purposes, PIPEDA will not apply (OPC, 2017b). Nonetheless, when they create a false impression of someone's private life, deepfake videos can cause real harms, as when a real video of a similar activity is non-consensually disclosed (Chapter 3).

One of the biggest challenges the OPC faces when it comes to protecting online reputation is asserting jurisdiction over websites that are based outside Canada. In some cases, foreign-based websites may not be subject to PIPEDA due to its operator(s) not having any real and substantial connection to Canada (OPC, 2016b). Moreover, for PIPEDA to apply, a website needs to be engaged in commercial activity; in some cases, personal information is posted without consent on websites set up for personal use (OPC, 2016b). If the OPC has jurisdiction, it can request that an organization (e.g., social media platform) remove content (The eQuality Project, n.d.), but enforcing the request requires initiating a case in the Federal Court (OPC, 2016a).

While the OPC is mandated to investigate complaints, it is not empowered to award compensation. The statute provides people with the option to pursue the matter in the Federal Court, but "damage awards are extremely rare and are limited to the most egregious situations" (Mackey, 2012). Moreover, as with tort law, individuals have limited opportunities to invoke redress under the federal privacy regime due to the difficulty of bringing private actions against violators (Scassa, 2018).

A lack of common principles enshrined in public and private sector privacy laws undermines the effectiveness of PIPEDA

Public-private partnerships involving digital technologies are sources of privacy risks (Therrien, 2021b). This is particularly relevant in the age of COVID-19, as several government-led, pandemic-related initiatives involved partnerships with the private sector. Government institutions were not required to ensure that consent for these initiatives was meaningful, since legal authority was based on consent obtained by a private sector organization (Therrien, 2021b). As a result, there was a risk that the public sector could implement a technological solution (e.g., telemedicine or e-learning platforms) that allowed a private sector partner to use personal information, even if it was collected for non-public health-related purposes (OPC, 2020a). An OPC investigation into actions taken by Statistics Canada highlights similar concerns; the latter started collecting detailed credit information about people in Canada from private sector companies, and had plans to collect further financial transactions and account balance data. These initiatives were privacy-invasive, but, in part due to the inadequacy of federal laws, the OPC's investigation did not find legal violations (Therrien, 2021b).

5.1.5 Protection of Privacy in Quebec

While common law governs the relationships among people in every other province, the *Civil Code* applies in Quebec. This key difference has consequences for the legal regime surrounding contracts, torts, and property (Beaulac & Gaudreault-DesBiens, 2017), among other things. In addition, Section 5 of Quebec's *Charter of Human Rights and Freedoms* recognizes privacy as a human right and guarantees the right to privacy by providing a direct right of action to affected people (Gov. of QC, 1976; Stoddart, 2007). In 1982, Quebec adopted the first law on privacy in the public sector (Gov. of QC, 1982) and, in 1994, became the first province in Canada to adopt a privacy law for the private sector (Delwaide & Aylwin, 2005). All of these laws are accompanied by jurisprudence on privacy issues (Delwaide & Aylwin, 2005).

A chapter of Quebec's *Civil Code* is devoted to privacy (i.e., Articles 35 to 41). Article 35 of the *Civil Code* establishes every person's right to the respect of their reputation and privacy; Article 36 provides a non-exhaustive list of actions that may invade a person's privacy; and Article 37 requires that "every person who establishes a file on another person" must have a "serious and legitimate reason for doing so" (Gov. of QC, 1991). A breach of the right to privacy can result in compensation through monetary, non-monetary, or punitive damages (Norton Rose Fulbright, 2012).

These privacy provisions of the *Civil Code* apply to digital spaces (Schwartz *et al.*, 2021). For example, there have been several civil lawsuits brought before Quebec courts with circumstances similar to the non-consensual sharing of intimate images. The remedies granted in these cases were based, among other things, on the privacy provisions of the provincial Charter and the *Civil Code*. However, damages were difficult to establish, the sums awarded were very small, and the deterring effect was weak (Boutin-Clermont, 2014).

Some concepts contained in the *Civil Code* — such as respect of reputation and right of personality — are not used in the common law outside Quebec. Although statutory privacy torts enacted in British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador strive to enhance privacy protections, they appear to apply in limited circumstances; most provinces have not implemented the legislation or related privacy concepts that exist in Quebec civil law (Stoddart, 2004).

Quebec's private sector privacy law has broader scope and stricter enforcement measures than PIPEDA

Quebec has undertaken a comprehensive reform of its private sector privacy regime, with the goal of adapting it to present-day realities. In 2021, the National Assembly of Quebec passed Bill 64, *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information* (Act 25) (Gov. of QC, 2021). Many of the obligations contained in this act align with privacy provisions under PIPEDA or the OPC's recommendations. However, the act's privacy obligations contain stringent enforcement measures rather than strong recommendations, as is the case under PIPEDA (McMillan, 2021). It creates a private right of action for individuals for the unlawful infringement of their statutory rights and the aforementioned privacy provisions of the *Civil Code* (OPC, 2020b).

Under Act 25, enterprises[10] must report confidentiality incidents, make reasonable efforts to reduce risk of harm, and prevent future incidents (Gov. of QC, 2021). A *confidentiality incident* is defined as "access to, use, or communication of personal information not authorized by law, as well as the loss or any infringement of the protection of such information" (McMillan, 2021). This definition is different from other Canadian privacy laws in that it treats the unauthorized use of personal information as a confidentiality incident. Act 25, therefore, "exceeds the scope of other Canadian data breach notification requirements" (McMillan, 2021) and has the effect of potentially creating a bifurcated notification regime: one for residents of Quebec and another for residents of other parts of the country.

In cases where there is a risk of serious injury arising from a confidentiality incident, an organization must notify the *Commission d'accès à l'information du Québec* and anyone whose personal information is impacted by the incident (Gov. of QC, 2021). This notification threshold is similar to the reporting threshold of a "real risk of significant harm" under PIPEDA (McMillan, 2021). Act 25 does not provide definitions for, or examples of, *risk of serious injury*. However, it establishes several criteria that organizations must consider in determining the level of seriousness of such a risk: sensitivity of information, anticipated consequences of how information will be used, and likelihood of information being used for harmful purposes (BLG, 2021). Although the assessment criteria under Act 25 seem to be similar to PIPEDA, the Commission may interpret the notification requirements differently than the OPC (BLG, 2021). As a result, residents of Quebec may be subject to different notification standards depending on which law — PIPEDA, or the new act formed by Act 25 — governs the organization reporting the incident.

10 A broad range of activities fall under the definition of enterprise. However, when determining whether an organization is an enterprise, or whether a person is carrying on an enterprise, courts consider the main activity, rather than ancillary activities (Delwaide & Aylwin, 2005).

5.1.6 Defamation Law

Defamation law in Canada protects reputation from injury by placing limitations upon freedom of expression, in cases where false statements cause injury to reputation. In this way, it balances two Canadian values: the quasi-constitutional value of protection of reputation (SCC, 1995; LCO, 2020) and the constitutional protection of freedom of expression, recognized in the *Canadian Charter of Rights and Freedoms* (GC, 1982). The principles of defamation in Canada are primarily dictated by common law, supplemented with legislation (which leads to variations across the country) (LCO, 2020). In Quebec, defamation falls under the civil liability provisions of the *Civil Code* (SCC, 2011). As both the values of free speech and protection of reputation are informed by context and social norms, defamation law is sensitive to the society and culture in which it operates. For the most part, defamation law evolves on a case-by-case basis, in response to specific claims brought before the courts.

Defamation law has been slow to adapt to the proliferation of the internet

While defamation law is not specific to online activity, according to the Law Commission of Ontario (LCO) (2020), "the internet is now the arena in which much, if not most, defamation occurs," and some of the harmful activities discussed in Chapter 3 may involve defamation. For example, some deepfake videos may create false statements of fact about a person and lead to a loss of reputation (McMillan, 2018). Victims and survivors of defamation may be entitled to damages and injunctive relief to prevent the dissemination of defamatory material. However, when a video contains a disclaimer that it is fake, an action for defamation may fail. The global nature of online activities can also create challenges for defamation cases in Canada, because Canadian courts may lack jurisdiction if the publisher of the video is located abroad (McMillan, 2018). Thus, individuals targeted by these videos may, in practice, have limited legal recourse when a video is labelled "fake" or when publishers operate beyond a Canadian court's jurisdiction.

The proliferation of online content has led to substantial changes in the scope and spread of defamation. What was once a local issue is now increasingly transnational, as defamatory content may be publicized around the world (LCO, 2020). Traditionally, defamation defendants were publishers or media organizations that produced newspapers, books, or television and radio broadcasts. However, in the internet age, defendants are often individual publishers who post material online. LCO (2020) notes the law has "strained to adapt" to these new types of cases, since it has, "for the most part, [...] operated within the boundaries of [the] traditional paradigm."

In light of these challenges, there have been calls to update defamation law (Laidlaw & Young, 2017; LCO, 2020). On the subject of intermediary liability for defamatory content posted by third parties, Laidlaw and Young (2017) argue that the "law is complex and confusing," leading to a governance framework that is "ill-suited to dealing with the issue of internet intermediary liability in defamation." The doctrine sometimes leads to intermediaries being found to be publishers in cases where "many would not think their conduct sufficiently blameworthy to ground liability." In light of uncertainty and confusion, some legal scholars are of the opinion that intermediaries should not be liable for the unlawful acts of third parties and, instead, should have procedures for handling defamation complaints and removal of allegedly defamatory content in narrow circumstances. These proposals aim to strike a balance between free speech and protection of reputation (Laidlaw & Young, 2017).

5.1.7 Anti-Money-Laundering Laws and Regulations, and the Role of FINTRAC

Anti-money-laundering laws and regulations provide other legal avenues meant to ensure the safety and security of people in Canada (GC, 2021e). As noted in Section 4.1, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) was created in 2000 to ensure Canada's compliance with international anti-money-laundering standards (FINTRAC, 2021a). It operates under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations, enforces the provisions of the *Anti-Terrorism Act*, and serves "as a clearinghouse, receiving, analysing, and disclosing financial intelligence (FININT) on suspected money laundering, terrorist financing, and threats to the security of Canada" (Pyrik, 2021).

FINTRAC does not have investigative and law enforcement powers, and it is detached from law enforcement agencies

FINTRAC is under the authority of the Department of Finance. It is independent from Canada's law enforcement agencies and lacks independent investigative powers. Section 40(a) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* specifies that FINTRAC "acts at arm's length and is independent from law enforcement agencies and other entities" (GC, 2000b). It is, however, authorized to disclose designated information, though such information does not include "open source information [...], a theory of the crime, or the internal written justification for disclosure" (Pyrik, 2021). Therefore, the recipients must duplicate FINTRAC's actions or use a production order to access information.

FINTRAC has a more limited mandate and fewer opportunities for cooperation than similar agencies in other jurisdictions (FINA, 2018). For example, the

Financial Crimes Enforcement Network (FinCEN) in the United States is also under the authority of the agency responsible for federal finances (Department of the Treasury), but the *USA Patriot Act* authorizes it to engage in certain activities that FINTRAC cannot undertake (e.g., order financial institutions to provide information about people or entities suspected of criminal activity upon the request of domestic and select foreign law enforcement agencies) (FINA, 2018). Meanwhile, the U.K. Financial Intelligence Unit is under the authority of the Home Office, which is responsible for public safety and immigration, and not HM Treasury. There are both advantages and disadvantages to FINTRAC being overseen by the Department of Finance; this organizational structure strengthens connections between FINTRAC and Canadian financial institutions but hampers cooperation between FINTRAC and law enforcement agencies (FINA, 2018; Pyrik, 2021).

FINTRAC continues to face challenges related to overseeing transactions that take place on peer-to-peer decentralized exchanges

Digital currencies, such as Bitcoin or Ether, can facilitate pseudonymous or anonymous transactions without third-party oversight or intervention (Section 4.1.2); these properties have made cryptocurrencies of interest to some criminal actors, such as those operating ransomware campaigns. To address these challenges, the Government of Canada amended the legal regime for the prevention of money laundering and terrorist financing. First, in 2020, a government regulation defined *virtual currency* as:

> *(a) a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or*
>
> *(b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).*
>
> GC (2020b)

Second, the definition of *money service business* (MSB) was amended to include anyone "dealing in virtual currencies" (Pyrik, 2021). These persons must register as MSBs with FINTRAC and adhere to reporting, record-keeping, "know your client," and compliance requirements (Bennett Jones, 2021). Third, the obligations of other reporting entities (such as banks, credit unions, insurance companies, and casinos) extend to virtual currency transactions (Bennett Jones, 2021). Taken together, these amendments are expected to ensure that FINTRAC can monitor the movement and uses of digital currencies and, as such, strip away at least some of their pseudonymity or anonymity.

Moreover, at the end of 2020, FINTRAC published red-flag indicators for money laundering and terrorist financing that use virtual currency transactions. These indicators were developed based on an analysis of laundering and terrorist cases, suspicious transaction reports, feedback from reporting entities, and materials published by international law enforcement organizations (Badour *et al.*, 2020). In 2021, FINTRAC published an updated version of these indicators (FINTRAC, 2021c).

Despite efforts to amend applicable rules, FINTRAC continues to face challenges related to overseeing transactions that take place on peer-to-peer decentralized exchanges (DEXs) that do not require a third-party gatekeeper or funder (Keatinge *et al.*, 2018; Dolny, 2021). The sourcing of high-volume and frequent privacy-coin transfers among anonymous individuals is, currently, very challenging to review, and the aforementioned guidance does not solve this problem (Dolny, 2021). In April 2021, US$122 billion in transactions took place on these platforms, compared to US$1 billion one year earlier (Osipovich, 2021); the average valuation of Bitcoin, one of the dominant cryptocurrencies, rose by 300% between January and December 2020 (DeMatteo, 2022). However, in the first half of 2022, the value of Bitcoin decreased by more than 50% from its all-time high, to a value less than in December 2020 (Gailey & Haar, 2022).

5.1.8 Canada's Anti-Spam Law

Fraud, cyber-bullying, and cyber-harassment may take place on e-commerce websites, or through the use of deceptive marketing, promotional emails, text messaging, or instant messaging. Canada's anti-spam law (CASL) plays an important role in preventing cyber-enabled crimes and harms by regulating the everyday activities of companies, such as sending emails to customers, operating a company website, and making mobile applications available for download (Olser, n.d.). According to GC (2021f), in the context of commercial activity, CASL prohibits, among others, the following: spamming, deceptive marketing, installing malware and spyware, hacking, and address harvesting. Penalties for some CASL violations can reach $1 million for individuals and $10 million for companies (GC, 2019c). While CASL creates a comprehensive governance regime to address a range of harmful activities, its successful implementation requires significant resources, public awareness and engagement, coordination with law enforcement agencies, and the clarification of some legal ambiguities.

CASL's provisions on intermediary liability are ambiguous

CASL "has created a strict liability offence for intermediaries that enable or benefit financially from the sending of unsolicited electronic messages or similar, including advertising brokers, electronic marketers, developers, and payment providers" (Laidlaw, 2019). For example, intermediaries could be liable for CASL violations by third parties. Concerns have been raised about these liability provisions, which could apply "even if the intermediary did not intend to assist in a contravention of CASL or was unaware that its activities enabled or facilitated contraventions" (Kratz, 2019). This regulatory framework has been described as "complex, onerous and ambiguous" (Kratz, 2018).

CASL's anti-malware requirements received widespread support

Unlike the provisions for the liability of intermediaries, CASL's anti-malware requirements received widespread support (Kratz, 2020). Section 8(1) of CASL provides that "a person must not, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system [...], unless the person has obtained the express consent of the owner or an authorized user of the computer system" (GC, 2010). In the Panel's view, this means CASL provides an avenue to take action against companies providing spyware or malware for the tracking and surveillance of intimate partners' personal devices. The actual efficacy of using CASL in these situations, however, remains to be seen until cases are investigated and action taken in some numbers.

Further, the Canadian Radio-television and Telecommunications Commission (CRTC) is planning to require that internet service providers block malware-carrying botnets (CRTC, 2022; Solomon, 2022). A botnet "is a network of malware-infected devices controlled as a group without the knowledge and consent of the device owners, and toward some malicious end" (CRTC, 2022). Botnets are used to facilitate malware and spam, distributed denial-of-service attacks, data breaches, and to give malicious actors unlimited access to networks. When the CRTC requirements come into force, internet providers will have to block botnets at the network level (CRTC, 2022; Solomon, 2022).

CASL vests law enforcement powers in the CRTC

Under CASL, the CRTC may issue penalties and take-down warrants to people and companies involved in disruptive marketplaces (Box 5.3). The CRTC's Chief Compliance and Enforcement Officer issues violation notices accompanied by penalties where there are "reasonable grounds to believe that a violation has

taken place" at which point alleged violators are given 30 days to pay or challenge the notices and penalties. Since its inception, the CRTC has issued penalties exceeding $1.4 million (GC, 2022c).

Box 5.3 CRTC Take-Down of Canadian HeadQuarters

In January 2022, the CRTC's Chief Compliance and Enforcement Officer issued penalties in the amount of $300,000 against several people in Canada for their participation in the Dark Web marketplace called Canadian HeadQuarters (also known as Canada HQ or Canadian HQ), which was eventually taken offline. Canadian HeadQuarters was one of the largest Dark Web marketplaces in the world. It specialized in "the sale of goods and services, including spamming services, phishing kits, stolen credentials, and access to compromised computers," which were used to facilitate malicious activities. The CRTC's investigation focused on several people who sent emails mimicking famous brands to access information about bank accounts and credit card numbers.

(GC, 2022c)

5.2 Select Foreign Regulatory Approaches

Canada is not alone in trying to grapple with the range of online criminal and harmful activities enabled, or made more prevalent, by ICTs. Many of Canada's allied nations have enacted legislation to address these ills or are working collectively to overcome cyber-enabled harms. In this section, the Panel examines select enacted laws and proposed regulatory approaches regarding cyber-enabled harms. Its focus is primarily on jurisdictions that have sociopolitical structures similar to Canada's, are connected to Canada through close diplomatic relationships (e.g., Five Eyes), and/or influence Canada's domestic law reform. The Panel also highlights some of the potential, or actual, limitations of these laws and regulations, including how they might sacrifice freedom of expression in exchange for more regulation.

State governance of online spaces may have a chilling effect on the exercising of people's rights

The so-called *chilling effect* describes any potential impact that state governance of the online environment — in particular, regulations intended to control online abuse, hate speech, or other online harms — may have on the rights of

individuals. In this context, it refers to "the idea that certain regulatory actions may 'chill' or deter people from exercising their rights online and in other digital contexts" (Penney, 2020). There are different philosophies about such regulations internationally. European-based models tend to focus on preventing online harassment and prioritize protecting personal dignity and reputation (Penney, 2019a). In contrast, the U.S. model favours free speech, or a broad immunity that seeks to avoid any legislative chilling effect on free speech. This fits neatly within the American legal tradition, which defines privacy as freedom from state interference (Penney, 2019a).

There is limited evidence on whether legislation has significant impact on chilling a user's online speech (Kendrick, 2012; Penney, 2017). This may be due, in part, to the fact that it is a difficult subject to study or quantify (Penney, 2020). The limited and emerging evidence that does exist relates largely to the application of the U.S. *Digital Millennium Copyright Act* (DMCA). Under DMCA, automated systems operated by private entities send take-down notices to online service providers, which then remove the content violating copyright laws and notify the user (Penney, 2019b). Tens of millions of these notices are sent daily, leading critics to suggest that the law is having a chilling effect online. A survey of 500 Google Blogger and 500 Twitter accounts provided early evidence linking the practice of automated take-down orders to the chilling effect (Penney, 2019b). For example, 75% of the survey's respondents indicated they would be "much less likely" or "somewhat less likely" "to speak or write about certain topics online" following the receipt of a personal DMCA notice. The same scenario would prompt 81% of respondents to be more careful about what they discuss online (Penney, 2019b). In addition, the survey found a link between DMCA and privacy concerns. For example, 81% of respondents indicated they would be more concerned about privacy, and would take additional steps to protect it, if they received a take-down order. Overall, Penney (2019b) found that privacy concerns proved to be the greatest predictor of the chilling effect.

However, those who oppose legislative or regulatory frameworks due to their potential to limit free speech often ignore the chilling effect that online harassment has on victims and the constitutional rights of those victims (Penney, 2020). Penney (2020) invokes the case of *Crouch v. Snell*, wherein the Supreme Court of Nova Scotia struck down the province's *Cyber-Safety Act* because it encroached on freedom of expression as guaranteed by the *Charter of Rights and Freedoms* (NSSC, 2015). While the Court acknowledged that cyber-bullying victims and survivors should have access to justice, Penney (2020) notes it failed to address the impact of online abuse on the victims' freedom of speech.

As outlined in Section 3.1, a growing body of evidence shows that online harassment has a significant chilling effect on targets by forcing them out of

online forums and online engagement (Franks, 2018; Penney, 2020). Franks (2018) states that "ample evidence exists for how harassment chills freedom of expression, mobility and association," adding that these impacts have a stronger chilling effect, especially on women and minorities, than any government action might. Some scholars argue that laws and regulations may even empower speech among women (Citron & Penney, 2019). For example, in a study of 1,200 online users in the United States, female participants indicated they would be more likely to contribute self-generated content or engage with social networking sites if laws protected them against online harms (Citron & Penney, 2019).

Research demonstrates that chilling effects do not necessarily involve self-censorship. Rather, they shape social behaviour by encouraging people to speak or act in a way that conforms to, or is in compliance with, perceived social norms. Penney (2022) argues that legal scholars have largely neglected this dimension of chilling effects, focusing instead on the relationship between chilling effects and freedom of speech and expression.

Finally, some commentators suggest that framing debates on regulating the online environment in terms of "free speech versus censorship" impairs meaningful discussions about addressing the very real and ubiquitous cyber-enabled harms examined in this report, and about how speech-inhibiting environments affect racialized and minoritized groups (Haggart & Tusikov, 2021). Digital public safety requires that policy-makers depart from this simplified view of the effects of regulation on speech (Haggart & Tusikov, 2021). A more responsive approach to ensuring public safety in the digital age consists of a combination of policies, including incentives for better corporate self-regulation and enhanced protections of data and privacy (including laws regulating accountable and transparent artificial intelligence) (Cusumano *et al.*, 2021) (Section 5.2.5).

5.2.1 Australia

The *Enhancing Online Safety Act 2015* treats certain digital communications as criminal offences

The Government of Australia brought in the *Enhancing Online Safety Act 2015* to respond to complaints about online harms, such as cyber-bullying of children and sharing "abhorrent violent material" (eSafety Commissioner, n.d.-a). The act created that country's eSafety Commissioner (Gov. of Australia, 2015), whose role originally covered the protection of children but, as discussed below, was later expanded to include everyone in Australia (Gov. of Australia, 2017). The eSafety Commissioner is an independent office supported by the national media regulator, the Australian Communications and Media Authority (Gov. of Australia, 2015;

eSafety Commissioner, n.d.-a). An amendment — the *Enhancing Online Safety (Non-Consensual Sharing of Intimate Images) Act 2018* — makes it an offence to share intimate images without consent (Gov. of Australia, 2018). It also prohibits people from sharing, without consent, images where a victim is not wearing the clothing they consistently wear in public for cultural or religious reasons (e.g., a Sikh man without his turban) (Gov. of Australia, 2018).

Depending on the situation, the eSafety Commissioner has the investigative powers and ability to seek civil or criminal penalties in conjunction with law enforcement agencies and the courts (eSafety Commissioner, n.d.-a). In short, the commissioner provides a new mechanism to address certain cyber-enabled crimes outside traditional law enforcement. Yar and Drew (2019) note that "the approach taken in Australia to [internet-based abuse], whilst still potentially suffering the same frustrations as other kinds of cybercrime regarding perpetrators, has focused on the actions that are within an achievable remit of preventing further [internet-based abuse] and disrupting the crime." For example, the commissioner also provides support to victims of image-based abuse by aiding in the removal of intimate images or videos (eSafety Commissioner, n.d.-a),[11] which Yar and Drew (2019) argue "is likely to be the most important outcome for victims." The Canadian government has cited Australia's eSafety Commissioner in its own policy and legislative proposals, describing it as a potential source of inspiration for domestic reforms (Meyer, 2021).

The *Sharing of Abhorrent Violent Material Act* created law enforcement reporting obligations for content, internet, and hosting providers

Another piece of Australian legislation is the *Sharing of Abhorrent Violent Material Act*, an amendment to the *Criminal Code Act 1995* that passed into law following the 2019 terror attack in Christchurch, New Zealand (Gov. of Australia, 2019). The amendment requires that content, internet, and hosting providers report "abhorrent violent conduct" occurring in Australia and hosted on its servers to the Australian Federal Police "within a reasonable time." It also makes it an offence for content and hosting service providers to "fail to remove access to abhorrent violent material expeditiously" (Gov. of Australia, 2019).

11 The eSafety Commissioner can provide support if the person pictured in the photograph or video, or the person who posted it, resides in Australia, or if the image is housed in Australia (eSafety Commissioner, n.d.-b).

The expansion of internet policing under the *Online Safety Act* raises human rights concerns

Australia's *Online Safety Act* that came into force in January 2022 expands the power of the eSafety Commissioner by:

- bringing the full range of online services into the cyber-bullying scheme (e.g., including online gaming and content-sharing platforms in addition to social media);
- enabling the eSafety Commissioner to require the removal of adult cyber-abuse material that targets an Australian;
- reducing the time a service provider has to comply with a take-down notice from 48 hours to 24 hours; and
- giving the eSafety Commissioner greater information-gathering powers to obtain identity information, including basic subscriber information for anonymous accounts.

eSafetyCommissioner (2021a)

While there was broad support for the bill in the Australian Parliament, the Australian Greens party opposed the measures, stating the eSafety Commissioner's expanded powers were excessive. The Greens noted that "this Bill would make the eSafety Commissioner the sole arbiter of internet content in Australia" (Mckim, 2021), adding this could result in the complaints process being abused by "people opposed to sex work, pornography and sexual health for LGBTIQ+ people" such that they "seek to have lawful online adult content removed" (Mckim, 2021).

A similar proposal in Canada also raised these concerns (Geist, 2021b). Human rights groups have pointed to the potential of legislation to encourage the automated and proactive monitoring of content by social media platforms, which can have unintended and harmful consequences to communities online (DRW, 2021). This could have considerable implications relating to censorship and freedom of expression, with evidence demonstrating that automation leads to the removal of significant amounts of legal content (Windwehr & York, 2020). Proactive monitoring may disproportionately harm marginalized groups, as automated processes disproportionately remove the content of some groups over others, namely Black, Indigenous, and LGBTIQ+ people (Digital Rights Watch, 2021; Geist, 2021c). Racial bias in artificial intelligence (AI) models is well documented, with multiple studies demonstrating that Black Americans are substantially more likely to have their content flagged compared to white Americans (Davidson *et al.*, 2019; Sap *et al.*, 2019).

There are important differences between the Australian and Canadian legal contexts

While Australia's legal system shares some similarities with Canada's, its approaches may not be appropriate for the Canadian context. One important distinction between the two countries' legal systems is that Australia does not have an enshrined bill of rights.[12] Laws in Canada must not violate the provisions of the *Charter of Rights and Freedoms*, which is part of the *Constitution of Canada* (GC, 2020a). The absence of a bill of rights has substantial practical implications. For example, in 2019, the High Court of Australia upheld the right of the Government of Australia to terminate the employment of a public servant because of negative tweets related to government policy (HCA, 2019; Triggs, 2019). In its decision, the High Court noted that, had the case occurred in Canada, the *Charter of Rights and Freedoms* may have provided some protections to the public servant (HCA, 2019; Triggs, 2019).[13]

5.2.2 New Zealand

The *Harmful Digital Communications Act* treats certain digital communications as criminal offences

In New Zealand, the *Harmful Digital Communications Act* (HDC Act), passed in 2015, addresses serious online harms that occur through digital communications (Gov. of NZ, 2015). According to Section 22(1) of the act, a communication is considered a criminal offence when (i) it is deemed to have the intention to cause harm; (ii) "posting the communication would cause harm to an ordinary reasonable person in the position of the victim;" and (iii) it did cause harm (Gov. of NZ, 2015). Harmful communications that do not meet this threshold can be addressed through civil action (Hunt, 2020). Under the HDC Act, people can report instances of online harm that breach the statutory principles of communications to Netsafe, an independent, not-for-profit agency that provides advice and works to resolve complaints (Netsafe, 2021). As of 2020, 556 people have faced criminal charges under the HDC Act, with an increasing number of charges in more recent years (e.g., 127 charges in 2020 versus 80 in 2016) (Harris, 2021). Amendments to the HDC Act addressed the sharing of non-consensual intimate images by removing the need for victims or survivors to demonstrate harm (as defined in the HDC Act). Sharing such images without consent constitutes a crime without victims or survivors having to satisfy the courts that they sustained "serious emotional distress" (Gov. of NZ, 2015, 2022).

12 Australians have five individual rights enshrined in their constitution: right to vote; protection against acquisition of property on unjust terms; right to a trial by a jury; freedom of religion; and prohibition of discrimination on the basis of state of residency (Gov. of Australia, 2010; AHRC, n.d.).

13 It is unknown whether the outcome of the case would have been the same or different in Canada.

Amendments to the *Films, Videos, and Publications Classification Act 1993* prevent and mitigate harms caused by the livestreaming of objectionable content

Amendments to the *Films, Videos, and Publications Classification Act 1993* are intended to provide for the prevention and mitigation of harms caused by the dissemination of "objectionable" material, such as content depicting horror, crime, cruelty, or violence (Gov. of NZ, 1993, 2021). The amended act provides that the livestreaming of objectionable content is a criminal offence that applies to the individual or group streaming the content, but not to the online content hosts, such as platforms. The act also gives the Inspectors of Publications and the Chief Censor new powers aimed at limiting the publication and dissemination of objectionable content (Gov. of NZ, 2021).

5.2.3 The United Kingdom

The draft *Online Safety Bill* introduces new duties for online service providers

In 2019, the Government of the United Kingdom published the *Online Harms White Paper* (Gov. of UK, 2019). Although, in drafting this paper, the U.K. government closely examined legal developments in Australia, Germany, and the European Union, the U.K. approach differs from the other jurisdictions in that it proposes a comprehensive regulatory framework to cover a wide variety of cyber-enabled crimes and harms in a single document (Gov. of UK, 2019).

To address the cyber-enabled crimes and harms mentioned in the White Paper, the U.K. Secretary of State for Digital, Culture, Media and Sport proposed a new regulatory framework in the *Online Safety Bill* (U.K. Parliament, 2022a). The bill establishes the obligations of online service providers that "facilitate user-to-user sharing of content, and/or have a search engine, or publish certain pornographic content" (Judson, 2022). Although services would have different duties depending on their size and functionalities, all services would be required to address priority offences, including child sexual exploitation and abuse, terrorism, threats, stalking, the publication of private sexual images, and the sale of drugs and weapons. Services would also be required to stop users from finding priority illegal content, reduce the length of time this content remains online, introduce risk mitigation and management measures, and specify in terms of service "how users would be protected from illegal content" (Judson, 2022). Furthermore, services likely to be accessed by children would be subject to additional duties, including mitigating the risk of harm to children, preventing them from finding harmful content, and specifying in terms of services "how children will be protected from harmful content" (Judson, 2022).

Under this bill, companies providing online services to users in the United Kingdom would be required to undertake certain duties of care, such as conducting risk assessments related to illegal content; ensuring freedom of expression, privacy, and protections for journalistic content; and developing complaint-reporting and record-keeping processes (Gov. of UK, 2021a, 2021c). Of note, one draft of the Bill included the requirement that a subset of the largest and most popular ICTs would be required to also specifically address content that is "legal but harmful" (Gov. of UK, 2021a). In supporting documentation, *legal but harmful* has been described as "likely to include issues such as abuse, harassment, or exposure to content encouraging self-harm or eating disorders" (Gov. of UK, 2022). This provision was removed from a subsequent draft of the Bill due to concerns around free speech (Sandle, 2022; U.K. Parliament, 2022b).

The current U.K. media regulator, Ofcom (Office of Communications), would be responsible for developing more detailed codes of practice and ensuring compliance with these requirements (Ofcom, 2020; Gov. of UK, 2021b). Ofcom would also be able to fine companies for non-compliance and would have the ability to block access to sites under certain conditions. Concerns have been raised that the new powers provided to the Secretary of State in the draft bill would threaten the independence of Ofcom from government interference (Perrin *et al.*, 2021).

The *Online Safety Bill* raises freedom of expression, accountability, and transparency concerns

As with similar enacted and proposed laws in other jurisdictions, critics have raised concerns that the *Online Safety Bill* jeopardizes freedom of expression and gives discretionary censorship powers to an administrative agency (Martin, 2021). Some technology companies have stated they will not know what they would need to censor under the bill (Fenwick, 2021; Martin, 2021). According to MacCarthy (2022), the bill is also missing several important features. One important omission is the lack of mandated access to social media data for independent researchers and auditors. This independent mechanism is crucial to assess the quality of social media companies' content moderation policies. The bill also minimizes the role of civil society groups, academics, technical experts, and industry representatives in the regulatory design process (MacCarthy, 2022). As of December 2022, the updated Bill was being scrutinized by Parliament and may undergo further changes (U.K. Parliament, 2022b).

5.2.4 The United States of America

The *Communications Decency Act* gives individual service providers freedom to develop their own content moderation policies

As Canada's closest international ally and trading partner, the decisions and activities undertaken by the U.S. government can have extraterritorial effects on people in Canada by encouraging Canadian governments to enact similar laws, facilitating cross-border law enforcement activities and trade. However, the U.S. approach differs substantially from that taken in the other Five Eyes. U.S. digital policy emphasizes the protection of free speech under the First Amendment of the *Constitution of the United States* (OECD, 2020b) and grants immunity to social media platforms for some user-published materials. There are some limits to this protection; the *United States Code* places restrictions on speech that solicits others to commit a felony (18 U.S.C. § 373) (Gov. of the US, n.d.-a), promotes prostitution or sex trafficking (18 U.S.C. § 2421A) (Gov. of the US, n.d.-b), or includes child sexual abuse material (CSAM) (18 U.S.C. § 2251–2260) (Gov. of the US, n.d.-c).

Section 230 of the *Communications Decency Act* (CDA), which came into law in 1996, has been central to discussions on mitigating online harms under U.S. law. Section 230 protects "interactive service providers" (e.g., a social media platform hosting third-party content) from liability over content posted by users on their platforms, with some limited exceptions (Brannon, 2019). According to Klonick (2018), "the purpose of this grant of immunity was both to encourage platforms to be 'Good Samaritans' and take an active role in removing offensive content, and also to avoid free speech problems of collateral censorship." Section 230 gives individual service providers freedom to develop their own content moderation policies. As such, nothing in Section 230 precludes service providers from removing and banning certain materials (Funk, 2021), nor does it grant immunity for federal crimes, such as publishing CSAM or content supporting terrorism. Platforms are subject to the same legal responsibility for publishing this content as anybody else. To hold a content host liable for CSAM, the government must prove it knowingly did not remove federally illegal content. However, the law does not create an obligation for platforms to proactively search for such illegal materials (Funk, 2021).

The *Fight Online Sex Trafficking Act* (FOSTA), passed in 2018, added an exception to Section 230 for sex trafficking and prostitution content (U.S. House of Representatives, 2018). This potentially makes platforms liable for posts related to sex work. As a result, websites began to censor parts of their sites that may be used for ads for prostitution (Tripp, 2019). Some consensual sex workers have been forced offline, which may have resulted in an increase in violence against them (Tripp, 2019; Newton, 2020) (Box 2.3).

Section 230 continues to be controversial, and various proposals have been considered to restrict the posting of hate speech, terrorist content, non-consensual images, or content contributing to cyber-stalking (Newton, 2020). The trade agreement among Canada, the United States, and Mexico (CUSMA) contains wording similar to Section 230 (Section 5.4).

The *Clarifying Lawful Overseas Use of Data (CLOUD) Act* minimizes baseline rule of law requirements for legal assistance requests

The CLOUD Act is a piece of U.S. federal legislation that may have global implications. One of the purposes of the act is to better enable foreign countries' authorities to obtain data about their countries' residents and citizens held by U.S.-owned companies. Under the act, the United States can enter into bilateral agreements with countries that "have robust protections for privacy and civil liberties" to obtain direct access to electronic evidence (DOJ, 2022a). In 2020, the first such bilateral agreement — with the United Kingdom — came into force. In 2019, it was announced that the United States was in negotiations with Australia and the European Union (DOJ, 2019a,b). In March 2022, the United States began negotiations with Canada (DOJ, 2022b).

Where a bilateral agreement between the United States and a foreign country exists, law enforcement agencies in either country can issue warrants or subpoenas to compel companies in the other country to provide data about residents of the requesting country (United States Congress, 2018). For example, the authorities in the United Kingdom can gain access to information about U.K. residents or citizens from U.S. companies and vice versa. However, if a U.K. law enforcement agency wants to get information about a U.S. resident from a U.S. company, a mutual legal assistance treaty (MLAT) is required.[14] The CLOUD Act includes mechanisms to challenge a warrant or subpoena if companies believe that the request violates the privacy laws of the country where data are housed (United States Congress, 2018).

Some legal experts and human rights advocates argue that the CLOUD Act fails to address serious issues regarding the origin of legal assistance requests (Guliani & Shah, 2018). While MLATs impose rule of law and human rights standards on requesting countries, the CLOUD Act minimizes these baseline requirements (Evans *et al.*, 2019). The global implication of the CLOUD Act is that residents of some requesting countries may be subject to reduced standards of protections compared to the ones they would have enjoyed under MLAT. Furthermore, Guliani and Shah (2018) argue that some requesting countries may use the information

14 MLATs are used by law enforcement agencies in conducting cross-border investigations (Dentons, 2021).

obtained under the CLOUD Act to violate human rights and target human rights activists. They go on to note that the departure from the requests assessment process linked to MLATs may result in law enforcement overreach and disclosure of information by companies writ large.

The proposed *Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act* threatens the rights to privacy and freedom of expression

The EARN IT Act, is a piece of legislation that was proposed in 2022 seeking to make electronic service providers "earn" the aforementioned Section 230 immunity over CSAM claims (United States Congress, 2022). In these cases, providers must demonstrate compliance with one of two "safe harbours" to become eligible for Section 230 protections. The first safe harbour consists of implementing federal best practices for the prevention of online child exploitation. The second option is adopting other "reasonable measures" in lieu of federal best practices (United States Congress, 2022).

Under the EARN IT Act, end-to-end encryption is likely to be considered contrary to best practices or an unreasonable measure. This is because encryption prevents a provider from seeing the content of files on its service (Pfefferkorn, 2020; Sly & Wheeler, 2022). A number of human rights advocates, academics, and organizations oppose the EARN IT Act, arguing that the potential ban on end-to-end encryption conflicts with the right to privacy. Also, by threatening tech companies with significant litigation exposure for inadequate CSAM compliance, EARN IT may lead to private censorship of legal speech, which may in turn have a chilling effect on freedom of speech and expression (Pfefferkorn, 2020). As of December 2022, this act has not been passed.

5.2.5 The European Union

The *General Data Protection Regulation* (GDPR) creates extraterritorial effects

The European Union's data and internet regulation instruments focus, first and foremost, on protecting the interests of consumers of digital services. Because the European Union is a strategic partner of Canada, E.U. legal reforms may have extraterritorial effects by applying to Canadian companies even those located outside the European Union or by encouraging domestic policy-makers to introduce similar consumer and data protection measures.

The GDPR came into effect in May 2018 and is the most comprehensive data protection law in the world. It establishes data protection as a fundamental right and promotes lawful processing of personal data and corporate compliance

(Jones & Kaminski, 2021). The GDPR has significant extraterritorial effects (EU, 2016). First, it applies to foreign data controllers if they offer goods or services to anyone located or residing in the European Union, or if they monitor behaviour within that jurisdiction. Second, it applies to the processing of personal data by a foreign data controller, where the law of a Member State applies by virtue of international agreements (e.g., consular posts) (EU, 2016). As a result, the GDPR's reach could extend to Canadian companies located outside the European Union that collect the data of E.U. residents.

There remain significant ambiguities regarding the definition of "personal data" under the GDPR

The GDPR attempts to address several challenges in the area of data protection law that are relevant to Canadian law reform. The first challenge is the meaning of *personal data* in light of changing technologies (Laidlaw, 2021b). The GDPR defines *personal data* broadly to include directly or indirectly identified and identifiable individuals and establishes different categories of sensitive personal data (EU, 2016). However, in some cases, it remains unclear whether what is collected or used constitutes personal data (Laidlaw, 2021b). For example, if a user is anonymous, then the collected data are not personal. However, many computer scientists argue that data anonymization is difficult, and a user can still be identified using data-mining techniques (Ohm, 2010). Further, inferential data present a critical privacy risk. Machine learning algorithms, for instance, can make connections between ordinary and anonymized data, drawing inferences about individuals that would be categorized as personal and/or sensitive (Wachter & Mittelstadt, 2019). The GDPR expanded the categories of sensitive data to include biometric and genetic data, but not inferential data (Laidlaw, 2021b).

There is growing momentum to improve GDPR consent models

The second challenge the GDPR attempts to address and that is relevant to Canada is the enhancement of consent models (Laidlaw, 2021b). The GDPR provides that consent must be "freely given, specific, informed, and unambiguous" (EU, 2016), and prohibits opt-out consent models. Moreover, it enables data subjects to withdraw consent, which triggers a right of erasure (which is a more accurate term than *right to be forgotten*) (EU, 2016). Despite these reforms, there is growing momentum to revamp consent models in the GDPR or other data protection laws, such as PIPEDA. In the European Union and Canada, many reform proposals focus on how to improve consent through better laws, technology, or some combination of both. Proposals for reform include strengthening accountability mechanisms for companies, such as "demonstrating compliance, encouraging industry codes of practice, using trusted third parties to vet apps and services, and shifting to a

risk-based approach" (Laidlaw, 2021b). Other suggestions include creating no-go zones, where organizations cannot rely on consent to collect and process personal data (ETHI, 2018). Ideas for technological safeguards include "codes on QR devices that lead consumer to more in-depth information, user managed portals or dashboards, and baking privacy into the design of products and services" (Laidlaw, 2021b).

Consent is only one of several lawful conditions for data processing under the GDPR, and revamping it does not fully address all instances when people may need enhanced protection of their data. Other conditions include the processing necessary for the performance of a contract; compliance with a legal obligation; protecting the vital interests of the data subject or another natural person; performance of a task carried out in the public interest; or the "legitimate interest" of the data controller (EU, 2016). In practice, many controllers may rely on the legitimate interests basis for their data-processing activities. Fraud protection, direct marketing, and processing personal data to improve a search engine may be considered legitimate reasons for data processing, meaning that they do not require consent (Edwards, 2018).

The GDPR cements and expands the scope of a right of erasure

The GDPR aims to empower data subjects by codifying their judicially recognized right of erasure (Laidlaw, 2021b). This right was confirmed in the Court of Justice of the European Union (CJEU) case *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja Gonzalez (Google Spain)*, before the GDPR came into effect (CJEU, 2014). In this case, Mr. Gonzalez requested that Google delist from its search results a link to an old bankruptcy. The CJEU held that Google was a data controller processing Mr. Gonzalez's data, and that he had a right for links to his data to be removed from search results when the data were "inadequate, irrelevant or no longer relevant, or excessive" (CJEU, 2014). The GDPR not only codified this right but also expanded its scope beyond search engines, confirming that the right is available against any data controller. Under the GDPR, any data subject has a right of erasure against any data controller, whether it is a platform, a large retailer, or a local store. The case has received attention in Canada as to whether a similar right is a legitimate interpretation of PIPEDA (Laidlaw, 2021b).

In 2021, Google adopted a global policy that allows people under 18 or their guardians to request the removal of pictures from Google search results (Sullivan, 2021). Although this policy is similar to the GDPR's right to erasure for people under 18, the GDPR's reach extends to requests to remove *any data* of an individual collected when they were a minor (EC, n.d.).

Implementation of the *e-Commerce Directive* varies among Member States

The *e-Commerce Directive* was adopted in 2000 to harmonize the obligations of information society services (ISS) (EU, 2000).[15] ISSs enjoy the same range of conditional safe harbours against liability that apply to "mere conduits" and providers engaging in "caching" or "hosting" of third-party content. The conditions for safe harbour are the most onerous for the hosts of third-party content. In order to avoid liability, the hosts shall not "have actual knowledge of illegal activity or information and, as regards claims for damages, [shall not be] aware of facts or circumstances from which the illegal activity or information is apparent" (EU, 2000). Evidence suggests, however, that the implementation of the directive varies greatly among Member States, that national liability laws remain highly fragmented, and that Member States are unclear about how they should apply it in light of the proliferation of new types of online services, such as social media companies (Madiega, 2020, 2021).

The *Digital Services Act* (DSA) modernizes the regime for online services

In 2022, the European Union adopted the DSA, which is intended to harmonize the obligations of online services, set higher standards for accountability and transparency, impose risk management obligations, and address online harms (EU, 2020; Madiega, 2021; EC, 2022a). The DSA mainly concerns intermediaries and platforms, such as "online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms" (Allen & Overy, 2020; EC, 2022a).

The most important provisions of the DSA are those that require platforms to mitigate the risk of harm, including transparency reporting and special duties for very large platforms (EU, 2020; EC, 2022b). Content moderation transparency reports need to contain information about government orders, notices submitted by users, actions taken by services on their own initiative, and information about measures against the misuse of automated content moderation tools (Nosák, 2021). These reports will allow researchers, oversight bodies, and the public to better understand the content moderation process, including who submits notices and why, and the grounds for taking down certain content (Nosák, 2021). In addition, very large online platforms (those with more than 45 million active monthly users in the European Union) are subject to special obligations regarding the spread of illegal and harmful content. They are required to put in place content moderation mechanisms, disclose their content-ranking algorithms, and provide

15 The directive defines them as any services normally provided for remuneration, at a distance, by electronic means, and at the individual request of the recipient (EU, 2000).

users with an opportunity to modify the content-ranking parameters (Allen & Overy, 2020; EP, 2022). The DSA also modernizes the liability regime for online intermediaries by requiring every hosting provider or online platform to create notice-and-take-down mechanisms for illegal content (EU, 2020). If such content is removed, an intermediary would be required to provide an explanation to the person who uploaded the content.

The *Digital Markets Act's* (DMA) interoperability requirements can weaken or undermine security and end-to-end encryption

The DMA is a law aimed at limiting the power of Big Tech companies that have a market capitalization of more than €75 billion and a user base of more than 45 million people in the European Union (Faife, 2022). Among other things, the DMA contains an interoperability requirement for messaging applications. Specifically, several gatekeepers — Apple, Google, Meta, and Microsoft — will be required to ensure the interoperability of their messaging services with other applications when requested by competitors. The goal of interoperability is to make it easier for users to transition from the gatekeepers to competing platforms, without impeding their ability to connect with users who want to stay on the larger platforms. As such, interoperability diminishes the power that gatekeepers wield over their users, and gives new services a chance to compete (Stoltz *et al.*, 2022).

Access to multiple messaging apps and services may protect users against governmental surveillance and censorship and improve the quality of services (Stoltz *et al.*, 2022). This is because new applications may offer state-of-the-art features that enhance users' privacy and provide consumer-friendly terms of service. However, the requirement of interoperability for encrypted messaging can weaken or undermine security and end-to-end encryption, which could negatively impact all users (Section 6.3). The DMA demonstrates that a technological solution that is relatively simple to convey as a policy can have unforeseen implications for security and human rights (Stoltz *et al.*, 2022). In this sense, the DMA presents similar challenges as U.S. proposals that facilitate law enforcement's access to encrypted data (Section 5.2.4).

5.2.6 Germany

Netzwerkdurchsetzungsgesetz (NetzDG) limits the online spread of illegal content

Germany's NetzDG is one of the most analyzed and influential pieces of online harms legislation. The NetzDG was passed in 2017 to limit the online dissemination of already-defined illegal content, such as depictions of violence, CSAM, and "symbols of unconstitutional and terrorist organisations," including

Nazi symbols and propaganda (Gov. of Germany, 1998; German Bundestag, 2017). The law was enacted following multiple efforts to introduce a "system of self-regulation" by social media companies to decrease hate speech on their platforms (Heldt, 2019). At the time of its implementation, the law was considered "arguably the most ambitious attempt by a Western state to hold social media platforms responsible for combating online speech deemed illegal under the domestic law" (Tworek & Leerssen, 2019).

The NetzDG requires that social network providers with two million or more registered users in Germany follow a set of regulations, with non-compliance potentially resulting in sizable monetary penalties (German Bundestag, 2017). Under the law, platforms must have a reporting mechanism that enables users to file complaints about content; once a complaint is received, the platform must review content and remove it if it is deemed illegal. The NetzDG did not create new criminal offences for online hate but rather new enforcement rules for large companies. Material that is "manifestly unlawful" must be removed within 24 hours, while all other illegal content must be removed within seven days (German Bundestag, 2017). In comparison, Canada's initial draft of a federal proposal to address harmful content online suggested a 24-hour time requirement for removing the following five categories of harmful content: "terrorist content; content that incites violence; hate speech; non-consensual sharing of intimate images; and child sexual exploitation content" (GC, 2022d). The proposal was criticized as being overly aggressive and encouraging over-censorship of non-harmful content (Andrey *et al.*, 2021b; Geist, 2021a; GC, 2022d).

NetzDG has led to platforms blocking legal content on their sites in Germany

Like other laws that govern harmful content, the NetzDG has been controversial. Critics have argued that the law could damage freedom of the press, freedom of expression, and have unintended negative effects (e.g., serve as an example for authoritative regimes to restrict speech further). The 24-hour removal provision raised concerns about the risk of over-blocking and censoring non-harmful content, as well as questions about the "privatisation of the judiciary due to the interpretation and application of criminal law by private companies" (Heldt, 2019). Heldt (2019) notes that these two outcomes could have a chilling effect on speech.

An analysis by Tworek and Leerssen (2019) found that "criticism from the tech industry, activists, and academics seemed to outweigh support." For example, as with other laws or proposal with deadlines for when platforms must respond to flagged content, Germany's removal requirement has been criticized for incentivizing the over-removal of content by platforms (HRW, 2018). Reporters Without Borders (2018) reports that the legislation has led to Meta, Twitter, and

Google blocking legal content on their sites in Germany. The majority of take-downs resulting from complaints, however, were due to violations of platforms' internal guidelines or terms of service rather than violations of German law (Tworek & Leerssen, 2019). Flagged content is evaluated against community guidelines first, before its legality in Germany is considered. As explained by Tworek and Leerssen (2019), "in this light, it may be that NetzDG's most important effect was to ensure swifter and more consistent removal of content within Germany under the companies' community guidelines."

A controversial amendment to NetzDG requires platforms to report hate speech to law enforcement

In June 2021, the *Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes* (*Act to Amend the Network Enforcement Act*) came into force. This amendment brings video-sharing platforms under the purview of the NetzDG, increases information requirements for social media providers, requires that these companies make their reporting channels for unlawful content more user-friendly, and introduces an appeal-and-reply process for the removal or blocking of access to content by companies (Library of Congress, 2021). This reform incorporates the provisions of the E.U. *Audiovisual Media Services Directive* into German law (Etteldorf, 2021).

A number of social media companies sued the German government over amendments to the NetzDG requiring platforms to proactively report hate speech to law enforcement. A German court ruled in favour of the companies on the grounds that the amendments violated E.U. law (Reuters, 2022). However, this decision applies only to the parties to the proceedings and does not change the law. The parties may appeal this decision in upper-level courts (Justiz Online, 2022).

5.3 International Cooperation

Mechanisms of bilateral and multilateral cooperation focus on collaborations between domestic intelligence and law enforcement agencies. For example, some countries, including Canada, have worked to strengthen international cooperation and harmonize their criminal laws around the Budapest Convention (Box 5.4).

Box 5.4 The Budapest Convention on Cybercrime

The *Convention on Cybercrime*, open for signing as of 2001, is the first international treaty meant to address cybercrime by harmonizing laws, supporting domestic law enforcement and prosecution, and increasing cooperation among signatories (COE, n.d-a,-b). As of January 2022, 66 states were parties to the convention; these include most E.U. countries, Australia, Canada, the United Kingdom, and the United States. Canada was one of the original signatories and ratified the convention in 2015 (COE, 2022).

The convention has two chief purposes: to provide guidelines for countries developing legislation on cybercrime, and to act as a legal framework for cooperation among Parties (COE, 2021a). Moreover, according to the Council of Europe, "indications are that private sector entities [...] are more likely to cooperate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place" (COE, 2021a).

In 2006, an additional protocol came into force, one that extends the scope of the convention to offences related to racist or xenophobic propaganda (COE, 2021b). Yet another protocol seeks to support greater cooperation from internet service providers and disclosure of electronic evidence (COE, 2021c). This would provide "a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards" (COE, 2021c). Civil society groups have criticized these provisions, as well as procedures for their adoption (Gullo & Rodriguez, 2021). The additional protocol was opened for signing in May 2022.

There are international cooperation efforts at the level of the G7 and the Five Eyes

Beyond the Budapest Convention, Canada is engaged in international cooperation efforts at the level of the G7 and the Five Eyes (Dizboni & Leuprecht, 2020). The members of the G7 are committed to implementing the United Nations Security Council resolutions that focus on, among other things, preventing violent extremism and terrorist use of the internet. Notably, G7 security ministers have been focusing on preventing the spread of hateful ideologies online and highlighting the importance of collaboration with the private sector (e.g., Meta, Twitter, Google, Microsoft) (Dizboni & Leuprecht, 2020). In a statement released

in 2018, security ministers listed a number of measures, including "the removal of content and accounts within 1 hour of upload, where technically feasible, without compromising accuracy" and preventing "the recurrence of violent extremist and terrorist content by contributing to and utilizing the Shared Industry Hash Database and by publishing performance metrics" (GC, 2018b). As with domestic take-down requirements, the G7 proposals on expedited content removal raise concerns about private censorship of legal speech and may have a chilling effect on freedom of expression.

In a joint communiqué issued in 2017, Five Eye ministers and attorneys general emphasized the need for a common strategy for working with communication service providers to limit the spread of online terrorist activities and propaganda (PS, 2017a). They also supported creating an industry forum led by Google, Meta, Microsoft, and Twitter. To tackle the challenges that encryption poses to public safety, the Five Eyes have urged technology companies to develop backdoors that allow law enforcement agencies to access encrypted messages, but this has been met with concerns related to human rights and privacy (PS, 2017a) (Section 6.3). Some have noted that the Five Eyes provides a better forum for developing more concrete and ambitious cooperation goals than the G7 because the G7 is more geographically diverse and aims to influence a variety of states by incorporating United Nations documents into its goal-setting process (Dizboni & Leuprecht, 2020).

The *Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online* is an example of international cooperation

New Zealand has been leading international efforts to remove terrorist and violent extremist online content through the *Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online*. The Governments of New Zealand and France co-created the initiative in response to the 2019 terrorist attack on the Muslim community in Christchurch, New Zealand (Christchurch Call, 2021). The call encourages participating governments and organizations to voluntarily limit the spread of terrorist and violent extremist content (TVEC) "in a manner consistent with international human rights law and fundamental freedoms" (Christchurch Call, 2021). As of 2021, 48 countries (including Canada), 10 technology companies, the European Commission, and 2 international organizations have joined the call (Christchurch Call, 2021), which asks participating governments to develop and support policies that counter the factors driving extremism and terrorism, support frameworks that minimize the amplification of TVEC, and enforce laws that prohibit TVEC (Christchurch Call, 2019).

5.4 Proposed Policy and Legislation to Address Online Harms in Canada

In Canada, various policy proposals on how to address online harms have been resurfacing and evolving over the years, but legislative activity on these issues accelerated in 2020. Many proposals coming from policy-makers, in response to cyber-enabled crimes and harms, advocate reforms of differing scope — from a comprehensive overhaul of the regulatory framework (e.g., regulating online communication service providers) to separate measures aimed at regulating different harmful activities (e.g., treating hate speech as a discriminatory practice under the *Canadian Human Rights Act*). Most of these proposals focus on designing the regulatory apparatus to oversee digital spaces, and on allocating functions to existing or new government agencies, such as the CRTC, the Canadian Human Rights Commission, and the Digital Safety Commission of Canada.

A non-legally binding digital charter contains principles relevant to digital public safety

In 2019, Innovation, Science and Economic Development Canada (ISED) released *Canada's Digital Charter in Action: A Plan by Canadians, for Canadians* (The Digital Charter) (ISED, 2019). The Digital Charter is an unenforceable policy statement that includes 10 principles (Figure 5.1) intended to "help guide the federal government's work, serving as a digital charter for Canadians to help address challenges and leverage Canada's unique talents and strengths in order to harness the power of digital and data transformation" (Choi, 2019; ISED, 2019). Several elements are critical to public safety, including safety and security, freedom from hate and violent extremism, and strong enforcement and real accountability (ISED, 2019). The Digital Charter also recognizes the importance of protecting individual rights, including privacy. It was meant to inform specific legislation and, as such, does not contain any legally enforceable privacy protection mechanisms and fails to give people more control over their data (Choi, 2019; Dubois & Martin-Bariteau, 2020b).

1	Universal Access	6	A Level Playing Field
2	Safety and Security	7	Data and Digital for Good
3	Control and Consent	8	Strong Democracy
4	Transparency, Portability and Interoperability	9	Free from Hate and Violent Extremism
5	Open and Modern Digital Government	10	Strong Enforcement and Real Accountability

Reproduced with permission from: ISED (2019)

Figure 5.1 Ten Principles of Canada's Digital Charter

The ten principles of Canada's digital charter were developed following a four-month national consultation process.

5.4.1 Legislative Proposals for Digital Content, Online Harms, and Privacy

Several pieces of proposed legislation related to digital content, online harms, and privacy have been introduced or proposed in Canada since the release of the Digital Charter. For example, in the 43rd Parliament (December 2019 – August 2021) (House of Commons of Canada, n.d.), Bills C-10 (2020), C-11 (2020), and C-36 (2021) proposed changes to legislation regarding online content, privacy protections, and hate speech, respectively, while the federal proposal to address harmful content online (Section 5.2.6) suggested new mechanisms to deal with online harm. All of these bills died on the Order Paper (i.e., failed to pass during the session) when a federal election was called for the fall of 2021, though some were reintroduced in substantially similar formats in subsequent parliamentary sessions. The Panel discusses these only briefly, in terms of the challenges they seek to address and the general approach they take.

Proposals to regulate online audio and audiovisual content had an overbroad reach and interfered with freedom of expression

In 2020, the government proposed Bill C-10 (*An Act to Amend the Broadcasting Act and to Make Related and Consequential Amendments to Other Acts)*, which intended to bring online audio and audiovisual content providers under the purview of the *Broadcasting Act* (Brideau *et al.*, 2020; House of Commons of Canada, 2021). The *Broadcasting Act* outlines the roles and powers of the CRTC to regulate and supervise Canada's broadcasting system. Currently, the act applies to traditional "over-the-air" broadcasters. This means that internet-based services, such as Netflix and Spotify, are not subject to the same requirements as traditional television and radio stations. Bill C-10 (2020) would have extended rules meant to promote Canadian content in terrestrial broadcasting environments to internet-based services (so-called "online undertakings"). The bill came under significant criticism on the grounds that it would unduly enable the government to regulate or interfere with individuals' free speech, as well as impair Canadian creators' abilities to be successful on online platforms, and ultimately died on the Order Paper (Raman-Wilms & Curry, 2021; Smith, 2021b; Geist, 2022a).

In February 2022, during the 44th Parliament, the bill — renamed the *Online Streaming Act* (C-11) — was reintroduced. The federal government argued the new bill addressed the controversial issues surrounding user-generated content in the previous iteration. The Minister of Canadian Heritage, Pablo Rodriguez, stated that the bill would not affect users, online creators, or digital-first creators, only the platforms that host content (Carbert, 2022; Gilmore, 2022). Initial reception of the proposal was mixed. The Canadian Independent Music Association and other music industry groups appeared to generally support the bill for its ability to protect and develop Canadian musicians and artists (Gilmore, 2022). It has been argued, however, that C-11 (2022) does not fix the fundamental problems with C-10 (2020) (Bhullar, 2022). One concern raised by legal experts is uncertainty created by the wording of the bill; for example, it could potentially cover any global audiovisual service that has Canadian customers (Geist, 2022a). Further, although the bill provides exemptions for user-generated content, it also includes criteria on when such content would not be exempt and minimal guidance on how these criteria would be applied (Geist, 2022a).

Another unpassed piece of Canadian legislation was Bill C-11 (2020) (*An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to Make Related and Consequential Amendments to Other Acts).* Among other things, the goal of the bill was to modernize how personal data and privacy are handled in the private sector in Canada, in light of the proliferation of digital data and applications (GC, 2020c). Commentary on Bill C-11 (2020), including from academics and the OPC, argued that, while the bill

represented a needed update to Canadian privacy legislation, it did not adequately address meaningful consent, the de-identification of personal data, or data mobility (portability) (e.g., Kenyon, 2021; OPC, 2021b; Scassa, 2021). The OPC noted that the bill's attempt to address privacy issues associated with the digital economy was misaligned and less protective than approaches taken in other jurisdictions (OPC, 2021b).

The goal of Bill C-36 was to protect people in Canada from hate speech in an online environment

In 2021, Bill C-36 proposed changes to address online hate through amendments to the *Criminal Code* and *Canadian Human Rights Act.* One objective of the bill was to address hate online by amending the *Canadian Human Rights Act* to:

> *provide that it is a discriminatory practice to communicate or cause to be communicated hate speech by means of the Internet or other means of telecommunication in a context in which the hate speech is likely to foment detestation or vilification of an individual or group of individuals on the basis of a prohibited ground of discrimination.*
>
> GC (2021h)

This amendment would have allowed the Canadian Human Rights Commission to admit complaints related to online hate disseminated by online communication service providers, giving it the authority to "adjudicate complaints and order remedies" related to online infractions (GC, 2021g,h). Bill C-36 (2021) died on the Order Paper when Parliament was dissolved in August 2021 (Smith, 2021b).

The proposal to address harmful online content encroached upon constitutional rights

The most comprehensive plan to address online harms in Canada was the federal proposal to address harmful content online, which (as noted in Section 5.2.6) sought to provide new mechanisms related to five categories: "terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate images, and child sexual exploitation content" (GC, 2021g). The nature of the proposal suggests the Government of Canada drew inspiration from legislation in other countries, especially Germany and Australia (Meyer, 2021; Tworek, 2021b) (Section 5.2). The primary entities to be regulated under the proposal were online communication service providers (OCSP). Such a service was defined as one "that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet" (GC, 2021i). This definition was specifically intended to include major platforms such as Facebook, YouTube, Pornhub, and Twitter, and to exclude online tools that

are not communication providers (e.g., fitness apps, travel review websites), private communications, and telecommunications service providers (GC, 2021g). The Panel finds that it is not entirely clear how the government arrived at its conclusions, given that many of the excluded websites had functionality that bore resemblance to websites and services that were to be captured under the plan.

OCSPs would be required to "take all reasonable measures" to ensure harmful content is inaccessible to users in Canada, including "whatever is reasonable and within their power" in terms of self-monitoring their platform for harmful content. User-flagged content would have to be reviewed by OCSPs within 24 hours and taken down if that content "should be made inaccessible" according to the definitions in the regulations. OCSPs would also be required to set up appeal systems for content authors and those who flag content (GC, 2021g).

The proposal included the creation of a Digital Safety Commission of Canada that would support three new entities to oversee and enforce the new rules: a Digital Safety Commissioner, a Digital Recourse Council of Canada, and an advisory board. The commissioner would administer and enforce the new requirements, take complaints from OCSP users about online content, issue compliance orders, inspect for OCSP compliance with the regulations and decisions, and issue fines in cases of non-compliance (GC, 2021i). In extreme cases of non-compliance related to child sexual exploitation or terrorist content, the commissioner could apply to the Federal Court to block part or all of an OCSP in Canada. The proposed Digital Recourse Council of Canada would be an independent avenue for OCSP users to appeal content moderation decisions made by an OCSP (GC, 2021g). Both the Digital Safety Commissioner and the Digital Recourse Council would be supported by the advisory board (GC, 2021g).

In addition to the aforementioned regulations and regulatory bodies, the proposal included modifications to current legislation regarding online harms. It introduced changes to the *Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons Who Provide an Internet Service*, which requires internet service providers to report instances of CSAM hosted on their servers to authorities (GC, 2011a) and links to CSAM not hosted on their service to the Canadian Centre for Child Protection (C3P) (GC, 2011b). Changes to the act included, among others, centralizing the reporting of CSAM through the RCMP's National Child Exploitation Crime Centre (NCECC), as recommended by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI, 2021); clarifying that the act applies to all types of internet services (including OCSPs); lengthening the computer data preservation requirement from 21 days to 12 months; and adding a requirement that any "persons who provide an internet service" must provide additional information to NCECC (judicial

authorization not being a requirement) in cases where a child pornography offence is identified (GC, 2021g; Parsons, 2022). It was not clear whether this additional information should include basic subscriber information or transmission data (GC, 2021g). However, some experts contended "that reporting and preservation obligations are of limited use," as law enforcement does not have time and resources to process all reported content and "cross-reference it with offline information" (GC, 2022e).

Finally, the federal proposal included changes to the *Canadian Security Intelligence Service Act* that would provide a new mechanism for CSIS to receive authorization to obtain basic subscriber information more quickly (GC, 2021i). Authorization would be issued by a judge of the Federal Court and subject to ministerial oversight (GC, 2021g).

In February 2022, the federal government released a written report summarizing the feedback received on the draft proposal and acknowledged that there were a number of "overarching concerns [...] related to the freedom of expression, privacy rights, the impact of the proposal on certain marginalized groups, and compliance with the Canadian Charter of Rights and Freedoms" (GC, 2022d). In March 2022, the Government of Canada appointed an expert advisory group whose mandate was, among other things, to suggest changes to the federal proposal (GC, 2022f).

Bill C-27 (2022) did not fully address the concerns of privacy advocates

In 2022, the Government of Canada introduced Bill C-27 (*An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts)* (House of Commons of Canada, 2022). This revised version of the former Bill C-11 (2020) died on the Order Paper prior t o the federal election in 2021 (Alavi *et al.*, 2022). Bill C-27 (2022) was a complex reform proposal that focused, among other things, on the de-identification of data, reforming consent as the basis for using data, and facilitating the use of data by the private and public sectors (Geist, 2022b). The proposed *Consumer Privacy Protection Act* (which would replace PIPEDA) did not apply to anonymized data and provided little background on how organizations should carry out data anonymization (Scassa, 2022a). It also attempted to incorporate the "legitimate interests" basis for data processing, available under the GDPR, into Canadian privacy law. However, compared to the GDPR, Bill C-27 (2022) made the "legitimate interests" exception potentially a more common basis for the use of personal data "without knowledge or consent" (Scassa, 2022b). Moreover,

provisions aimed to facilitate the government's use of private sector data did not contain adequate protections of collective or individual privacy and minimized protections available under applicable laws (Scassa, 2022c).

Canada's obligations related to intermediary liability under the Canada-United States-Mexico Agreement (CUSMA) are unclear

Intermediary liability is a complex issue that crosses different jurisdictions and areas of law. Canada does not have broad intermediary liability laws such as those in the European Union, or the *E-Commerce Directive* and Section 230 of the *Communications Decency Act* in the United States; rather, intermediary liability in Canada has primarily developed in the common law of defamation and copyright law (Laidlaw, 2021b). In addition, Article 19.17 of CUSMA requires Parties to provide online intermediaries with protections against liability relating to their hosting of user-generated content (GC, 2020d). The wording of this provision is modelled after Section 230 of the U.S. *Communications Decency Act*. However, CUSMA does not incorporate Section 230 into Canadian law. The agreement allows for domestic interpretation of these provisions, and a Party may comply with Article 19.17 through its laws, regulations, or judicial application of existing legal doctrines (Ha-Redeye, 2021). Some legal experts recommend introducing legislation in Canada that would clarify how Article 19.17 of CUSMA will be applied in general, and to Canadian and third-country intermediaries in particular (Krishnamurthy *et al.*, 2020).

5.5 Summary

To address the charge, which required the assessment of evidence and knowledge of leading practices for preventing and countering threats to public safety, the Panel focused on current and potential legal avenues that could apply in Canada. The existing domestic web of legal frameworks — torts, criminal law, Quebec's civil law, provincial and federal privacy legislation, and other instruments — empowers individuals, state agents, and private organizations to address criminal and harmful behaviours that occur through ICTs.

This web, however, is complex and faces challenges due to the development of new and modified ICTs. Criminal law, it has been argued, has a blind-spot when it comes to engaging with the experiences of women and girls who are victims and survivors of cyber-enabled violence. FINTRAC's potential to prevent cyber-enabled fraud and money laundering is limited by a lack of investigative and law enforcement powers. An outdated understanding of privacy in tort law fails to protect participants in a data-driven economy. Defamation law has strained to adapt to the global nature of online activities and is ill equipped to address the

issue of internet intermediary liability. Finally, public-private cooperation and a lack of enforcement powers present challenges for the federal privacy regime applicable to private sector organizations. In sum, the Panel found that technological change presents challenges for both public and private law, with the effect that policy-makers are considering how domestic law reform might overcome some of the challenges that ICTs pose for public safety in Canada.

Proposals on how best to use law to enhance the overall health of the online ecosystem are being made around the world. Australia, Germany, New Zealand, the United Kingdom, the United States, and the European Union have introduced or passed legislation that seeks to address the proliferation of cyber-enabled crimes and harms. The Panel found, however, that none of the approaches fully solve the problem. On one hand, measures aimed at increasing regulatory oversight over digital spaces (e.g., state-sanctioned take-down notices) have led to the over-removal of legal content and raised freedom of expression concerns. A lack of state intervention under some immunity and safe harbour regimes, on the other hand, grants private corporations discretion over how to best curate online speech and may lead to under-regulation of digital spaces. These issues, as well as differences in legal systems and legal cultures, need to be considered when assessing the extent to which approaches from other jurisdictions are appropriate for the Canadian context.

While this chapter provided an overview of existing and proposed laws and regulations, the *enforcement* of laws applicable to cybercrime faces an additional set of challenges, which are examined in Chapter 6.

6

Law Enforcement Challenges and Opportunities

Chapter Findings

- Insufficient resources within law enforcement agencies and the broader justice system present a key barrier to investigating and prosecuting cyber-enabled crime in a timely manner.
- The criminal justice system is unable to effectively deal with the increasingly digital nature of crime because of insufficient general and specialized digital knowledge at the prevention, investigation, and prosecution stages.
- A range of digital tools are available to support the prevention and investigation of cyber-enabled crime, but each has legal, societal, and privacy implications that should be independently assessed and monitored before, during, and after they are put in use.
- Poor communication within and across law enforcement agencies can lead to confusion and inefficient application of resources.
- Critical data gaps around the frequency and impact of cyber-enabled crime hinder the ability of law enforcement agencies and governments to address challenges and evaluate the effectiveness of interventions.

Canada is facing considerable challenges in applying existing frameworks that prohibit certain harmful behaviour taking place online. This means that, even in cases where there are laws or regulations that enable law enforcement agencies to respond to such harms, these same agencies are often stymied in their abilities to investigate and prosecute criminal activities. Effective police services are essential for protecting public safety and human rights in a democratic society, and the demands placed on these services in Canada have increased substantially. The challenges faced by law enforcement in applying laws against online harm stem primarily from insufficient adaptation of existing structures and approaches to a criminal landscape drastically altered by digital technologies.

This chapter begins by outlining the substantial data and knowledge gaps that exist around cyber-enabled crime in Canada, which make it impossible to accurately understand impacts, effectively allocate resources, or engage in any meaningful evaluation of new measures. Despite these critical data gaps, the evidence is clear that instances of cyber-enabled crime are increasing, under-reported, and straining the capacity of Canada's law enforcement agencies. The severe shortage of specialized digital skills within law enforcement has led to

considerable delays in processing digital evidence. At the same time, a lack of basic digital skills makes it difficult for generalist officers to respond to cyber-enabled crime. This shortage in specialists is partially tied to the systemic challenges created by the outdated organizational structure of law enforcement agencies in Canada and a resistance to change, despite the expanded roles police are expected to play. To address these challenges, the Panel discusses opportunities to modernize law enforcement through increased professionalization, improved digital training, and cross-agency coordination.

The chapter then considers challenges facing criminal investigations, starting with outlining the difficulties law enforcement face in accessing digital evidence. The Panel reviews opportunities and considerations related to processing data, digital detection, and online reporting before moving to a more in-depth discussion of the benefits and risks associated with artificial intelligence (AI). For example, violations resulting from the use of facial recognition technology (FRT) by law enforcement were predicted by many experts and illustrate the substantial risks of new technologies being deployed without appropriate guidance, transparency, and accountability. The Panel emphasizes the necessity of having clear guidelines for law enforcement on the tools and approaches they use, as well as independent assessment prior to the deployment of new technologies, and ongoing monitoring to ensure human rights and privacy are protected. Finally, the Panel briefly outlines the challenges created by capacity constraints across the criminal justice system, including within the court system, which are particularly damaging given the constitutionally mandated timelines to bring criminal cases to trial.

The Panel finds that the challenges facing Canadian law enforcement in light of the proliferation of cyber-enabled crime are substantial and will only increase as cyber-threat actors find new ways to use technology as a tool to inflict harm. These challenges demand that law enforcement agencies improve their approaches to preventing, investigating, and prosecuting cyber-enabled crimes. Using digital tools in compliance with privacy and human rights requirements can support law enforcement agencies as they seek to ensure public safety is protected from malicious actors.

6.1 Data Gaps

There are insufficient data to assess the frequency and impact of cybercrime in Canada

Historically, the best Canada-wide data, collected and housed by Statistics Canada, have been severely insufficient for several reasons, including inconsistent definitions and reporting across departments (Chapter 1). This gap critically results in a lack of reliable and consistent cybercrime data; it prevents police organizations from understanding the full extent of the problem and from using the best cybercrime intervention and prevention strategies (Dupont, 2021). Changes in how cybercrimes are reported in Canada may partially address this challenge (StatCan, 2021c). It has been announced that police across the country will be expected to categorize cyber-assisted and cyber-enabled criminal activities using the North American Cyber Classification Compendium (NACCC) and share these data with Statistics Canada (Section 1.3.2).

Data limitations extend to the makeup of police units and the specific capacity gaps they face. For instance, it is difficult to determine how many digital forensics specialists there are in Canada, because police forces and Statistics Canada do not collect this information systematically and consistently (Dupont, 2021).

Increasing the frequency of cyber-victimization surveys in Canada (which are administered in other countries, such as the United Kingdom) may aid the planning and implementation of effective cybercrime measures (Dupont, 2021). Such surveys are useful in directing resources to help victims and survivors of cyber-enabled crime, but they also help identify approaches to prevent victimization. In particular, regularly updating statistics related to cyber-victimization would be particularly useful for crimes that are chronically under-reported, as limited information on frequency and impact can be gleaned from police-reported crime statistics. Further, reliable statistics and research that measure both the prevalence of cybercrime and its direct and indirect impacts on people would help in the development, implementation, and evaluation of strategies to combat it (Dupont, 2021). Until reliable, consistent, and effective statistical reporting takes place, it will be challenging for governments in Canada to identify where problems lie, where actions are addressing existing illegal or harmful activities, and where further resources may be needed.

A lack of data minimizes the magnitude of the impact of cyber-enabled crime and prevents robust evaluation of interventions

In the view of the Panel, the substantial data gaps related to cyber-enabled crime in Canada can create an illusion that its impacts are not severe or prevalent, despite the growing body of qualitative or anecdotal evidence suggesting

otherwise. It also makes it difficult to accurately direct resources and actions toward where they might have the greatest impact, simply because the areas most in need of resources are not always immediately apparent. Moving forward, new policies, approaches, or technologies implemented to support public safety would be of greater benefit if they were accompanied by a robust public record of online harms and crimes, and could support high-quality research; this is presently lacking in the policing field in Canada. Evaluation partly entails establishing a baseline that is currently impossible, given the dearth of data related to cyber-enabled crime and its impact in Canada. Filling gaps and supporting robust evaluation would have substantial benefits for policy-makers and law enforcement specialists, such as enabling them to better understand and address challenges, direct resources, and expand the most effective new initiatives.

6.2 Structure and Staffing

6.2.1 Specialized and Basic Digital Skills

There is a shortage of the specialized expertise and resources needed to analyze digital evidence

In recent decades, policing has become more complex and progressively more demanding for a range of reasons, including the proliferation of cybercrime (Leuprecht, 2019) and judicial decisions that require officers to follow investigative procedures seen as complicated or time-consuming (e.g., accessing basic subscriber information, discussed in Section 6.3.1). At the same time, resources to investigate cyber-enabled crimes, including up-to-date expertise and technical resources, are becoming scarcer (Dupont, 2021). While insufficient capacity has practical implications for all types of crime, the problem may be particularly acute for cyber-enabled crime (or other crimes with substantial cyber elements).

Digital evidence has several traits that differ from physical evidence. It is frequently wider in scope, may be more personally sensitive, is generally mobile, and requires different training, expertise, and tools (Goodison *et al.*, 2015). Investigations often involve multiple electronic devices (e.g., laptops, smartphones, GPS units) that may contain relevant digital evidence, each with different infrastructures and operating systems (Vincze, 2016). It is unlikely that one investigator has the specialized knowledge to examine every device involved, meaning that several investigators must work in tandem, stretching staff capacity (Vincze, 2016).

Even if the technological tools needed to analyze and process digital evidence are available, specialized policing often requires significant manual labour. For instance, sophisticated database search tools can narrow down possible matches for a perpetrator, but the final match is conducted by police officers

themselves through lengthy manual assessments (Watson & Huey, 2020). Some of the technology-enabled opportunities discussed in Section 6.3.3 will reduce the demand for labour, but they will not address the issue of insufficient capacity writ large as there is a shortage of personnel with the digital expertise needed to fill cyber-specific roles. The problem is partially due to the paramilitary structure of policing outlined in Section 6.2.2.

Capacity constraints have resulted in digital evidence backlogs

Both the high prevalence of cybercrime and the need for specialized expertise have prompted the creation or expansion of specialized police units, which often have long processing times due to insufficient resources, a growing number of requests for technical assistance, and large amounts of data and equipment seized during investigations (Baril, 2014; Dupont, 2021). These digital evidence backlogs are made worse by a lack of available equipment (Goodison *et al.*, 2015). This is a problem across many jurisdictions.

In England and Wales, for example, as of March 2022, there were over 12,000 digital devices waiting to be examined across 32 forces (ITV News, 2020). Simon Kempton, technology lead for the Police Federation of England and Wales, explained that investigators were "overwhelmed" by digital evidence. He also noted that "the biggest issue with having a backlog of devices is it is resulting in disclosure issues, with potentially vital pieces of evidence not making it to court in time" (ITV News, 2020). Although data on backlogs in Canada could not be identified, similar issues exist domestically, in the experience of Panel members.

There is a shortage of basic digital skills within law enforcement

Beyond insufficient staffing for specialized roles, law enforcement widely lacks the general digital skills needed to respond to cyber-enabled crime. One study found that more than 60% of police officers in England and Wales felt unprepared to respond to cybercrime incidents (Burruss *et al.*, 2020). Relatedly, a survey of patrol officers in the United States found that most officers believed local law enforcement should not be the primary responder to cybercrime incidents, which would be better served by specialized units (Bossler & Holt, 2012). Similar findings have been reported in Australia (Cross *et al.*, 2021). Furthermore, the general level of knowledge about the characteristics of cybercrime and how to preserve digital evidence is low (Dupont, 2021). These skills deficits may be impacting how officers respond to reports of cyber-enabled crime. A survey-based study of police officers in England and Wales found that, despite most officers being exposed to cybercrime incidents, they spend a relatively small proportion of their work hours responding to them compared to other types of crime (Holt *et al.*, 2019).

While equivalent data are not available in Canada, similar trends have been observed (Dupont, 2021).

Increased funding for enhancing cybersecurity in Canada has not been directed to local law enforcement

Dupont (2021) argues that the most challenging thing about fighting cyber-enabled crime in Canada (e.g., online exploitation) is the lack of capacity to deal with the sheer volume of incidents that occur. As discussed in Chapter 3, the majority of these crimes occur from within Canada, meaning they are under the jurisdiction of local law enforcement agencies (including the RCMP). Of note, while "enhancing Canada's cyber security" was addressed in the 2022 federal budget, the vast majority of new funding ($875.2 million over five years) was directed to the Communications Security Establishment (CSE),[16] with no funding under this initiative earmarked for Public Safety Canada or the RCMP (GC, 2022b).

6.2.2 Recruiting and Retaining Specialists

The paramilitary structure of policing in Canada does not lend itself to retaining the specialized skills needed to investigate cyber-enabled crime

In Canada, most police services follow a paramilitary model whereby there is a rigid rank structure and common basic training (Fry & Berkes, 1983; SECU, 2021). The paramilitary structure of policing generally brings in new recruits at the bottom of the police hierarchy, with initial training focused on rapid response and patrol, regardless of the particular needs of a given police force. While officers may join a force with specialized digital skills, or develop these skills on the job, the promotion system does not incentivize skills development. As explained by CCA (2014), the current system "privileges promotion for time served over specialization and development of expertise." Furthermore, the Panel notes that accepting promotion and moving up the ranks often require officers who have developed specialized digital skills to move into divisions where they cannot apply those skills or develop them further.

The challenges created by the promotion ranks within law enforcement are not unique to Canada. Some policing agencies are, however, taking steps to encourage skills development and ongoing education. For example, the national gendarmerie[17] in France began a program in 2018 that provides support to gendarme officers who want to pursue a PhD (CGE, 2022). This includes tuition,

16 A small portion of new funding was earmarked "to expand cyber security protection for small departments, agencies, and Crown corporations" (GC, 2022b).

17 The gendarmerie nationale is a branch of the French Armed Forces that is responsible for policing in France's rural regions (Terrill, 2013).

days off, and guidance (e.g., identifying potential supervisors, making connections with relevant business experts). Once their degree is complete, gendarme are provided with a special pin to display on their uniform, reflecting the gendarmerie's desire to showcase and reward ongoing education (Ministère de l'Intérieur, 2019).

Internal perceptions of cybercrime and the role of digital specialists can impact capacity

A lack of appreciation for cyber-specialists working in the policing ecosystem, coupled with their low visibility, can also contribute to or augment capacity constraints. One study found that the work Canadian police officers do in internet child exploitation units is not always recognized as "police work," which can lead investigators to experience feelings of alienation, cynicism, and low career satisfaction (Spencer *et al.*, 2020). Another study in Australia found that specialists in cyber units feel they do not get adequate resources or recognition for their work, which negatively impacts staff recruitment (Harkin & Whelan, 2019). Staff's negative experiences result, in part, from upper management, supervisors, and police officers in other units often having a limited understanding of the nature of the work and the needs of cyber-policing units; this has a corresponding impact on these specialists' willingness to stay, as it does on broader organizational commitment to invest in ongoing cyber-related training (Harkin *et al.*, 2018).

The placement of cyber-enabled crime within an informal hierarchy of criminal activities influences both police perceptions and how they respond when these activities are reported (Dupont, 2021). An interview-based study from Australia found that law enforcement may minimize the harms of online partner abuse, cyber-stalking, and cyber-harassment (Powell & Henry, 2018). This reaction may be partly due to law enforcement officers feeling as if they lack the skills to respond to cyber-enabled crime effectively (Dupont, 2021). Police acknowledgement of cyber-fraud, for example, is important for victims, as it can validate their concerns, encourage reporting, and help alleviate feelings of shame (Cross & Blackshaw, 2015).

The civilianization of law enforcement is increasing, but the salaries of employees with specialized digital skills will have to be comparable to, or higher than, those of uniformed officers

Civilianization refers to the use of civil employees (i.e., non-officers) within police forces to carry out select tasks. In theory, it allows officers to focus their attention on aspects of law enforcement that they are uniquely capable of performing (Kostelac, 2008). CCA (2014) found that the proportion of civilians working in police forces relative to officers was on the rise in Canada, although there was limited information on the exact positions they were filling. Having said this,

cybercrime units across Canada have begun civilianizing some of their positions. In 2019, the Ontario Provincial Police (OPP) opened a centre for cyber operations that includes a cybercrime investigations team, a digital forensics team, and a forensic video analysis unit, relying on a blend of uniformed members, special constables, and civilians with technical expertise (Goldfinger, 2019). Likewise, in 2021, the RCMP announced it would also be incorporating 35 civilian investigators into its operations (Northcott, 2021).

Two of the cited benefits of hiring civilian staff — they are paid less than officers and can build up stable expertise in a force (CCA, 2014) — are not applicable to civilians with high-level digital skills. To attract highly qualified personnel to work in digital forensics, salaries and benefits may need to be comparable to that of officers (Kiedrowski *et al.*, 2015), while fully trained specialists may demand even higher salaries to compete with those in the private sector (Dupont, 2021). While, in theory, the lack of promotion keeps expertise in place, the absence of any opportunities for advancement in civilian positions may cause specialists to leave police organizations after a few years, particularly if their salaries are considerably lower than those in the private sector. As a result, setting up civilian positions that are not competitive with other public or private sector roles may lead to recruitment challenges and frequent turnover, with the effect that the civilianization of law enforcement may not improve its current specialized digital skills shortage. Increased professionalization of policing in Canada (Section 6.2.4) may therefore be a more effective measure to ensure sustained capacity of digital specialists in Canada's police forces.

6.2.3 Cooperation and Coordination

There are cooperation challenges within and across law enforcement agencies

A range of law enforcement agencies across Canada have responsibility over different jurisdictions and, in some cases, different criminal activities (StatCan, 2020b). Coordination among law enforcement agencies is especially relevant for crimes that occur across jurisdictions, as is often the case for cyber-enabled crime. In these types of crimes, victim and perpetrator may be physically located in different jurisdictions, and digital evidence is often hosted by an international service provider (e.g., social media platforms) (Powell & Henry, 2018). Cyber-enabled crime is highly globalized, and police organizations are often organized locally, making it difficult for them to adapt their intervention tactics (Dupont, 2021).

A lack of coordination and mutual understanding regarding what information can be shared between law enforcement and intelligence agencies in Canada is a concern (NSIRA, 2019a; Carvin *et al.*, 2021b). While there are many instances where

information flow among intelligence agencies should be limited, a review of CSIS's Internal Security Branch found that CSIS did not have clear policies and procedures on how and when it can and should report and share intelligence with law enforcement (e.g., suspected criminal activity found during a security assessment) (NSIRA, 2019b). Based on the analysis of one case, there were delays in the process of intelligence sharing (NSIRA, 2019b). Another review found that some cooperation barriers between CSIS and the RCMP involve incompatible or insecure inter-agency communication systems, and resistance to disclose CSIS sources and methods in criminal prosecutions (NSIRA, 2019a). This has resulted in the under-utilization of CSIS intelligence in RCMP investigations (NSIRA, 2019a), which may undermine efforts to combat cybercrime in Canada. There are also coordination challenges among different units within a given force — a problem that is not unique to Canada. Specialized police units that deal with a variety of cybercrime investigative actions (e.g., forensics, intercepting electronic communications, cyber-attacks) are not always well integrated with the efforts of locally based frontline police officers or criminal prosecutors (Goodison *et al.*, 2015; Dupont, 2021).

6.2.4 Opportunities to Modernize Law Enforcement

Professionalization of policing could support the development of specialized digital skills, but standardization of digital skills training remains elusive

Police officers in Canada take on a range of different roles, each of which requires specific skills; that said, some officers may not be sufficiently trained to succeed in their role. This includes tackling the growing issue of cyber-enabled crime, which requires specialized digital skills not needed for exclusively non-digital crimes (Dupont, 2021). There have been calls for police forces to move toward increased professionalization for a variety of reasons, including enabling the differentiation of roles within law enforcement and less reliance on generalist police officers (CCA, 2014). While generalists will still be required, particularly for responder work, differentiation would enable officers to specialize in a particular field and stay in that field, even as they are promoted.

Professionalization can include formal accreditation, such as standardization and qualification, which removes some of the training burden from law enforcement agencies themselves (CCA, 2014). Standardization also creates uniformity across law enforcement agencies and supports accountability and legitimacy. As with many other professional occupations, continuous professional development can be linked to both accreditation and advancement, ensuring employees are encouraged and rewarded for continuing to develop their skills (CCA, 2014).

A core question is how to professionalize digital training for police forces, given the lack of standardization across police training institutions, universities, and colleges (Goodison *et al.*, 2015; Dupont, 2021). For example, the British Columbia Institute of Technology's two-year Bachelor of Technology degree in forensic investigation includes courses in digital forensics, cybersecurity, legal evidence, and network security, among others. Most of these courses can also be accessed individually for professional development (BCIT, n.d.). By comparison, Toronto Metropolitan University's Cybersecurity, Data Protection and Digital Forensics certificate comprises six required courses (in network security and digital forensics investigation, among others) and it can be completed in a year (TMU, 2022). Overall, opportunities exist for Canada's higher education sector to develop and provide specialized training through diplomas, degrees, or single courses tailored to law enforcement employees.

Not all policing agencies, however, are able to send officers to post-secondary institutions; even when they can, the lack of standardization can lead to gaps in some of the material taught (Stigall & Choo, 2021). Currently, there is insufficient training available in specific areas, including Canada-specific cyber legalities, cryptocurrency, cybercrime prevention, victim assistance, and digital and network forensics (Beesley, 2021). Standardization is not a trivial exercise, however, and past efforts to align cyber-related training internationally (e.g., via the International Organization on Computer Evidence) have not been successful (Dupont, 2021).

There are opportunities for the private sector to play a greater role in handling digital evidence and supporting training

Some law enforcement agencies have determined that their internal training capabilities are insufficient for providing training in specialized digital skills. In the United Kingdom, for example, His Majesty's Inspectorate of Constabulary has noted that the College of Policing cannot provide sophisticated specialist training; therefore, these skills need to be provided through relationships with external partners (HMIC, 2015). The Constabulary notes several benefits of using third-party training providers, including not needing to maintain training infrastructure, reducing costs of developing programs, and allowing law enforcement to "benefit from the private sector's knowledge base" (HMIC, 2015).

Another U.K. proposal, which would similarly see the public sector learning from the private sector, would have law enforcement officers enter into secondments, in order to transfer knowledge between the police and the private sector (Hitchcock *et al.*, 2017). Under this model, specialized police officers (or other police employees) could be sent to work in technology companies for a few months, in order to gain new digital skills. There is, however, a risk that some

technology companies may shy away from these secondments (and relationships). Furthermore, increasing public-private collaboration on security and surveillance issues demands strict reporting requirements, risk assessment, and frequent evaluations of any relationship, so as to ensure that privacy is protected.

Beyond training, the Panel believes opportunities exist for law enforcement to collaborate with the private sector in carrying out specific tasks that require highly specialized equipment and skills. Such partnerships could take advantage of the important role the private sector already plays in digital security. For example, private sector organizations might be contracted to trace and seize cryptocurrency or carry out network forensics. Taking advantage of the private sector capacity to carry out these time-intensive tasks could free up police time and resources. Such partnerships would need to be implemented carefully, in order to preserve the independence and integrity of police investigations and potential criminal prosecutions.

Training all officers in general digital knowledge would improve the ability of law enforcement to investigate cybercrime

Training wider staff in general digital knowledge does not seek to make all officers tech experts. Rather, it teaches them new digital skills that support a range of police work since "digital information can enrich [...] criminal investigations" (Leukfeldt *et al.*, 2013). Further, it may help officers with little cyber experience overcome their hesitancy with handling cyber cases. Using online training platforms can make such training available to all officers at a limited cost (Dupont, 2021).

This type of training is being used in Canada and elsewhere (Dupont, 2021). In France, the training curriculum for the national gendarmerie has been updated to reflect the growing importance of digital skills, with the introduction of a pilot program that substantially increases the digital elements in basic training (Hours, 2022). The gendarmerie explains that the course is not intended to train specialists but rather to integrate more digital knowledge and understanding across all departments. Similarly, in Switzerland, l'Institut Suisse de Police has developed E-CC (e-learning cybercrime) training to quickly disseminate introductory training to the 20,000 police officers in the country. The training is available in all three of Switzerland's official languages, and is also accessible to some civil employees (Brugoni, 2018).

In Canada, the Canadian Police Knowledge Network (CPKN)'s Cybercrime Training and Digital Competency Development for Canadian Law Enforcement project strives to provide this type of training to all officers (CPKN, 2021). The project began by identifying 10 digital competencies related to digital evidence,

cybercrime, and cyber-enabled crime, as well as the different roles people hold in law enforcement (e.g., first responder, cybercrime analyst) (Beesley, 2021). A matrix was then developed that considered the competency level needed for people in different roles. For instance, first responders require low competency levels in cryptocurrency and blockchain, while cybercrime analysts require high levels of competency.

Following the development of this competency matrix, an analysis found there were substantial gaps related to the training for generalist law enforcement roles (Beesley, 2021). Focus groups made of "industry and policing anti-cybercrime practitioners and experts from across Canada" had broad consensus that additional cybercrime training was needed and that this training was "required at all levels, from basic to advanced" (Beesley, 2021). CPKN is in the process of working with experts to develop a generalist training program, in both official languages, for frontline workers (CPKN, 2021).

Creating new training programs or courses takes time, and it can be difficult to keep up with evolving technologies. As with training focused on specialized skills, there are opportunities to partner with the private sector or academic institutions to develop and instruct courses in the basic digital skills relevant for all officers in law enforcement. Even when training is available, however, it may not be used to its full potential. Several online courses relevant to cybercrime are available in CPKN's course catalogue,[18] but registration is not mandatory, and it is up to individual forces or officers to decide whether to take them (Dupont, 2021). Furthermore, most courses are not free (although they are low-cost), and many are only available in English (CPKN, 2022). The result is that, while Canada has a promising method of training officers, this training is not taken up by, or available to, all officers who would benefit from it.

Coordination bodies can support the allocation of resources and avoid duplication of efforts

Recognizing that resources are limited, several countries have set up coordinating bodies that facilitate the pooling of resources and try to avoid the duplication of efforts. These bodies can also support collaboration with international law enforcement — something that is particularly important given that online crime often crosses state borders. The Budapest Convention (Box 5.4) provides a framework to support international coordination efforts.

The exact structure and mandate of coordinating bodies vary by jurisdiction. One example is the National Cyber Crime Network in the United Kingdom, first

18 The CPKN course catalogue hosts short courses developed by other content providers, such as city police services, the RCMP, and not-for-profits (CPKN, 2022).

established in response to the *National Cyber Security Strategy 2016 to 2021* (Gov. of UK, 2021c). The network includes several units, each with its own role. The National Crime Agency's National Cyber Crime Unit provides leadership and coordination, while regional and local cybercrime units are responsible for the investigation of offences and helping local communities protect themselves from cybercrime. Action Fraud (housed by the City of London Police) is responsible for carrying out analysis and triage based on centralized crime reporting. Crimes deemed particularly serious or complex are referred to the National Crime Agency or regional networks, while all other cases are given to local forces (Gov. of UK, 2021c). Beyond avoiding duplication of effort, a centralized coordination body may ensure that the most serious crimes are investigated by teams with the greatest capacity, thus freeing up others to investigate other cybercrimes.

In Canada, the National Cybercrime Coordination Unit (NC3) has played a coordination role since it reached operating capability in April 2020 (RCMP, 2021d). The unit, staffed by both RCMP and civilians, is expected to reach full capability in 2024 (RCMP, 2021d). The NC3 is a three-part system operated by the RCMP (2020c) with the goal of "reduc[ing] the threat, impact and victimization of cybercrime in Canada" (RCMP, 2021d). The NC3 is expected to include a Public Reporting Website, which will allow individuals and businesses to report malware, hacking, cyber-fraud, identity theft, forgery, and extortion, among other forms of cybercrime (RCMP, 2020c). From there, reports are collected by the NC3 Internal Solution, a centralized data repository where new reports are analyzed and compared against its database to identify potentially related cybercrime reports, incidents, and ongoing investigations. The goal of this step is to connect cybercrime investigators across all jurisdictions, and provide the tools and support to collect, analyze, and share data and information via the Police and Partner Portal. Because of the potentially sensitive nature of the data contained in the NC3 Internal Solution database, access is carefully controlled and provided selectively to authorized law enforcement and security partners (RCMP, 2020c).

The NC3 has already had some success. Along with other Canadian partners, it worked with Europol on Operation GoldDust (City of Calgary, 2021). This operation targeted the REvil ransomware family that sold malware to customers, who would then use it to carry out attacks to encrypt or steal data, then extort payment in return for those data. Investigators estimated that approximately 600 infections (out of 7,000 worldwide) using this malware happened in Canada. The Canadian investigation identified infrastructure in Canada, as well as infrastructure and suspects in many countries in both Europe and Asia. The prosecution of suspects is being carried out in the United States and countries in the European Union (City of Calgary, 2021).

6.3 Criminal Investigations

6.3.1 Access to Digital Evidence

Digital evidence is often a critical part of police investigations

Digital communication of some type is used as a tool in most criminal activity. As a result, digital information is often an integral part of the evidence needed to investigate and prosecute crime. This means that law enforcement needs to be able to work with evidence from digital spaces in order to operate most effectively. There have been some modifications to legal frameworks in recognition of the growing importance of digital evidence, chiefly the *Protecting Canadians from Online Crime Act*, which introduced specialized investigative tools that could be used to obtain digital evidence as well as sanctions for service providers that do not comply (GC, 2014). Tools include changes to the rules around search warrants and production orders as they relate to digital evidence, as well as the introduction of preservation demands to prevent the deletion of electronic evidence. The Department of Justice has noted that, "while it was expected that numerous *Charter* challenges would arise from the new investigative powers, this has not yet proved to be the case" (JUS, 2020). Beyond the existence of warrants and production orders, there is limited guidance for law enforcement on the tools it can use to access data in the course of an investigation; this opens the door to privacy violations, if tools are applied inappropriately (Section 6.3.5).

Law enforcement requires warrants to access basic subscriber information (BSI)

Access to BSI — which can include a subscriber's name, IP address, physical address, telephone number, and email address — by law enforcement continues to be an issue of discussion in Canada. In *R. v. Spencer*, the Supreme Court of Canada found that BSI cannot be obtained without prior judicial approval when there are no "exigent circumstances" (SCC, 2014b), and that the *Personal Information Protection and Electronic Documents Act* (PIPEDA) did not provide law enforcement with lawful authority to compel this information from information custodians. In short, law enforcement agencies cannot request BSI data from a service provider because obtaining information that enables authorities to draw a link between a person's identity and their online activities constitutes a constitutionally protected search. Before this ruling in 2014, police would routinely request and obtain BSI directly from service providers (JUS, 2020).

As there are no specific laws designed to provide access to BSI, current practice often uses a general production order, which is applicable for any type of information (NLCA, 2019; JUS, 2020). Of note, in *R. v. Bykovets*, the Court of Appeal of Alberta held that police could legally obtain an IP address without judicial

authorization, as "an IP address does not tell police where the IP address is being used or, for that matter, who is using it. Nor is there a publicly available resource from which the police can learn this or other subscriber data" (ABCA, 2022).[19] In that case, police later used a production order to secure the name and address of the subscriber associated with the IP address.

Since *R. v. Spencer,* there have been some efforts to create mechanisms that would enable law enforcement to access BSI without a warrant, often using a perceived need for baseline identifiers or the investigation of child sexual abuse material (CSAM) as rationale (Parsons, 2022). These discussions often, however, shift to enabling access to BSI for all investigations or even non-criminal events (Parsons, 2022).

Existing mechanisms for accessing data housed outside Canada are seen by law enforcement as slow and cumbersome

Even when a court order has been obtained, it can be challenging to access data that may be criminal evidence (e.g., usernames, IP addresses) from service providers (Carter & Daskal, 2018). For example, identifying which service providers have access to, or outright possess, the relevant sought-out digital evidence (Carter & Daskal, 2018). The process of accessing information can be onerous even when the appropriate data custodian is identified. Interview-based studies reveal frustration among Canadian sex crime investigators, who noted that legal procedures that "were once very short to access someone's home now take multiple days… to access something like an IP address" (Dodge *et al.*, 2019). Participants in the study also described lengthy and laborious international warrant processes when seeking access to information from companies located outside Canada, such as Meta.

If data are housed outside Canada, the *Mutual Legal Assistance in Criminal Matters Act* (MLACMA) provides the Department of Justice with the legal authority to request court orders in countries that have a mutual legal assistance agreement (MLA) with Canada (GC, 2019d; JUS, 2020). In the 2017–2018 fiscal year, there were 114 outgoing MLA requests seeking digital evidence, down from 128 the year before. This is substantially lower than the number of incoming requests the Department of Justice receives seeking digital evidence housed in Canada (448 in 2017–2018) (JUS, 2020). An evaluation of the Investigative Powers for the 21st Century Initiative (IP21C) noted that "several representatives of Canadian law enforcement stated that they will avoid the lengthy MLA process if at all possible" (JUS, 2020). Parsons (2016) notes, however, that, "while the timeliness of accessing information through [Mutual Legal Assistance Treaties (MLATs)] is an issue for Canadian authorities, it isn't a problem that a new Canadian law can fix.

[19] This decision has been appealed to the Supreme Court of Canada (SCC, 2022).

Instead, fixing the MLAT process will require additional resourcing in the receiving country to accelerate the process of reviewing the foreign warrant."

The MLAT-related challenges facing Canadian law enforcement agencies may be lessened in the coming years. Canada and the United States have begun negotiations under the U.S. CLOUD Act (Section 5.2.5), which would enable Canadian authorities to serve judicial orders directly to American providers for information they hold about Canadian residents suspected of a crime (DOJ, 2022b). If these negotiations are successful and appropriate processes are implemented, the time and effort it takes to obtain information from American companies would be substantially reduced, though this would not ameliorate MLAT-related challenges where information is held outside Canada and the United States.

6.3.2 Encryption

Law enforcement has cited encryption as a challenge for investigating criminal activities

Encryption is "the process of encoding information so that it can only be understood by its intended recipient" (Masoodi & Rand, 2021). It is essential for national security, and for protecting human rights and public safety (Gill *et al.*, 2018). Encryption is used as a secure method for sending and storing different types of data, which ensures their "confidentiality, integrity, and authenticity" (Masoodi & Rand, 2021) and protects internet users from criminal threats. Encryption can be applied to data stored in a specific device or system (i.e., data at rest), or to data transmitted among applications or via the internet (i.e., data in transit), which are often harder to decrypt (Parsons, 2019). Many messaging applications, such as WhatsApp and Signal, are increasingly implementing end-to-end encryption, whereby "only the sender and the intended recipient can view the contents of the message in plaintext" (Masoodi & Rand, 2021). Encryption applications play important roles in protecting personal data, privacy (Chapter 2), intellectual property, and cybersecurity (CACP, 2016; PS, 2020). It also "enables the exercise of fundamental rights and freedoms, including freedom of thought, belief, opinion, expression, and association" (Parsons, 2019).

Devices and applications routinely integrate encryption into their regular operation. While this may protect individuals, it can also limit the information law enforcement agencies can access, even after obtaining judicial authorization to access digital evidence. Law enforcement agencies have identified encryption as a challenge in investigating cybercrime and collecting digital evidence; the Canadian Association of Chiefs of Police having previously highlighted encryption as a significant investigative challenge, even when lawful judicial authorizations are obtained (CACP, 2016). Challenges related to encryption have, in particular,

been identified in investigations of online child sexual exploitation and abuse, cyber-fraud, organized crime, and extremism (CACP, 2016; PS, 2017b). Echoing this perspective, the Government of Canada issued a joint statement with the Five Eyes highlighting the challenges related to encryption (Section 5.3).

In the evaluation of IP21C, a federal prosecutor stated that the number of authorized wiretaps has "declined dramatically over the past few years due to encryption," and noted that this has led police to "revert to other means of uncovering information" (e.g., undercover officers) (JUS, 2020); none of this information, however, has been stated in any provincial or federal government report on the use of wiretaps in Canada (Parsons & Molnar, 2018). Other reasons for the decline in wiretaps may include the use of digital tools (e.g., hacking, on device investigation tools or ODITs). Of note, ODITs[20] have been used by law enforcement in Canada but not included in wiretap reports, despite the fact that wiretap orders are used to deploy them (ETHI, 2022; Forrest, 2022; RCMP, 2022a).

The Dark Web creates unique challenges for law enforcement

The increasing use of encryption technology across digital systems and products has also led to the creation and propagation of illicit online marketplaces, anonymous online networks, and communications and sales infrastructures operating on the Dark Web (Lukings & Lashkari, 2022b) (Section 4.2). The anonymized environment makes it difficult to tie criminal activities on the Dark Web to specific groups or individuals, since law enforcement often cannot identify or trace digital evidence within that space. While Canadian law enforcement agencies attempt to monitor Dark Web content and activity, software that can "adequately detect and monitor illegal access, communications, activities, and encrypted content transmitted over the Dark Web" is currently unavailable (Lukings & Lashkari, 2022b).

There are some tools that monitor the Dark Web for specific types of illegal material. For example, Project Arachnid (Box 6.1) scans forums on the Dark Web, and take-down notices can be issued in cases where Dark Web postings are linked to files hosted on the Open Web (C3P, 2021). A range of automatic scraping tools that monitor the Dark Web for data are available (AlKhatib & Basheer, 2019); these tools are used by individuals to determine whether their personal data have been compromised, but also by private sector companies to identify whether their data (which may include information on customers or users) have been breached.

20 ODITs are computer programs installed on a device, such as a smartphone, without the owner's knowledge, in order to allow law enforcement to collect digital evidence (RCMP, 2022b).

Challenges related to accessing encrypted data are not solely technical

While encryption has been referenced by law enforcement as an investigative barrier, the degree to which it disrupts or delays investigations is not entirely clear. Federal and provincial reports on electronic surveillance in Canada do not mention encryption-related barriers to intercepting communications (Parsons & Molnar, 2018). While encryption slows down some criminal investigations, it does not necessarily inhibit them, and law enforcement agencies have other means of accessing evidence that do not require de-encryption (e.g., getting production orders to access cloud backups) (Parsons, 2019; West & Forcese, 2020; Masoodi & Rand, 2021).

There have been cases where encryption was identified as a problem by the RCMP, but, upon analysis, the stated issues did not appear to be insurmountable (Parsons, 2016); the key challenges identified by the RCMP were related to factors beyond encryption itself. These include delays in collecting evidence, equipment malfunction or misuse, failure to use other available data collection tools, and lack of cooperation from internet and telecommunications service providers (CACP, 2016; Parsons, 2016; Powell & Henry, 2018). Furthermore, law enforcement agencies note they lack the technological tools and expertise to overcome encryption (Boutilier, 2016; Masoodi & Rand, 2021), indicating this may be a resource and personnel issue as much as a solely technical one.

Backdoor or frontdoor access points on encrypted devices provide access for law enforcement, but build in vulnerabilities

Specific design features may overcome technical barriers related to encryption. Like wiretapping in phone systems, devices could be designed to give law enforcement agencies backdoor access to these data, in limited circumstances. This approach has precedence. Many email providers encrypt messages but retain a key to the communications housed on their servers (Finklea, 2021). In 2010, the RCMP obtained a decryption key for consumer-grade BlackBerry devices. This key let investigators decipher more than a million communications among members of a mafia organization (Ling & Pearson, 2016; Pearson & Ling, 2016). There are concerns, however, that any sort of backdoor entry point would inevitably be exploited by malicious actors (Dheri & Cobey, 2019; Dupont, 2021). Backdoor access points reduce the structural integrity of digital systems and build in vulnerabilities. As Dheri and Cobey (2019) explain, "backdoors cannot be installed to make criminal communications vulnerable without, at the same time, making government and individual communications susceptible to criminal, terrorist, or foreign hacking."

Some law enforcement officials argue that the term *backdoor access* sounds secretive and would prefer the term *frontdoor access*, where there is a "clear understanding of when they are accessing a device" (Finklea, 2021). Such access would be provided by the key-holder (or key-holders for a multipart encryption key) in cases where investigators have demonstrated they have a lawful basis for accessing the material (Nakashima & Gellman, 2015; Finklea, 2021). This approach faces the same fundamental challenge of building potential entry-point vulnerabilities into the system.

In the absence of backdoor entry points, law enforcement agencies in Canada require clear guidance on what they can do to overcome encryption. Dheri and Cobey (2019) suggest law enforcement agencies may develop their own tools to hack software, in order to overcome encryption, but there is ambiguity about when these tools can be applied. Some scholars have raised questions about how such hacking might be lawfully applied by law enforcement agencies. Bellovin *et al.* (2014) argue that lawful hacking should be done using existing vulnerabilities, and that such vulnerabilities be reported on discovery or purchase to the vendor, potentially leading to an increase in overall security. Parsons (2014), noting a dichotomy in the context of govware (i.e., malware "designed for, or purchased by, government agencies"), explains:

> *Getting into the hacking business means that the Government of Canada is put at odds with itself: on the one hand, government has established organizations to better secure critical governmental and commercial digital infrastructure and, on the other, govware would be instrumentally more useful if there were no ways for targeted individuals to detect or block its presence or activities.*

Beyond this, data breaches at companies that make lawful hacking tools have occurred, which demonstrates that these tools are being sold to governments engaging in serious human rights violations. In 2015, for example, Hacking Team, a developer of technology marketed to governments and law enforcement based in Milan, reported that nearly 400 GB of its internal data, including client files and financial data, were leaked by hackers (Singh, 2015). These data showed that Hacking Team had sold its software to several countries that repress human rights, including Ethiopia, Kazakhstan, Republic of Sudan, Saudi Arabia, and others. These hacking tools may be used for activities that are technically considered legal within these countries, but which would be considered illegal when viewed through the lens of Canadian or international laws. Furthermore, the Canadian Centre for Cyber Security (2022a) notes that "foreign governments have almost certainly used these commercial tools against Canadians and groups of interest inside Canada."

There are also concerns about how these tools are being used by governments in democratic countries. An investigation by the Citizen Lab, in collaboration with civil society groups, found that at least 65 people in Catalonia were targeted by, or infected with, spyware from the NSO Group (Pegasus) or Candiru (Scott-Railton *et al.*, 2022). Both of these are mercenary surveillance companies that sell their spyware to government clients. People affected included activists, academics, and elected officials and members of Catalonia's government, as well as individuals located in other E.U. countries and Switzerland. The investigation did not conclusively attribute the attacks to "a specific government," but noted that "extensive circumstantial evidence points to the Spanish government" (Scott-Railton *et al.*, 2022). It also noted that the spyware was active when Catalan officials and the Spanish government were in negotiations around the autonomy of Catalonia.

6.3.3 Processing and Sharing Digital Evidence

Automation can improve the efficiency of digital forensics

As noted in Section 6.2.1, staffing constraints create a bottleneck in the processing of digital evidence. These constraints are compounded by inefficient processes whereby forensic examiners are spending time carrying out repetitive and mundane tasks. When digital devices are examined on a "one-to-one basis," a single digital forensic examiner needs to run each digital device through all investigative steps on a single workstation (Saliba, 2021). As explained by Jad Saliba (2021), founder and chief technology officer of Magnet Forensics, "many of [the required] tasks are basic and don't involve much more than connecting a device or clicking through prompts." Therefore, there may be an opportunity to use automation to carry out the mundane and repetitive tasks so that forensic examiners can focus their time on data analysis and providing extracted data to investigators.

The use of automation may also open the door to simultaneously processing data for multiple devices at once, and aid in the standardization of workflow. Police forces have recognized a need for increasing automation. For example, the technology lead for the Police Federation of England and Wales has noted "a need for forces to invest in technology which can help speed up this process by extracting and sorting [data from digital devices] automatically" (ITV News, 2020). Ultimately, automation could increase throughput, reduce the time needed to process a digital device, and ensure consistency. The Panel notes that any digital forensics system, as well as its automated processes, needs to be accessible to defence attorneys for evaluation, in order to ensure that criminal defendants are given a fulsome opportunity to mount their defences.

Tools that make digital evidence more accessible within law enforcement could speed up investigations

There are delays related to digital evidence even after data from a device have been extracted. Currently, it is difficult for non-technical investigators to access any data extracted from digital devices. This means that, in many cases, the officers who have the most intimate knowledge of an investigation are provided only with static reports (once forensic examiners have had the time to prepare them), unless they engage in time-consuming methods to access the data (e.g., drive to forensic examiner site, learn how to use complex software used by forensic examiners) or obtain the data through vulnerable methods (e.g., sharing USBs). This problem could be eased by a simplified evidence review system that allows officers to securely log in and review case evidence themselves. These systems would need to be accompanied by processes that enable independent oversight, ensure evidentiary chains of custody are preserved, and ensure officers cannot accidentally or intentionally modify forensically derived information. Effective accessible evidence systems would help remove some of the bottlenecks involved in moving case data through the judicial system.

6.3.4 Digital Detection and Reporting

Digital detection tools can be used to detect online CSAM

Automated multi-modal detection tools can be used to detect CSAM by monitoring online images and file names, and by assessing multiple variables. For example, a perceptual hashing algorithm for image matching can be applied to CSAM, as is done with Microsoft's PhotoDNA, which is used to compare publicly available images against those held in the National Center for Missing and Exploited Children (NCMEC) database (Westlake *et al.*, 2012; Edwards *et al.*, 2021). This strategy improves efficiency insofar as it is faster than relying on individual officers to visually analyze images (Edwards *et al.*, 2021). Some automated programs "crawl" across multiple websites by following related links once activated on a known CSAM site (Edwards *et al.*, 2021). This process identifies the volume of CSAM while also assisting law enforcement in following a path of distribution, with the end goal of taking down a central site and preventing future access and distribution among users (Westlake *et al.*, 2012; Edwards *et al.*, 2021). A popular example of this tool is Project Arachnid, which has had a dramatic impact on the capacity of investigators to detect and address CSAM images (Box 6.1). Importantly, automated cyber-detection strategies may be especially useful to the health of investigators themselves, as they are at an increased risk of secondary traumatic stress due to repeated viewing of harmful images on the job (Burns *et al.*, 2008).

There are some limitations to crawlers, including the time and resources needed to train officers in their application and the selection of the most effective keywords, which allows crawlers to produce the best results (Edwards *et al.*, 2021). Furthermore, effective safeguards and ongoing oversight mechanisms for crawlers are needed to ensure they are not used to access data that are subsequently processed for purposes unrelated to CSAM.

Box 6.1 Project Arachnid

Launched in 2017 by the Canadian Centre for Child Protection (C3P), Project Arachnid is an automated tool that scans the Open Web and Dark Web for CSAM or other harmful and abusive material relating to children (C3P, 2021). The system can detect tens of thousands of images per second. Once an illegal image has been detected, the system issues take-down notices to sites hosting the content (C3P, 2021). C3P works in collaboration with global partners, including international NGOs and tip-lines for reporting CSAM. The collaboration reduces duplication and increases the unique number of take-down notices for CSAM (C3P, 2017).

Project Arachnid was designed as a victim-centric model, in that it is intended to facilitate early detection and take-down. This lessens the chances of victims and survivors coming across material or having that material distributed or replicated across websites (C3P, 2017). In addition to dealing with the images in real time, Project Arachnid collects data that can be used by the international community in assessing the extent of online exploitation of children, as well as potential ways to address the harms (C3P, 2017). As of 2021, Project Arachnid has detected and verified 5.4 million images and sent take-down notices to 760 service providers globally at the rate of approximately 3,500 removal notices issued daily (C3P, 2021).

Online reporting is used in Canada to detect CSAM

Internet service providers in Canada are required to report sites that host CSAM to Cybertip.ca (GC, 2011b; Cybertip.ca, n.d.); individuals are also encouraged to report potential harmful or illegal acts to the tip-line. Cybertip.ca is meant to be an easy and anonymous way to report suspicious or concerning behaviour. It accepts reports about CSAM, luring a child, non-consensual distribution of intimate images, making sexually explicit material available to a child, arranging with another person to commit a sexual offence against a child, commercial sexual exploitation of children, trafficking of children, and travelling to sexually exploit

a child (Cybertip.ca, 2022b). Reports can be made by anyone, but the harmful behaviour must be targeted toward children or youth under the age of 18. The *Child and Family Services Act* of Manitoba mandates the reporting of "child pornography" to C3P, which operates Cybertip.ca (Gov. of MB, 2014, 2022). Nova Scotia also mandates the reporting of CSAM but, in that province, the reporting entity is any law enforcement agency (Gov. of NS, 2008).

Cybertip.ca was piloted in 2002 (C3P, 2017) and officially adopted in 2004 as part of the *National Strategy for the Protection of Children from Sexual Exploitation on the Internet*. Upon receipt of reports, Cybertip.ca assesses and triages its information to aid law enforcement agencies in determining criminality and jurisdiction (C3P, 2017). It is operated by C3P and supported by the Canadian Association of Chiefs of Police, the RCMP, and the Criminal Intelligence Service of Canada; as part of C3P, it has signed protocols with 28 law enforcement services across Canada to provide resources to the public (Cybertip.ca, 2022c). The tip-line's goals and strategy have evolved since its inception, largely due to the new utilities offered by Project Arachnid. As of 2021, Cybertip.ca's public reporting initiative (excluding Project Arachnid) has processed over 360,000 reports. Of these, over 23,300 were forwarded to law enforcement agencies, over 1,000 were forwarded to child welfare agencies, and over 127,300 were "actioned internationally" (Cybertip.ca, 2022d).

Cybertip.ca, along with its C3P partner sites, also provides resources to help victims get pictures or videos of themselves removed from the internet. Resources include letter templates and contact information for popular social media platforms (NeedHelpNow.ca, 2022). For instance, NeedHelpNow.ca offers advice on getting sensitive content removed from online services, contacting perpetrators, contacting law enforcement (e.g., when and how), finding legal guidance, and helping victims and survivors find the support they need. Cybertip.ca only provides services to victims and survivors under the age of 18, but much of the advice and resources provided by Cybertip.ca and NeedHelpNow.ca can be helpful to anyone concerned about the non-consensual distribution of intimate images. There appears to be no formal reporting service comparable to Cybertip.ca for adults in Canada.

Online reporting has been used in other jurisdictions to support adult victims and survivors of online, image-based abuse

Portals such as Cybertip.ca exist globally and are often connected through INHOPE, an international organization consisting of approximately 50 hotlines or tip-lines spanning across 40 countries and dedicated to the reporting and removal of CSAM (INHOPE, 2020). It provides educational material as well as advanced tools to help member countries' hotlines efficiently share reported cases, escalate new cases, and reduce the number of duplicate investigations (INHOPE, 2020).

In some cases, the associated hotlines are equipped to deal with all levels of harmful intimate imagery, while others focus exclusively on CSAM (INHOPE, 2020).

The Government of Australia offers something comparable to Cybertip.ca through its eSafety portal, esafety.gov.au. This website is intended to provide information, resources, and reporting tools to help the Australian public have safer experiences online (Yar & Drew, 2019; eSafety Commissioner, 2021b). While 73% of reported cases of image-based abuse between 2020 and 2021 targeted adults, eSafety noted it did not have formal powers to investigate adult cyber-abuse cases (eSafety Commissioner, 2021b). However, in January 2022, new online safety laws came into effect that expanded its ability to help adults subjected to online harm (eSafety Commissioner, 2022a).

Triggering an eSafety investigation requires that the report meet a certain content threshold (e.g., includes real or fake intimate imagery) and was made by the person shown in the intimate image, or their parent or guardian (in the case of a minor), or by another person authorized to report on their behalf (Yar & Drew, 2019; eSafety Commissioner, 2022b). If these criteria are met, the regulator has the power to initiate the removal of intimate images, level fines and penalties, or undertake other regulatory actions against the person responsible. In 2021, eSafety was able to have 90% of image-based abusive material removed upon request (eSafety Commissioner, 2021b). Despite the successes of Australia's approach, large American technology firms such as Meta, Google, and Apple (represented by the industry group DIGI) believe Australia's online safety laws are inconsistent, confusing, and difficult to conform to; as such, these companies have requested that any new laws be streamlined into a single legislative act (Brookes, 2022).

6.3.5 Artificial Intelligence (AI)

Applications that use AI have potential benefits for law enforcement, but they also have unique ethical and privacy considerations

While the definition of *AI* remains in flux, the term is used in this report to describe machine-assisted applications, including those based on machine learning, deep learning, and reinforcement learning (CCA, 2022). Advancements in hardware and software, the availability of huge amounts of data, and a growing industry focus on AI have led to the creation of applications across a range of fields, including decision-making and law enforcement. Looking ahead, it is likely that "few fields will remain untouched by AI" (CCA, 2022).

While many AI applications have potential uses in law enforcement contexts — such as helping to locate suspects or victims, or detecting crimes such as fraud — there are widespread concerns related to their use, and a lack of guidance about when a particular tool is appropriate. Foremost, there are concerns that privacy is being

violated during the collection of data from sources an AI is trained on or applied to; it has been noted that many big datasets and their associated AI algorithms are based on non-consensual data collections or analyses (Leslie, 2020). AI applications also have the potential to perpetuate, or even amplify, discrimination and biases inherent in the datasets used to train them (Barocas & Selbst, 2016). This is a considerable risk in the context of law enforcement because of the history of systemic racism in Canada's policing systems (SECU, 2021). There are also risks that AI applications will suffer from the so-called "black-box problem," where it is difficult or, in some cases, impossible to ask machine learning and AI algorithms to show their work (Section 2.1.2); it raises fundamental problems for the administration of justice when black boxes prevent a defendant from mounting a fulsome defence, or when individuals have negative interactions with law enforcement agencies due to "mathwashed" bias in the algorithms (Robertson *et al.*, 2020). Because of these risks, transparency, independent evaluation and monitoring of ethical issues, and data inputs used for AI in law enforcement are important (Section 6.3.6). As a CCA (2022) report notes, in the context of science and engineering research, "risks emerge because there are gaps between the principles for the responsible development of AI and their operationalization, as well as a paucity of stronger regulatory measures overall."

AI and cross-case analytics can be leveraged to support the identification and sharing of data

There are opportunities to use AI applications to speed up the analysis of digital evidence and ease the burden placed on officers and staff carrying out digital forensics (Rigano, 2019). AI can be used to identify relevant data that provide starting points for investigators. In this way, digital approaches, including AI systems, can uncover the evidence relevant to a case faster than a manual approach (Novak *et al.*, 2019; Shute *et al.*, 2021). For example, one technology company notes AI can be used to scan text messages for certain phrases or themes rather than reading every message entirely, and can show how certain artefacts connect to one another (Police1 BrandFocus Staff, 2018).

Appropriate testing and oversight of such tools is important, however, as analyses of some automated forensic tools reveal biases, which could lead to certain communities being over-policed based on historical encounters with law enforcement (Koepke *et al.*, 2020).

AI could be used to support cross-case analytics across law enforcement agencies, something that is particularly important for cyber-enabled crime, where evidence (and perpetrators and victims) can be cross-jurisdictional. The Panel notes that such systems would need to be designed to interoperate without revealing case details to different agencies, absent memorandums of understanding and specific authorization to access information linked to criminal proceedings.

Law enforcement has used FRT to aid investigations

Computer-enabled FRT is a type of biometric identification, which depends on images such as passport photos and mugshots (OPC, 2011; Crumpler & Lewis, 2021). FRT takes an image of a person's face and translates it into data that can be compared quantitatively against other facial data (EFF, 2017; Crumpler & Lewis, 2021). Many facial recognition algorithms rely on measuring the size and shape and relative placement of facial features, which are then compared to others on a one-to-one basis (i.e., comparing two images to determine whether they are of the same person) or a one-to-many basis (i.e., finding a match within a database) (Crumpler & Lewis, 2021). Access to high-performance computing, parallel-processing techniques, and cloud-based platforms has accelerated research and overcome the challenges of object identification and extrapolation due to different lighting, image angles, and changing facial expressions.

Currently, FRT data are less accurate than other forms of biometric data, but the technology is contactless (unlike fingerprint scanning) and can rely on lower-resolution or poor-quality imaging (compared to iris scanning). The result is that FRT can be used to identify individuals in public spaces and in automated image tagging (Robertson, 2021), often in ways that are not apparent to those subjected to the surveillance. Whereas someone likely knows when their fingerprints are being scanned, the same is not true of optical surveillance. To date, governments and law enforcement agencies have used FRT for a range of applications, including identity verification at international borders, verifying government service eligibility, and generating leads to help find wanted individuals (e.g., Braga, 2017; Robertson *et al.*, 2020; Rakheja, 2021).

The use of FRT by law enforcement has led to privacy violations in Canada

As facial recognition algorithms improve and databases expand, the ability to identify any person on the street and see their arrest history, social media presence, and any number of personal details — in real time and with just a photograph — is becoming possible (Klosowski, 2020). While technical experts work to enhance the functionality of FRT systems, some legal and ethical experts have warned that, even in its current form, FRT actively threatens the public's right to privacy by employing widespread public surveillance in ways unique to specific realizations of facial recognition algorithms (EFF, 2017; Robertson *et al.*, 2020).

FRT can, in some cases, connect traditional mugshot practices and algorithmic policing; available mugshots are often used to build a database of facial images to be analyzed (Robertson *et al.*, 2020; Hao, 2021). According to Canada's *Identification of Criminals Act*, mugshots can be collected without consent when an individual

has been charged, convicted, or alleged to have committed an indictable offence (GC, 1985). Those found innocent or for whom charges have been dropped have the right to have these data destroyed (in some cases, this is only done by request) (Robertson *et al.*, 2020). Mugshots are not the only items that facial recognition software can use to build image databases, however. Clearview AI, for example, has harvested over 10 billion facial images "from public-only web sources, including news media, mugshot websites, public social media, and many other open sources" (Clearview AI, 2021). In June 2021, the Office of the Privacy Commissioner (OPC) ruled that the RCMP's use of Clearview AI violated Canada's privacy laws because the company built its databank using images scraped off the internet without consent. The OPC found that "the onus was on the RCMP to ensure the database it was using was compiled legally," while the RCMP maintained this would be an "unreasonable obligation and [...] the law does not expressly impose a duty to confirm the legal basis for the collection of personal information by its private sector partners" (OPC, 2021c).

In July 2020, Clearview AI announced it would voluntary withdraw its facial recognition services in Canada in response to privacy investigations across the country (Daigle, 2020), stating that it was "prepared to consider maintaining this status for a further two years, in order to allow the various Commissioners to provide detailed and meaningful guidelines as to how Canadian law proposes to deal with artificial intelligence" (OPC, 2021d). Following a joint investigation with the OPC, the privacy protection authorities of three provinces (British Columbia, Alberta, and Quebec) concluded that Clearview AI was in violation of privacy legislation (including PIPEDA) and recommended the company cease collecting and using images of people without their consent, and delete all images and biometrical facial arrays that had been collected without consent (OPC, 2021d).[21]

Similar decisions have been made elsewhere. In the United Kingdom, the Information Commissioner's Office ordered Clearview AI to stop collecting or using data related to U.K. residents, and to delete existing data from its system, following a joint investigation between its own office and the Office of the Australian Information Commissioner (ICO, 2022). That bilateral investigation found that Clearview AI violated the privacy of citizens in both the United Kingdom and Australia (OAIC, 2021; ICO, 2022). These cases demonstrate the questionable legality and ethics associated with the creation of Clearview AI's facial recognition systems, which have been used by policing bodies in Canada and peer countries.

These ethical issues, along with the technical collection of facial databases, are made more complicated still due to the black-box problem. When an FRT system

21 Clearview AI Inc. has indicated it will appeal these decisions (Hill, 2021; Lyons, 2021).

generates a match, it is often not clear whether biases in the analyzed data, training data (in machine learning contexts), or algorithm operation have been properly considered and accounted for (Buolamwini & Gebru, 2018). Facial recognition has been shown to be particularly problematic when it comes to identifying people with darker skin tones, and it identifies gender based on outdated stereotypes (Buolamwini & Gebru, 2018; Simonite, 2018; NSF, 2019). This leads to falsely identifying suspects in one-to-many analyses, poor results in one-to-one image comparisons, and the misgendering of subjects (Schiebinger *et al.*, 2021). As a result, critics of FRT have raised concerns over the use of these programs, in that they reinforce policing biases (e.g., against racialized people) rather than reduce them (Condie & Dayton, 2020; Tsui, 2020). These technical biases, along with ethical concerns, have led some cities and law enforcement agencies to place a moratorium on the use of FRT, and to calls by some academics and civil liberties advocates to halt their use by policing agencies.

6.3.6 Oversight and Guidance

With appropriate oversight and guidance, FRT and other AI technologies have the potential to support law enforcement

One of the by-products of the controversy around the use of FRT in Canada may be a reduced willingness among law enforcement agencies to invest in any digital technologies, even if those technologies do not have the same privacy or ethical concerns as FRT. The problems related to the use of FRT by Canadian law enforcement were not unexpected, as many experts — including academics, advocacy groups, and those in civil society — identified how the technology could misidentify racialized people and predicted it would lead to privacy violations (Braga, 2017; NSF, 2019; Hill, 2020; Leslie, 2020; Robertson *et al.*, 2020).

Given that these issues were foreseen, some have noted that, with the appropriate regulations, oversight, and transparency, FRT could be an important tool for criminal investigations (Robertson *et al.*, 2020; OPC, 2021c). As explained by Daniel Therrien, former Privacy Commissioner of Canada, "FRT is a powerful tool that has the potential to offer great benefits to society, but it can also be a highly invasive surveillance technology fraught with many risks" (OPC, 2021c). Recognizing the utility of FRT, the OPC, along with its provincial and territorial colleagues, developed draft guidance for law enforcement to ensure that "any use of FRT complies with the law, minimizes privacy risks and respects privacy rights" (OPC, 2021c).

Guidance on and oversight of the use of new technologies in law enforcement can help identify potential privacy or ethical issues before they are implemented

The privacy, societal, and legal challenges stemming from the use of digital technologies in law enforcement are not unique to Canada. Other jurisdictions have implemented mechanisms to identify potential legal and ethical issues before new, or advanced, technologies are used. One such example is New Zealand's Advisory Panel on Emergent Technologies, which provides publicly available guidance to the New Zealand Police (Box 6.2).

In Canada, the RCMP created the National Technology Onboarding Program in March 2021 in order "to centralize and bring more transparency to the processes that govern how the RCMP identifies, evaluates, tracks and approves the use of new and emerging technologies and investigative tools that involve the collection and use of personal information" (RCMP, 2021e). The Panel could not identify additional details about the program or whether it had, as of June 2022, reached operational status. In 2022, the Toronto Police Services Board introduced a policy governing the use of AI technology (TPSB, 2022), which states that all use of technology, including AI, must adhere to eight guiding principles: "legality, fairness, reliability, justifiability, personal and organizational accountability, transparency, privacy, and meaningful engagement." Further, procedures and processes for the review and assessment of new AI technologies will be developed in consultation with the Information and Privacy Commissioner of Ontario, Ontario's Ministry of the Attorney General, and the province's Anti-Racism Directorate, as well as other external experts and stakeholders. The review and assessment of new technologies includes establishing a risk category of the potential for harm. Board approval is required prior to the procurement, utilization, and deployment of new technologies; those deemed to be of extreme risk[22] will not be approved, and those deemed to be of high or moderate risk will be subject to additional oversight by the board and reporting by the Chief of Police (TPSB, 2022).

22 Examples of factors that may lead to an "extreme risk" designation include applications lacking a qualified human to evaluate an AI tool's recommendation; applications that lead to mass surveillance; and applications that "predict or assign likelihood" to a person or "group to offend or reoffend" (TPSB, 2022).

Box 6.2 New Zealand's Advisory Panel on Emergent Technologies

The Advisory Panel on Emergent Technologies in New Zealand was established to advise the New Zealand Police, in recognition that officers and staff are "increasingly encounter[ing] emergent technology in their day-to-day work" that may enable them to carry out their duties more effectively, but which may have important ethical, privacy, or other implications that should be considered (New Zealand Police, 2021). As explained by the New Zealand Police (2021), "adopting technologies that are not perceived to be sufficiently well understood, publicly accepted, or appropriately regulated has the potential to undermine public trust and confidence in the agency deploying them, especially where any negative impacts (such as impingement on privacy or inequitable impacts on certain groups) may be perceived to outweigh public benefits."

The purpose of the independent advisory panel is to provide guidance on the policy and ethical implications of emergent technologies (or a "significant new functionality within an existing technology") that may be used in law enforcement. The advisory panel also considers algorithms used by the police (New Zealand Police, 2021). A formal process has been established whereby the Commissioner of Police (or their delegate) refers issues to the advisory panel. Referrals include a timeframe within which advice is sought, generally in the order of four to eight weeks (with more time provided in certain cases). Advice is transmitted to the commissioner in writing, along with — if appropriate — a presentation to a police audience (New Zealand Police, 2021). This process is done in confidence, but the New Zealand Police has remarked that it is "committed to making the expert panel's advice public wherever possible — acknowledging this may not be possible in every case, for example where disclosure would breach commercial obligations" (New Zealand Police, 2022). Advice is expected to be arrived at through consensus, but opinion(s) dissenting from the majority may be recorded in cases where consensus is impossible (New Zealand Police, 2021).

The advisory panel is expected to have expertise in data and technology, ethics and human rights, privacy, Te Ao Māori, Māori data and data sovereignty, and public policy (New Zealand Police, 2021). The panel includes up to six independent members (including the chair), who are appointed by the Commissioner of Police for multi-year terms. One additional expert may be brought in on an ad hoc basis when specific additional expertise is needed. The members of this panel are eligible for remuneration (New Zealand Police, 2021).

6.4 Prosecution

The challenges created by capacity constraints are amplified by constitutionally mandated timelines to bring criminal cases to trial

The various capacity challenges faced by law enforcement agencies outlined in Section 6.2 become even greater barriers when combined with the constraints across Canada's justice system. Notably, time limits were imposed by the Supreme Court of Canada in its *R. v. Jordan* decision of 2016, which affirmed that the right to be tried within a reasonable time is guaranteed by the *Canadian Charter of Rights and Freedoms*. The ruling stated that the time between someone's arrest and trial could be no more than 18 months in provincial/territorial courts and 30 months in superior courts (SCC, 2016b; JUS, 2019). If this time limit is exceeded, criminal cases can be stayed (i.e., suspended), barring exceptional circumstances — prosecutors can make a case if delays were due to circumstances beyond their control (SCC, 2016b; JUS, 2019).

Law enforcement agencies have faced difficulty in collecting and analyzing the necessary evidence within those timelines (Cohen *et al.*, 2021). Moreover, when cases move to court, they are more complex than they were in the past and require more time to complete (JUS, 2019). The bulk effect is that limited resources may be focused on serious or high-profile crimes, so that more common or less severe cyber-criminal activities are neither investigated nor prosecuted, especially in cases when substantial resources are needed for both. Indeed, Cohen *et al.* (2021) explain that some investigations of serious crimes involving digital evidence often lack sufficient police resources and personnel to meet the timelines required by *R. v. Jordan*. This means that, since the ruling, hundreds of cases involving serious crimes — such as murder, sexual assault, and drug-related offences — have been stayed (LCJC, 2017).

Staff shortages beyond those in law enforcement negatively impact the ability of the broader criminal justice system to prosecute cybercrime

Within Canada's justice system, capacity constraints to combat cybercrime go beyond law enforcement agencies; these constraints were compounded by the COVID-19 pandemic, which caused further backlogs and increased cybercrime incidents (Nesbitt & Hansen, 2021). Underfunding, insufficient personnel, inadequate data, and too few judges in federally appointed positions are some of the barriers that continue to persist (LCJC, 2017). As of April 2022, there were 58 vacancies for federally appointed judges across Canada, with positions unfilled in 9 provinces or territories as well as in federal-level courts (FJA, 2022). Shortages of crown prosecutors have also been reported in several parts of the country

(Taylor, 2017; Parsons, 2021). The issue is particularly acute in Alberta; according to a CBC news article, Alberta Justice reported it had 47 unfilled positions (out of a total of 378) as of September 30, 2021 (Parsons, 2021). In November of that year, the Alberta Crown Attorneys' Association stated that approximately 1,200 provincial court cases were "at risk of being stayed" because of this shortage (Parsons, 2021).

There is a lack of basic digital skills within the broader criminal justice system

A dearth of basic digital skills among people working in the criminal justice system, beyond law enforcement, is creating challenges with respect to the prosecution of cyber-enabled crimes. Criminal prosecutors and judges generally have low levels of expertise in, and awareness of, cybercrime-related topics (Harkin & Whelan, 2019). This can result in heavier workloads for police officers, who need to write longer reports with additional technology-specific context and explanations (Watson & Huey, 2020). Further, complicated or highly technical justifications can prove to be a challenge for the defence, making it difficult or prohibitively expensive for an accused person to contest evidence. Digital skills gaps therefore put additional strain on a system where resources are stretched thin. As with police, training and skills upgrading related to cybercrime may be beneficial for prosecutors and judges (Dupont, 2021).

6.5 Summary

To answer the Sponsor's question about challenges brought about by advances in digital technologies, and what these mean for investigating and prosecuting crimes or addressing online harms, the Panel focused this chapter on the on-the-ground difficulties faced by law enforcement agencies as they apply existing laws and regulations in Canada. The Panel found that key challenges stem from the organizational structure of police forces, which is based on a generalist model that is ill suited for the modern law enforcement landscape. This structure has contributed to significant knowledge gaps, and to difficulties in establishing and retaining the critical digital skills needed to investigate the growing number of reported cyber-enabled crimes. Beyond specialized skills, many generalist officers lack the basic digital skills needed to tackle the changing nature of crime in the digital age.

In addition to structural and staffing challenges, law enforcement agencies face practical challenges related to criminal investigation and digital evidence analysis, as a result of advances in digital technologies. These include difficulties in acquiring needed digital information in a timely fashion, overcoming

encryption, and finding mechanisms to detect illegal material among legal content. At the same time, many of the same technologies and regulations that make it challenging for law enforcement to acquire or analyze data (e.g., production orders, encryption) are also essential for protecting public safety and privacy.

The chapter also considered select emerging practices and tools that may be applied in Canada to help overcome some of the challenges created by digital technologies. These practices include increasing the digital skills training of people working across the criminal justice system, but also moving policing toward increased professionalization, whereby officers are able to specialize and be rewarded for having, and improving, high-level digital skills. There are also opportunities to use digital technologies to help prevent, identify (through detection and reporting), and investigate cyber-enabled crime. Each new technology comes with its own ethical considerations, however, and its application without adequate guidance and oversight can lead to privacy or human rights violations against the very people police are tasked with protecting. This, in turn, hinders law enforcement further by perpetuating a distrust of all technology or new approaches. The Panel concluded that, moving forward, suitable regulation and ongoing oversight, transparency, and accountability in the use of new technologies or models can support their appropriate integration and use in law enforcement.

7

Panel Reflections

The proliferation of ever-changing digital technologies presents urgent challenges for public safety in Canada. These technologies are ubiquitous across society and are being used to cause substantial harms to all people living in Canada, even those who are offline or rarely use ICTs. At the same time, people are unsure about where to turn when they are targeted and lack access to resources that could prevent, mitigate, or remedy cyber-enabled harms. This report highlights many instances where approaches taken by different orders of government, law enforcement, and the private sector were insufficient, or were not adapted to address the challenges presented by the changing digital landscape.

Existing domestic laws meant to uphold public safety and provide remedies for victims and survivors of harmful activities often fall short when it comes to responding to ever-evolving threats and harms. Criminal law, torts, Quebec civil law, and federal privacy legislation offer a patchwork of approaches, but none fully addresses the need to enhance people's control over their data or gives them timely access to effective remedies. Moreover, not all cyber-enabled harms can or should be addressed through state-sanctioned rules. Some require a multifaceted approach grounded in community support, educational programs, and corporate social responsibility.

Governments around the world have embarked on legal reforms to strengthen public safety in the digital context. This report examined an array of implemented and proposed policies in jurisdictions that have some sociopolitical similarities with Canada and are connected to Canada through close diplomatic relationships, namely Australia, Germany, New Zealand, the United Kingdom, the United States, and the European Union. These reforms criminalize certain online harms, expand the administrative state's regulatory reach into digital spaces, expedite the removal of some content, and reform data-processing consent requirements, among other things. Some measures, however, have encouraged greater policing of online speech and users, resulting in the removal of legal content and thus raising freedom of expression and privacy concerns.

While policy-makers across Canada can learn from foreign experience, all orders of government need to consider the Canadian legal and social contexts when assessing the applicability of foreign approaches to domestic issues. For example, unlike Canada, Australia does not have an enshrined bill of rights, while U.S. digital policy emphasizes the protection of free speech under the First Amendment of the *Constitution of the United States*. These legal challenges are exacerbated by the fact that not all online harms meet the threshold of illegal behaviour. While legal reform may be necessary to address some online harms, alternative policy measures will be more effective in preventing and remediating harm, in other cases, and responding to the needs of victims and survivors.

Some cyber-enabled harms that violate criminal law are ICT-enabled crimes. This report has demonstrated that the enforcement of digital public safety faces its own set of challenges related to the prevention, investigation, analysis, and prosecution of cyber-enabled crimes. The Panel identified data volume, a lack of resources, and skills gaps, as well as outdated organizational structures, as the main obstacles to law enforcement's effective work. Improving the digital skills of people working across the criminal justice system, crafting reforms that enable officers with specialized digital skills to advance while continuing to develop and apply those skills, and professionalizing policing to a greater extent may all help jurisdictions overcome some of the challenges created by the changing nature of crime in Canada. There is also a range of digital technologies that can be used to facilitate the identification, prevention, and investigation of cyber-enabled crime. Regulation, transparency, and oversight, however, are essential to ensure that any adopted technology or model meets certain ethical and human rights standards when integrated and used in law enforcement.

Finally, public intervention alone cannot enhance the overall health of the online ecosystem. Private sector organizations, and online social media platforms in particular, play an important role in this process. While some voluntary corporate efforts are directed at limiting the proliferation of harmful material, online content spreads quickly across different platforms all over the world, defying content moderation measures. Moreover, to the extent that inflammatory content drives user engagement, platforms lack incentives to introduce reforms that will substantially change their self-regulation models.

In the area of digital public safety, governance challenges are exacerbated by the fact that public and private efforts aimed at detecting and preventing cyber-harms often incorrectly see privacy and security as being at odds. In the Panel's view, security and privacy can be mutually reinforcing — meaning that security-enhancing policies need not minimize important privacy protections, such as people's ability to control who gets access to their data, when, and for what purpose.

The Panel's report emphasizes looming privacy and security challenges presented by digital technologies and the urgent need to address these challenges, while taking into consideration complex social and legal issues underpinning digital public safety. Digital technologies present substantial public safety challenges that transcend national borders. These challenges will only increase as new technologies enter the market. Reforms of varying scope and size to better ensure digital public safety are feasible. Fostering a safer online ecosystem is a collective endeavour that includes civil society, policy-makers, law enforcement agencies, and the private sector — one that relies on international cooperation along with legal and non-legal approaches informed by the experiences of victims and survivors.

References

Aaronson, S. A. & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law, 21*(2), 245-272.

AARP. (2022). Cryptocurrency Fraud. Retrieved March 2022, from https://www.aarp.org/money/scams-fraud/info-2019/cryptocurrency.html.

Abacus Data. (2021). *Online Hate and Racism Canadian Experiences and Opinions on What to Do About It*. Ottawa (ON): Abacus Data.

ABCA (Court of Appeal of Alberta). (2022). *R. v. Bykovets, 2022 ABCA 208*. Calgary (AB): ABCA.

Abreu, R. L. & Kenny, M. C. (2018). Cyberbullying and LGBTQ youth: A systematic literature review and recommendations for prevention and intervention. *Journal of Child and Adolescent Trauma, 11*(1), 81-97.

Adee, S. (2020). What Are Deepfakes and How Are They Created? Retrieved January 2022, from https://spectrum.ieee.org/what-is-deepfake.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1-15.

Ahmad, H. (2017). Youth de-radicalization: A Canadian framework. *Journal for Deradicalization, 12*, 119-168.

AHRC (Australian Human Rights Commission). (n.d.). How are Human Rights Protected in Australian Law? Retrieved January 2022, from https://humanrights.gov.au/our-work/rights-and-freedoms/how-are-human-rights-protected-australian-law.

Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The State of Deepfakes: Landscape, Threats, and Impact*. Amsterdam, Netherlands: Deeptrace.

Al-Khateeb, H. M., Epiphaniou, G., Alhaboby, Z. A., Barnes, J., & Short, E. (2017). Cyberstalking: Investigating formal intervention and the role of corporate social responsibility. *Telematics and Informatics, 34*(4), 339-349.

Al-Qazzaz, K. (2020). Islamophobia is on the Rise During COVID-19. Retrieved December 2022, from https://policyoptions.irpp.org/magazines/october-2020/islamophobia-is-on-the-rise-during-covid-19/.

Alavi, S., Charleston, E., Du Perron, S., El-Khoury, D.-N., Freedman, B., Gauthier, J., . . . Windt, D. (2022). *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for Businesses*. Toronto (ON): Borden Ladner Gervais LLP.

Albin-Lackey, C. (2013). *Without Rules: A Failed Approach to Corporate Accountability*. New York (NY): Human Rights Watch.

Albu, O. B. & Flyverbom, M. (2016). Organizational Transparency: Conceptualizations, Conditions, and Consequences. *Business & Society, 58*(2), 268-297.

Alexander, J. (2015). *How Technology is Killing Privacy*. Allendale (MI): Grand Valley State University.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

AlKhatib, B. & Basheer, R. (2019). Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation. *Journal of Digital Information Management, 17*(2), 51.

Allen & Overy. (2020). The Digital Services Act Package Is Here. Retrieved April 2020, from https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-digital-services-act-package-is-here.

Allen, B. (2019). Revenge Porn and Sext Crimes: Canada Sees More than 5,000 Police Cases as Law Marks 5 Years. Retrieved November 2021, from https://www.cbc.ca/news/canada/saskatchewan/revenge-porn-and-sext-crimes-canada-sees-more-than-5-000-police-cases-as-law-marks-5-years-1.5405118.

Andrey, S., Rand, A., Masoodi, M. J., & Bardeesy, K. (2021a). *Rebuilding Canada's Public Square*. Toronto (ON): Ryerson University.

Andrey, S., Rand, A., Masoodi, M. J., & Tran, S. (2021b). *Private Messaging Public Harms: Disinformation and Online Harms on Private Messaging Platforms in Canada*. Toronto (ON): Ryerson University.

Apple. (2022). An Update on AirTag and Unwanted Tracking. Retrieved April 2022, from https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/.

Aquilina, K. (2010). Public security versus privacy in technology law: A balancing act? *Computer Law & Security Review, 26*, 130-143.

Ardill, L. (2021). Know the Facts: TikTok's Latest Move Against Misinformation. Retrieved June 2021, from https://www.siliconrepublic.com/companies/tiktok-know-the-facts-new-fact-checking-feature.

ASIO (Australian Security Intelligence Organisation). (2021). *ASIO Annual Report 2020-21*. Canberra, Australia: Gov. of Australia.

Askanius, T. (2021). On frogs, monkeys, and execution memes: Exploring the humor-hate nexus at the intersection of neo-Nazi and alt-right movements in Sweden. *Television & New Media, 22*(2), 147-165.

Austin, L. (2012). *Privacy, Shame and the Anxieties of Identity*. Toronto (ON): University of Toronto.

AUSTRAC (Australian Transaction Reports and Analysis Centre). (2018). New Australian Laws to Regulate Cryptocurrency Providers. Retrieved February 2022, from https://www.austrac.gov.au/new-australian-laws-regulate-cryptocurrency-providers.

Awan, I. & Zempi, I. (2015). *We Fear for our Lives: Offline and Online Experiences of Anti-Muslim Hostility*. United Kingdom: Tell MAMA, Birmingham City University, Nottingham Trent University.

Badour, A., Shah, S., & Berg, E. (2020). FINTRAC Guidance on Red Flag Indicators Associated With Virtual Currency Transactions. Retrieved April 2022, from https://www.mccarthy.ca/fr/node/68556.

Bailey, J. (2008). Towards an equality-enhancing conception of privacy. *The Dalhousie Law Journal, 31*(2), 267-309.

Bailey, J. (2015). A Perfect Storm: How the Online Environment, Social Norms, and Law Shape Girls' Lives. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens*. Ottawa (ON): University of Ottawa Press.

Bailey, J. & Shayan, S. (2016). Missing and murdered Indigenous women crisis: Technological dimensions. *Canadian Journal of Women and the Law, 28*(2), 321-341.

Bailey, J., Steeves, V., & Dunn, S. (2017). *Submission to the Special Rapporteur on Violence Against Women, Re: Regulating Online Violence and Harassment Against Women*. Ottawa (ON): University of Ottawa.

Bailey, J. & Mathen, C. (2019). Technology-facilitated violence against women & girls: Assessing the Canadian criminal law response. *Canadian Bar Review, 97*(3), 664-696.

Baird, K., McDonald, K. P., & Connolly, J. (2020). Sex trafficking of women and girls in a southern Ontario region: Police file review exploring victim characteristics, trafficking experiences, and the intersection with child welfare. *Canadian Journal of Behavioural Science/Revue canadienne des sciences du comportement, 52*(1), 8-17.

Balkin, J. (2009). The future of free expression in a digital age. *Pepperdine Law Review, 36*(2), 427-444.

Ballard, B. & Parsons, C. (2022). Mixed traditions: Evaluating telecommunications transparency. *Internet Policy Review, 11*(1), 1-30.

Bambauer, D. E. (2013). Privacy versus security. *Journal of Criminal Law and Criminology, 103*(3), 667-684.

Bankston, K. S. & Soltani, A. (2014). Tiny constables and the cost of surveillance: Making cents out of United States v. Jones. *The Yale Law Journal Online, 123*, 335-357.

Baril, D. E. (2014). *La transformation des enquêtes policières due à l'influence des technologies: perspective d'une unité policière spécialisée en analyse judiciaire informatique*. Montréal (QC): Université de Montréal.

Barocas, S. & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671-732.

Baron, J., O'Mahony, A., Manheim, D., & Dion-Schwarz, C. (2015). *National Security Implications of Virtual Currency*. Santa Monica (CA): RAND Corporation.

Bastug, M. F., Douai, A., & Akca, D. (2020). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. *Studies in Conflict & Terrorism, 43*(7), 616-637.

BBC News. (2021). Twitter Suspends 70,000 Accounts Linked to QAnon. Retrieved June 2021, from https://www.bbc.com/news/technology-55638558.

BCIT (British Columbia Institute of Technology). (n.d.). Forensic Investigation. Retrieved January 2022, from https://www.bcit.ca/programs/forensic-investigation-digital-forensics-and-cybersecurity-option-bachelor-of-technology-full-time-part-time-845jbtech/#overview.

BCPC (Provincial Court of British Columbia). (2012). *R. v. Corby, 2012 BCPC 561*. Vancouver (BC): BCPC.

BCSC (Supreme Court of British Columbia). (2022). *R. v. Coban, 2022 BCSC 1810*. New Westminster (BC): BCSC.

BDC (Business Development Bank of Canada). (2022). Crowdfunding. Retrieved April 2022, from https://www.bdc.ca/en/articles-tools/entrepreneur-toolkit/templates-business-guides/glossary/crowdfunding#.

Beaulac, S. & Gaudreault-DesBiens, J.-F. (2017). *Droit civil et common law: convergences et divergences*. Ottawa (ON): Fédération des ordres professionnels de juristes du Canada.

Becker, M. (2019). Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology, 21*, 301-317.

Beesley, P. (2021). *Competency-Based Management Framework for Digital Competencies in Canadian Policing*. Charlottetown (PE): Canadian Police Knowledge Network.

Bell, S. (2020). CSIS Warns about Conspiracy Theories Linking COVID-19 to 5G Technology. Retrieved December 2022, from https://globalnews.ca/news/7496689/csis-conspiracy-theories-coronavirus-covid-19-5g-technology/.

Bellemare, A. & Ho, J. (2020). Social Media Firms Catching More Misinformation, But Critics Say 'They Could Be Doing More'. Retrieved November 2021, from https://www.cbc.ca/news/science/social-media-platforms-pandemic-moderation-1.5536594.

Bellemare, A., Ho, J., & Nicholson, K. (2020). Quebec Police Investigating Possible Link between Cell Tower Fires and 5G Coronavirus Conspiracy Theories. Retrieved December 2022, from https://www.cbc.ca/news/canada/coronavirus-conspiracy-theory-5g-fires-quebec-1.5560570.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

Bellovin, S. M., Blaze, M., Clark, S., & Susan Landau, L. (2014). Lawful hacking: Using existing vulnerabilities for wiretapping on the internet. *Northwestern Journal of Technology and Intellectual Property, 12*(1), Article 1.

Benesch, S., Ruths, D., Dillon, K. P., Saleem, H. M., & Wright, L. (2016). *Counterspeech on Twitter: A Field Study*. Ottawa (ON): Kanishka Project, Public Safety Canada.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York (NY): Oxford University Press.

Bennett, C. J. & Raab, C. D. (2018). *The Governance of Privacy: Policy Instruments in Global Perspective*. New York (NY): Routledge.

Bennett Jones. (2021). Changes to AML and Virtual Currency Regulations for Reporting Entities and Money Service Businesses. Retrieved April 2022, from https://www4.bennettjones.com/Blogs-Section/Changes-to-AML-and-Virtual-Currency-Regulations-for-Reporting-Entities-and-Money-Service-Businesses#.

Bennett Moses, L. (2007). Recurring dilemmas: Law's race to keep up with technological change. *Journal of Law, Technology & Policy, 2007*(2), 239-285.

Bennett, W. L. & Livingston, S. (2020). Conclusion - Defending Democracy in the Disinformation Age. In W. L. Bennett & S. Livingston (Eds.), *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States*. New York (NY): Cambridge University Press.

Berentsen, A. & Schär, F. (2018). A short introduction to the world of cryptocurrencies. *Federal Reserve Bank of St. Louis Review, 100*(1), 1-16.

Berger, J. M. (2019). The Dangerous Spread of Extremist Manifestos. Retrieved May 2022, from https://www.theatlantic.com/ideas/archive/2019/02/christopher-hasson-was-inspired-breivik-manifesto/583567/.

Bernaciak, C. & Ross, D. (2022). How Easy Is It to Make and Detect a Deepfake? Retrieved October 2022, from https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/.

Berners-Lee, T. (2019). I Invented the World Wide Web. Here's How We Can Fix It. Retrieved December 2022, from https://www.nytimes.com/2019/11/24/opinion/world-wide-web.html.

Bernier, C. (2012). *The Integral Role of Civil Society in Balancing Privacy and National Security.* Paper presented at International Intelligence Review Agencies Conference, Ottawa (ON).

Bessi, A., Petroni, F., Del Vicario, M., Zollo, F., Anagnostopoulos, A., Scala, A., . . . Quattrociocchi, W. (2016). Homophily and polarization in the age of misinformation. *The European Physical Journal Special Topics, 225*(10), 2047-2059.

Beswick, S. (2022). *Tort Law: Cases and Commentaries* (2nd ed.). Vancouver (BC): University of British Columbia.

Bhullar, R. (2022). Online Streaming Act Bill C-11 Repeats Bill C-10's Mistakes. Retrieved April 2022, from https://openmedia.org/article/item/online-streaming-act-bill-c-11-repeats-bill-c-10s-mistakes.

Bidgoli, M. & Grossklags, J. (2016). *End User Cybercrime Reporting: What We Know and What We Can Do to Improve It.* Paper presented at 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver (BC).

Binns, C. A. & Kempf, R. J. (2021). Who Has Legal Responsibility for Safety and Security in Hotels Versus Home Sharing? In C. A. Binns & R. J. Kempf (Eds.), *Safety and Security in Hotels and Home Sharing*. Cham, Switzerland: Springer.

Bitwise Asset Management. (2019). *Bitwise Asset Management - Presentation to the U.S. Securities and Exchange Commission*. Washington (DC): Bitwise Asset Management.

BLG (Borden Ladner Gervais). (2021). *Québec Privacy Law Reform: Compliance Guide for Organizations*. Montréal (QC): BLG.

Blumenfeld, W. J. & Cooper, R. M. (2010). LGBT and allied youth responses to cyberbullying: Policy implications. *International Journal of Critical Pedagogy, 3*(1), 114-133.

Bohannon, M. (2018). The State of Encryption: How the Debate Has Shifted. Retrieved March 2022, from https://opensource.com/article/18/6/listening-susan-landau.

Bond, S. (2021). Unwelcome on Facebook and Twitter, QAnon Followers Flock to Fringe Sites. Retrieved November 2021, from https://www.npr.org/2021/01/31/962104747/unwelcome-on-facebook-twitter-qanon-followers-flock-to-fringe-sites.

Booker, B. (2021). Facebook Removes 'Stop The Steal' Content; Twitter Suspends QAnon Accounts. Retrieved June 2021, from https://www.npr.org/sections/insurrection-at-the-capitol/2021/01/12/956003580/facebook-removes-stop-the-steal-content-twitter-suspends-qanon-accounts.

Bossler, A. M. & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management, 35*(1), 165-181.

Bothamley, S. & Tully, R. J. (2018). Understanding revenge pornography: Public perceptions of revenge pornography and victim blaming. *Journal of Aggression Conflict and Peace Research, 10*(1), 1-10.

Boutilier, A. (2016). Encryption Creating a Barrier for Police, Documents Suggest. Retrieved March 2022, from https://www.thestar.com/news/canada/2016/07/02/encryption-creating-a-barrier-for-police-documents-suggest.html.

Boutilier, A. & Ling, J. (2020). Canadian Forces Reservist Who Stormed Rideau Hall Grounds Faces 22 Charges. Retrieved December 2022, from https://www.thestar.com/politics/federal/2020/07/03/rcmp-release-new-details-of-armed-man-who-gained-access-to-rideau-hall-grounds-thursday.html.

Boutin-Clermont, M.-A. (2014). Chronique - La Criminalisation du "revenge porn" : Entre Théorie et Pratique. Retrieved May 2022, from https://www.editionsyvonblais.com/blogue/marie-andree-boutin-clermont/chronique-la-criminalisation-du-revenge-porn-entre-theorie-et-pratique-30/.

Braga, M. (2017). Facial Recognition Technology is Coming to Canadian Airports This Spring. Retrieved April 2022, from https://www.cbc.ca/news/science/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344.

Brannon, V. C. (2019). *Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230*. Washington (DC): Congressional Research Service.

Brennen, J. S., Simon, F. M., & Nielsen, R. K. (2021). Beyond (mis)representation: Visuals in COVID-19 misinformation. *The International Journal of Press/Politics, 26*(1), 277-299.

Brey, P. (2017). Theorizing Technology and its Role in Crime and Law Enforcement. In M. R. McGuire & T. J. Holt (Eds.), *The Routledge Handbook of Technology, Crime and Justice*. Abingdon, United Kingdom: Routledge.

Brideau, I. & Brosseau, L. (2019). *The Distribution of Legislative Powers: An Overview*. Ottawa (ON): Library of Parliament.

Brideau, I., de Billy Brown, G., Lord, F., & Ménard, M. (2020). *Bill C-10: An Act to Amend the Broadcasting Act and to Make Related and Consequential Amendments to Other Acts*. Ottawa (ON): Library of Parliament.

Bridgman, A., Merkley, E., Zhilin, O., Loewen, P. J., Owen, T., & Ruths, D. (2021). Infodemic pathways: Evaluating the role that traditional and social media play in cross-national information transfer. *Frontiers in Political Science, 3*, 648646.

Bridgman, A., Lavigne, M., Baker, M., Bergeron, T., Bohonos, D., Burton, A., . . . Loewen, P. (2022). *Mis- and Disinformation During the 2021 Canadian Federal Election*. Montréal (QC): Media Ecosystem Observatory.

Brighton, M. (2004). BT Puts Block on Child Porn Sites. Retrieved February 2022, from https://www.theguardian.com/technology/2004/jun/06/childrensservices.childprotection.

Broll, R. & Huey, L. (2015). "Just being mean to somebody isn't a police matter": Police perspectives on policing cyberbullying. *Journal of School Violence, 14*(2), 155-176.

Broll, R., Dunlop, C., & Crooks, C. V. (2018). Cyberbullying and internalizing difficulties among Indigenous adolescents in Canada: Beyond the effect of traditional bullying. *Journal of Child & Adolescent Trauma, 11*(1), 71-79.

Brookes, J. (2022). Big Tech Says it is Confused by Australia's Growing Online Safety Laws. Retrieved January 2022, from https://www.innovationaus.com/big-tech-says-it-is-confused-by-australias-growing-online-safety-laws/.

Brown, A., Gibson, M., & Short, E. (2017). Modes of cyberstalking and cyberharassment: Measuring the negative effects in the lives of victims in the UK. *Annual Review of Cybertherapy and Telemedicine, 15*, 57-63.

Browning, K. (2021). Extremists Find a Financial Lifeline on Twitch. Retrieved December 2022, from https://www.nytimes.com/2021/04/27/technology/twitch-livestream-extremists.html.

Brownsword, R. (2008). *Rights, Regulation, and the Technological Revolution*. Oxford, United Kingdom: Oxford University Press.

Brugoni, M. (2018). Le e-learning cybercrime : Une formation harmonisée. *POLCANT info, 109*, 12-13.

Bull, M. (2021). Exclusive: What is data poisoning and why should we be concerned? Retrieved May 2022, from https://internationalsecurityjournal.com/what-is-data-poisoning/.

Buolamwini, J. & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 81*, 77-91.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology, 14*(2), 20-31.

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2020). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis. *Policing: An International Journal*, *43*(1), 105-119.

Bygrave, A. L. (2010). Privacy and data protection in an international perspective. *Scandinavian Studies in Law*, *56*, 165-200.

C3P (Canadian Centre for Child Protection). (2016). *Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis*. Winnipeg (MB): C3P.

C3P (Canadian Centre for Child Protection). (2017). *Cybertip.ca: 15-Year Anniversary Report*. Winnipeg (MB): C3P.

C3P (Canadian Centre for Child Protection). (2021). *Project Arachnid: Online Availability of Child Sexual Abuse Material*. Winnipeg (MB): C3P.

CACP (Canadian Association of Chiefs of Police). (2016). *Resolutions Adopted at the 111th Annual Conference*. Ottawa (ON): CACP.

CAFC (Canadian Anti-Fraud Centre). (2020). Fraud Initiated by Telephone Call. Retrieved February 2022, from https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/telephone-telephonique-eng.htm.

CAFC (Canadian Anti-Fraud Centre). (2021a). Report Fraud and Cybercrime. Retrieved January 2021, from https://www.antifraudcentre-centreantifraude.ca/report-signalez-eng.htm.

CAFC (Canadian Anti-Fraud Centre). (2021b). Top 10 Frauds Targeting Canadians in 2020. Retrieved November 2021, from https://www.antifraudcentre-centreantifraude.ca/features-vedette/2021/frauds-10-fraudes-eng.htm.

CAFC (Canadian Anti-Fraud Centre). (2021c). Canadian Anti-Fraud Centre (Home Page). Retrieved November 2021, from https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

CAFC (Canadian Anti-Fraud Centre). (2021d). Service Scams. Retrieved November 2021, from https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/service-eng.htm#a3.

Campbell, R. & Lovenduski, J. (2016). *Footprints in the Sand: Five Years of the Fabian Women's Network Mentoring and Political Education Programme*. London, United Kingdom: Fabian Society.

Canada Centre (Canada Centre for Community Engagement and Prevention of Violence). (2018). *National Strategy on Countering Radicalization to Violence*. Ottawa (ON): Government of Canada.

Canadian Centre for Cyber Security. (2020a). *National Cyber Threat Assessment, 2020*. Ottawa (ON): Communications Security Establishment.

Canadian Centre for Cyber Security. (2020b). Social Media Account Impersonation. Retrieved February 2022, from https://cyber.gc.ca/en/guidance/social-media-account-impersonation.

Canadian Centre for Cyber Security. (2021a). Cyber Threat and Cyber Threat Actors. Retrieved August 2022, from https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

Canadian Centre for Cyber Security. (2021b). *Cyber Threat Bulletin: The Ransomware Threat in 2021*. Ottawa (ON): Communications Security Establishment.

Canadian Centre for Cyber Security. (2022a). *National Cyber Threat Assessment, 2023-2024*. Ottawa (ON): Communications Security Establishment.

Canadian Centre for Cyber Security. (2022b). *How to Identify Misinformation, Disinformation, and Malinformation*. Ottawa (ON): Communications Security Establishment.

Caneppele, S. & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66-79.

Carbert, M. (2022). Liberals Re-Introduce Broadcasting Act Bill, Pledge Amendments Will Ensure Individual Social Media Users Are Exempt. Retrieved February 2022, from https://www.theglobeandmail.com/politics/article-liberals-re-introduce-broadcasting-act-bill-pledge-amendments-will/.

Carlini, N. & Farid, H. (2020). Evading Deepfake-Image Detectors with White- and Black-Box Attacks. Retrieved August 2022, from https://arxiv.org/pdf/2004.00622.pdf.

Carter, W. A. & Daskal, J. C. (2018). *Low-Hanging Fruit*. Washington (DC): Center for Strategic & International Studies.

Carvin, S., Juneau, T., Forcese, C., & Pyrik, J. (2021a). The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). In *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*. Toronto (ON): University of Toronto Press.

Carvin, S., Juneau, T., & Forcese, C. (2021b). Conclusion. In S. Carvin, T. Juneau & C. Forcese (Eds.), *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*. Toronto (ON): University of Toronto Press.

CBA (Canadian Bankers Association). (2022). Focus: Protecting Canadians from Fraud. Retrieved May 2022, from https://cba.ca/protecting-canadians-from-fraud.

CCA (Council of Canadian Academies). (2014). *Policing Canada in the 21st Century: New Policing for New Challenges. The Expert Panel on the Future of Canadian Policing Models*. Ottawa (ON): CCA.

CCA (Council of Canadian Academies). (2021). *Waiting to Connect: The Expert Panel on High-Throughput Networks for Rural and Remote Communities in Canada*. Ottawa (ON): CCA.

CCA (Council of Canadian Academies). (2022). *Leaps and Boundaries: The Expert Panel on Artificial Intelligence for Science and Engineering*. Ottawa (ON): CCA.

CCADE (Canadian Citizens' Assembly on Democratic Expression). (2021). *Canadian Citizens' Assembly on Democratic Expression: Recommendations to Strengthen Canada's Response to New Digital Technologies and Reduce the Harm Caused by Their Misuse*. Ottawa (ON): Public Policy Forum.

CCJCSS (Canadian Centre for Justice and Community Safety Statistics). (2021). *Uniform Crime Reporting Survey (UCR) Manual*. Ottawa (ON): Statistics Canada.

CDPDJ (Commission des droits de la personne et des droits de la jeunesse). (2022). Exploitation. Retrieved January 2022, from https://cdpdj.qc.ca/en/your-obligations/prohibited-practices/exploitation.

Cerulus, L. (2020). How Anti-5G Anger Sparked a Wave of Arson Attacks. Retrieved December 2022, from https://www.politico.com/news/2020/04/30/how-anti-5g-anger-sparked-a-wave-of-arson-attacks-across-europe-228050.

CGE (Conférence des grandes écoles). (2022). La gendarmerie nationale développe et valorise les parcours doctoraux. Retrieved June 2022, from https://www.cge.asso.fr/liste-actualites/la-gendarmerie-nationale-developpe-et-valorise-les-parcours-doctoraux/.

Chainlink. (2022). What is a DEX (Decentralized Exchange)? Retrieved September 2022, from https://blog.chain.link/dex-decentralized-exchange/#:~:text=A%20decentralized%20exchange%20(DEX)%20is,transfer%20and%20custody%20of%20funds.

Chandler, J. (2009). Privacy vs. National Security: Clarifying the Trade-Off. In I. Kerr, V. Steeves & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. New York (NY): Oxford University Press.

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance, 12*(1), 101-114.

Chertoff, M. (2017). A public policy perspective of the dark web. *Journal of Cyber Policy* 2(1), 26-38.

Chesney, B. & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*, 1753-1820.

Choi, T. (2019). Canada's Digital Charter Not Strong Enough to Soothe Privacy Concerns on Sidewalk Labs: Critics. Retrieved May 2022, from https://globalnews.ca/news/5337890/canada-digital-charter-sidewalk-labs/.

Christchurch Call. (2019). The Christchurch Call to Action: To Eliminate Terrorist & Violent Extremist Content Online. Retrieved July 2021, from https://www.christchurchcall.com/call.html.

Christchurch Call. (2021). *Christchurch Call Community Consultation: Final Report*. Wellington, New Zealand: Christchurch Call.

CIGI (Centre for International Governance Innovation). (2021). *Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa*. Waterloo (ON): CIGI.

Citron, D. K. (2009). Cyber civil rights. *Boston University Law Review, 89*, 61-125.

Citron, D. K. & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review, 40*, 345-391.

Citron, D. K. & Penney, J. W. (2019). When law frees us to speak. *Fordham Law Review, 87*(6), 2317-2335.

City of Calgary. (2021). Calgary Police Service and RCMP Contribute to Ransomware Arrests and Seizures Overseas in Operation GoldDust. Retrieved January 2022, from https://newsroom.calgary.ca/calgary-police-service-and-rcmp-contribute-to-ransomware-arrests-and-seizures-overseas-in-operation-golddust/.

CIVIX Canada. (2022). CTRL-F: Find the Facts. Retrieved May 2022, from https://ctrl-f.ca/en/.

CJEU (Court of Justice of the European Union). (2014). *Google Spain SL and Google Inc. v AEPD and Mario Costeja González*. Luxembourg City, Luxembourg: CJEU.

Clark, R., Kreps, S., & Rao, A. (2022). Shifting Crypto Landscape Threatens Crime Investigations and Sanctions. Retrieved June 2022, from https://www.brookings.edu/techstream/shifting-crypto-landscape-threatens-crime-investigations-and-sanctions/.

Clearview AI. (2021). Clearview AIs Facial Recognition Platform Achieves Superior Accuracy & Reliability Across All Demographics in NIST Testing. Retrieved April 2022, from https://www.clearview.ai/press-release-nist-facial-recognition-accuracy.

CMIC (Crypto Market Integrity Coalition). (2022). Public and Unequivocal Pledge. Retrieved February 2022, from https://www.cryptomarketintegrity.com/#The-Pledge.

Cockfield, A. J. (2007). Protecting the social value of privacy in the context of state investigations using new technologies. *U.B.C. Law Review, 40*(1), 41-67.

COE (Council of Europe). (2021a). *Acceding to the Budapest Convention on Cybercrime: Benefits*. Strasbourg, France: COE.

COE (Council of Europe). (2021b). Details of Treaty No.189. Retrieved January 2022, from https://www.coe.int/en/web/conventions/full-list2?module=treaty-detail&treatynum=189.

COE (Council of Europe). (2021c). New Treaties. Retrieved January 2022, from https://www.coe.int/en/web/conventions/new-treaties.

COE (Council of Europe). (2022). Chart of Signatures and Ratifications of Treaty 185. Retrieved October 2022, from https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

COE (Council of Europe). (n.d.-a). The Budapest Convention (ETS No. 185) and its Protocols. Retrieved January 2022, from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

COE (Council of Europe). (n.d.-b). Budapest Convention. Retrieved October 2022, from https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/.

Cohen, I. M., Davies, G., Pastia, C., McCormick, A., Lee, Z., Osterberg, E., . . . Schenk, A. (2021). *An Examination of The Impact of Court Rulings on Police Investigation Time and Resources*. Abbotsford (BC): University of the Fraser Valley.

Colliver, C., Comerford, M., King, J., Krasodomski-Jones, A., Schwieter, C., & Tuck, H. (2021). *Digital Policy Lab '20 Companion Papers*. London, United Kingdom: Institute for Strategic Dialogue.

Condie, B. & Dayton, L. (2020). Four AI Technologies That Could Transform the Way We Live and Work. Retrieved April 2022, from https://www.nature.com/articles/d41586-020-03413-y.

Cook, J. (2019). Here's What It's Like to See Yourself in a Deepfake Porn Video. Retrieved January 2022, from https://www.huffpost.com/entry/deepfake-porn-heres-what-its-like-to-see-yourself_n_5d0d0faee4b0a3941861fced.

Cook, J. (2021). A Powerful New Deepfake Tool Has Digitally Undressed Thousands of Women. Retrieved January 2022, from https://www.huffpost.com/entry/deepfake-tool-nudify-women_n_6112d765e4b005ed49053822.

Corb, A. (2015). Hate and Hate Crime in Canada. In N. Hall, A. Corb, P. Giannasi & J. G. D. Grieve (Eds.), *The Routledge International Handbook on Hate Crime*. Abingdon, United Kingdom: Routledge.

Couvillon, M. A. & Ilieva, V. (2011). Recommended practices: A review of schoolwide preventative programs and strategies on cyberbullying. *Preventing School Failure, 55*(2), 96-101.

CPKN (Canadian Police Knowledge Network). (2021). Policing in a Digital World: Competencies and Training for Canadian Law Enforcement. Retrieved January 2022, from https://www.cpkn.ca/en/news/competency-based-management-framework-for-digital-competencies-in-canadian-policing/.

CPKN (Canadian Police Knowledge Network). (2022). Course Catalogue. Retrieved February 2022, from https://www.cpkn.ca/en/course-catalogue/.

CRA (Canada Revenue Agency). (2021). Guide for Cryptocurrency Users and Tax Professionals. Retrieved February 2022, from https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html.

Craft, S., Ashley, S., & Maksl, A. (2017). News media literacy and conspiracy theory endorsement. *Communication and the Public, 2*(4), 388-401.

Crosby, A. (2021). Policing right-wing extremism in Canada: Threat frames, ideological motivation, and societal implications. *Surveillance & Society, 19*(3), 359-363.

Cross, C. & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing: A Journal of Policy and Practice, 9*(2), 119-128.

Cross, C. (2016). 'They're very lonely': Understanding the fraud victimisation of seniors. *International Journal for Crime, Justice and Social Democracy, 5*(4), 60-74.

Cross, C., Richards, K., & Smith, R. (2016). *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support (Report to the Criminology Research Advisory Council Grant: CRG 29/13-14)*. Canberra, Australia: Australia's Criminology Research Advisory Council.

Cross, C. (2017). "I've lost some sleep over it": Secondary trauma in the provision of support to older fraud victims. *Canadian Journal of Criminology and Criminal Justice, 59*(2), 168-197.

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends and Issues in Crime and Criminal Justice, 635*, ti78207.

CRTC (Canadian Radio-television and Telecommunications Commission). (2022). *Compliance and Enforcement and Telecom Decision CRTC 2022-170*. Ottawa (ON): CRTC.

Crumpler, W. & Lewis, J. A. (2021). *How Does Facial Recognition Work?* Washington (DC): Center for Strategic & International Studies.

CSA (Canadian Securities Administrators). (2020). *CSA Staff Notice 21-327: Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets*. Ottawa (ON): CSA.

CSA & IIROC (Canadian Securities Administrators & Investment Industry Regulatory Organization of Canada). (2021). *Staff Notice 21-329 Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements*. Ottawa (ON): CSA & IIROC.

CSIS (Canadian Security Intelligence Service). (2018). *Who Said What? The Security Challenges of Modern Disinformation*. Ottawa (ON): CSIS.

CSIS (Canadian Security Intelligence Service). (2021a). *Public Report 2020*. Ottawa (ON): CSIS.

CSIS (Canadian Security Intelligence Service). (2021b). *Foreign Interference: Threats to Canada's Democratic Process*. Ottawa (ON): CSIS.

CSIS (Canadian Security Intelligence Service). (2022). *Protecting National Security in Partnership with All Canadians*. Ottawa (ON): CSIS.

Culliford, E. & Heath, B. (2021). Facebook Knew About, Failed to Police Abusive Content Globally, Documents Show. Retrieved April 2022, from https://www.reuters.com/technology/facebook-knew-about-failed-police-abusive-content-globally-documents-2021-10-25/.

Cumbo-Steinmetz, S., Guest, L., Shah, R., & Reynolds, M. (2020). Ontario Recognizes New Privacy Tort. Retrieved June 2022, from https://www.torys.com/Our%20Latest%20Thinking/Publications//2020/01/ontario-recognizes-new-privacy-tort/.

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2021). Social Media Companies Should Self-Regulate. Now. Retrieved October 2022, from https://hbr.org/2021/01/social-media-companies-should-self-regulate-now.

Cybertip.ca. (2022a). Canadian Coalition Against Internet Child Exploitation. Retrieved October 2022, from https://cybertip.ca/en/about/ccaice/.

Cybertip.ca. (2022b). Report Types. Retrieved January 2022, from https://cybertip.ca/en/report/types/.

Cybertip.ca. (2022c). Our Results. Retrieved January 2022, from https://cybertip.ca/en/about/results/.

Cybertip.ca. (2022d). Partners. Retrieved January 2022, from https://cybertip.ca/en/about/partners/.

Cybertip.ca. (n.d.). Mandatory Reporting. Retrieved October 2022, from https://www.cybertip.ca/app/en/projects-mandatory_reporting.

d'Anglejan-Chatillon, A., Grewal, R., Lévesque, É., & Vieira, C. (2021). The Virtual Currency Regulation Review: Canada. In M. S. Sackheim & N. A. Howell (Eds.), *The Virtual Currency Regulation Review* (4th ed.). London, United Kingdom: Law Business Research Ltd.

Daigle, T. (2020). Clearview AI Stops Offering Facial Recognition Software in Canada Amid Privacy Probe. Retrieved April 2022, from https://www.cbc.ca/news/science/clearview-ai-stops-facial-recognition-in-canada-1.5639380.

Dan, V., Paris, B., Donovan, J., Hameleers, M., Roozenbeek, J., van der Linden, S., & von Sikorski, C. (2021). Visual mis- and disinformation, social media, and democracy. *Journalism & Mass Communication Quarterly, 98*(3), 641-664.

Daswani, Y. & Pearson, H. (2014). Preventing Revenge Porn. Retrieved August 2021, from http://www.keepcalmtalklaw.co.uk/preventing-revenge-porn/.

Daubs, K. (2022). Scammers Hijacked my Phone Number: There's Nothing I Can Do About Spoofing Attacks. Retrieved February 2022, from https://www.thestar.com/news/gta/2022/01/27/spammers-are-using-my-number-and-theres-nothing-i-can-do-why-spoofed-calls-are-more-than-a-nuisance.html?rf.

Davidson, T., Bhattacharya, D., & Weber, I. (2019). *Racial Bias in Hate Speech and Abusive Language Detection Datasets.* Paper presented at Third Workshop on Abusive Language, Florence, Italy.

Davis, J. (2021). Old Methods, New Technologies. In J. Davis (Ed.), *Illicit Money: Financing Terrorism in the Twenty-First Century.* Boulder (CO): Lynne Rienner Publishers.

Dawson, L. L. & Amarasingam, A. (2021). Homegrown terrorist radicalization: The Toronto 18 in comparative perspective. *Manitoba Law Journal, 44*(1), 1-33.

De Coninck, D., Frissen, T., Matthijs, K., d'Haenens, L., Lits, G., Champagne-Poirier, O., . . . Salerno, S. (2021). Beliefs in conspiracy theories and misinformation about COVID-19: Comparative perspectives on the role of anxiety, depression and exposure to and trust in information sources. *Frontiers in Psychology, 12*, 646394.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review, 34*(2), 193-203.

Décary-Hétu, D. & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55-75.

DEDC (Special Joint Committee on the Declaration of Emergency). (2022). *Evidence Number 007. Tuesday, May 10, 2022.* Ottawa (ON): House of Commons of Canada.

Delwaide, K. & Aylwin, A. (2005). *Learning from a Decade of Experience: Quebec's Private Sector Privacy Act*. Ottawa (ON): Office of the Privacy Commissioner of Canada.

DeMatteo, M. (2022). Bitcoin Price History: 2009 to 2022. Retrieved June 2022, from https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-price-history/#:~:text=2020%3A%20The%20Coronavirus%20Pandemic&text=By%20December%202020%2C%20Bitcoin's%20price,highest%20it%20had%20ever%20been.

Dentons. (2021). The Use and Limits of Mutual Legal Assistance Treaties: A Case Study in Canada and the United Kingdom. Retrieved May 2022, from https://www.dentons.com/en/insights/articles/2021/may/27/the-use-and-limits-of-mutual-legal-assistance-treaties-a-case-study-in-canada-and-the-united-kingdom.

Devlin, K. (2020). Attacks on 5G phone Masts Putting Lives at Risk, No10 Warns Amid Coronavirus Conspiracy Theories. Retrieved December 2022, from https://www.independent.co.uk/news/uk/politics/5g-coronavirus-phone-mast-attack-arson-conspiracy-theory-downing-street-a9450066.html.

Dheri, P. & Cobey, D. (2019). Lawful Access and Encryption in Canada: A Policy Framework Proposal. Retrieved February 2022, from http://www.canlii.org/t/sm6c.

DHS (United States Department of Homeland Security). (2021). *National Terrorism Advisory System Bulletin - January 27, 2021*. Washington (DC): DHS.

Di Meco, L. (2019). *#She Persisted: Women, Politics & Power in the New Media World*. Washington (DC): The Wilson Center.

Dias Oliva, T., Antonialli, D. M., & Gomes, A. (2021). Fighting hate speech, silencing drag queens? Artificial intelligence in content moderation and risks to LGBTQ voices online. *Sexuality & Culture*, *25*(2), 700-732.

Digital Rights Watch. (2021). Explainer: The Online Safety Bill. Retrieved November 2021, from https://digitalrightswatch.org.au/2021/02/11/explainer-the-online-safety-bill/.

Dinha, F. (2021). VPNs May Be Putting Users at Risk. Retrieved October 2022, from https://www.forbes.com/sites/forbestechcouncil/2021/06/08/vpns-may-be-putting-users-at-risk/?sh=29f73cfa6588.

Dizboni, A. & Leuprecht, C. (2020). Instruments and Arrangements Against Online Terrorism Relating to International Cooperation. In J. Vacca (Ed.), *Online Terrorist Propaganda, Recruitment, and Radicalization*. Boca Raton (FL): CRC Press.

Dodge, A. & Spencer, D. C. (2018). Online sexual violence, child pornography, or something else entirely? Police responses to non-consensual intimate image sharing among youth. *Social & Legal Studies*, *27*(5), 636-657.

Dodge, A. (2019). Nudes are forever: Judicial interpretations of digital technology's impact on "revenge porn". *Canadian Journal of Law and Society 34*(1), 121-143.

Dodge, A., Spencer, D., Ricciardelli, R., & Ballucci, D. (2019). "This isn't your father's police force": Digital evidence in sexual assault investigations. *Australian & New Zealand Journal of Criminology*, *52*(4), 499-515.

Doffman, Z. (2020). Ashley Madison Hack Returns to 'Haunt' its Victims: 32 Million Users Now Watch and Wait. Retrieved May 2022, from https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/.

DOJ (United States Department of Justice). (2019a). Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton. Retrieved January 2022, from https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

DOJ (United States Department of Justice). (2019b). Joint US-EU Statement on Electronic Evidence Sharing Negotiations. Retrieved January 2022, from https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

DOJ (United States Department of Justice). (2022a). CLOUD Act Resources. Retrieved January 2022, from https://www.justice.gov/dag/cloudact.

DOJ (United States Department of Justice). (2022b). United States and Canada Welcome Negotiations of a CLOUD Act Agreement. Retrieved May 2022, from https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.

Dolny, T. (2021). Finding needles in haystacks: Statutory reform recommendations for quasi-criminal insolvencies involving online money laundering. *Annual Review of Insolvency Law, 19*, 16.

Donovan, J. (2019). How Hate Groups' Secret Sound System Works. Retrieved January 2022, from https://www.theatlantic.com/ideas/archive/2019/03/extremists-understand-what-tech-platforms-have-built/585136/.

Douek, E. (2020). *The Rise of Content Cartels*. New York (NY): The Knight First Amendment Institute at Columbia University.

DRW (Digital Rights Watch). (2021). *Submission to the Department of Infrastructure, Transport, Regional Development and Communication on the Proposed Online Safety Bill 2020.* Melbourne, Australia: DRW.

Dubois, E. & Martin-Bariteau, F. (2020a). Citizenship in a Connected Canada. In E. Dubois & F. Martin-Bariteau (Eds.), *Citizenship in a Connected Canada: A Research and Policy Agenda.* Ottawa (ON): University of Ottawa Press.

Dubois, E. & Martin-Bariteau, F. (2020b). Next Steps for a Connected Canada. In E. Dubois & F. Martin-Bariteau (Eds.), *Citizenship in a Connected Canada: A Research and Policy Agenda.* Ottawa (ON): University of Ottawa Press.

Duncanson, S., Brinker, C., Twa, K., & O'Neill Sanger, M. (2021). Federal UNDRIP Bill Becomes Law. Retrieved April 2022, from https://www.osler.com/en/resources/regulations/2021/federal-undrip-bill-becomes-law.

Dunn, S. & Petricone-Westwood, A. (2018). *More than "Revenge Porn": Civil Remedies for the Non-Consensual Distribution of Intimate Images.* Paper presented at 38th Civil Litigation Conference, Mont-Tremblant, QC.

Dupont, B. (2016). La gouvernance polycentrique du cybercrime: Les réseaux fragmentés de la coopération internationale. *Cultures & Conflits*(102), 95-120.

Dupont, B. (2019). The Ecology of Cybercrime. In R. Leukfeldt & T. J. Holt (Eds.), *The Human Factor of Cybercrime* (1st ed.). Abingdon, United Kingdom: Routledge.

Dupont, B. (2021). La police et la prévention de la cybercriminalité. In B. Dupont, A. Amicelle, R. Boivin, F. Fortin & S. Tanner (Eds.), *L'avenir du travail policier*. Montréal (QC): Les Presses de l'Université de Montréal.

Durrani, T., Silcoff, S., & O'Kane, J. (2022). Emergencies Act Won't Stop Protest Funding, Crypto CEO Says. Retrieved March 2022, from https://www.theglobeandmail.com/business/article-emergencies-act-wont-stop-protest-funding-crypto-ceo-says/.

Dwoskin, E., Whalen, J., & Cabato, R. (2019). Content Moderators at YouTube, Facebook and Twitter See the Worst of the Web — and Suffer Silently. Retrieved December 2022, from https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/.

Dwoskin, E., Oremus, W., Timberg, C., & Tiku, N. (2021a). Racists and Taliban Supporters Have Flocked to Twitter's New Audio Service After Executives Ignored Warnings. Retrieved June 2022, from https://www.washingtonpost.com/technology/2021/12/10/twitter-turmoil-spaces/.

Dwoskin, E., Tiku, N., & Timberg, C. (2021b). Facebook's Race-Blind Practices Around Hate Speech Came at the Expense of Black Users, New Documents Show. Retrieved December 2022, from https://www.washingtonpost.com/technology/2021/11/21/facebook-algorithm-biased-race/.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., . . . Spreng, R. N. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Psychological Sciences*, *75*(3), 522-533.

EC (European Commission). (2022a). The Digital Services Act Package. Retrieved October 2022, from https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

EC (European Commission). (2022b). Digital Services Act: Commission Welcomes Political Agreement on Rules Ensuring a Safe and Accountable Online Environment. Retrieved June 2022, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.

EC (European Commission). (n.d.). Do We Always Have to Delete Personal Data if a Person Asks? Retrieved October 2022, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en.

Edmonds, J. & Flahault, A. (2021). Refugees in Canada during the First Wave of the COVID-19 Pandemic. *International Journal of Environmental Research and Public Health*, *18*(3), 947.

Éducaloi. (2022). Protecting Seniors from Exploitation and Abuse. Retrieved January 2022, from https://educaloi.qc.ca/en/capsules/protecting-seniors-from-exploitation-abuse/.

Edwards, G., Christensen, L. S., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends & Issues in Crime and Criminal Justice, 636*, ti78313.

Edwards, L. (2018). Data Protection: Enter the General Data Protection Regulation. In L. Edwards (Ed.), *Law, Policy and the Internet*. London, United Kingdom: Hart Publishing.

EFF (Electronic Frontier Foundation). (2017). *Street-Level Surveillance: Face Recognition*. San Francisco (CA): EFF.

Enders, A. M., Uscinski, J. E., Seelig, M. I., Klofstad, C. A., Wuchty, S., Funchion, J. R., . . . Stoler, J. (2021). The relationship between social media use and beliefs in conspiracy theories and misinformation. *Political Behavior, Jul 7*, 1-24.

EP (European Parliament). (2022). Digital Services Act: Regulating Platforms for A Safer Online Space for Users. Retrieved October 2022, from https://www.europarl.europa.eu/news/en/press-room/20220114IPR21017/digital-services-act-regulating-platforms-for-a-safer-online-space-for-users.

Equality Now. (2019). The Role of Technology on Facilitating and Addressing Sex Trafficking. Retrieved August 2021, from https://www.equalitynow.org/vienna_may2019.

eSafety Commissioner. (2021a). *Online Safety Act 2021 Fact Sheet*. Sydney, Australia: Government of Australia.

eSafety Commissioner. (2021b). *Office of the eSafety Commissioner Annual Report 2020-21*. Canberra, Australia: Government of Australia.

eSafety Commissioner. (2022a). New Online Safety Laws Come Into Force. Retrieved October 2022, from https://www.esafety.gov.au/newsroom/media-releases/new-online-safety-laws-come-force.

eSafety Commissioner. (2022b). What Is Serious Online Abuse? Retrieved January 2022, from https://www.esafety.gov.au/report/what-is-serious-online-abuse.

eSafety Commissioner. (n.d.-a). Our Legislative Functions. Retrieved July 2021, from https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions.

eSafety Commissioner. (n.d.-b). Report to the eSafety Commissioner. Retrieved January 2022, from https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-esafety-commissioner.

ESDC (Employment and Social Development Canada). (2019). *What We Heard Report: Financial Crimes and Harms Against Seniors*. Ottawa (ON): ESDC.

ETHI (Standing Committee on Access to Information, Privacy and Ethics). (2018). *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*. Ottawa (ON): House of Commons of Canada.

ETHI (Standing Committee on Access to Information, Privacy and Ethics). (2021). *Ensuring the Protection of Privacy and Reputation on Platforms such as Pornhub*. Ottawa (ON): House of Commons of Canada.

ETHI (Standing Committee on Access to Information, Privacy and Ethics). (2022). *Evidence. Number 031. Monday, August 8, 2022*. Ottawa (ON): House of Commons Canada.

Etteldorf, C. (2021). October Entry into Force for NetzDG Appeal Procedure. Retrieved April 2022, from http://merlin.obs.coe.int/article/9334.

Etzioni, A. (2005). The Limits of Privacy. In A. I. Cohen & C. H. Wellman (Eds.), *Contemporary Debates in Applied Ethics*. Malden (MA): Blackwell Publishing.

EU (European Union). (2000). *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market*. Brussels, Belgium: European Parliament and Council of the European Union.

EU (European Union). (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. Brussels, Belgium: European Parliament and Council of the European Union.

EU (European Union). (2020). *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*. Brussels, Belgium: European Parliament and Council of the European Union.

Europol (European Union Agency for Law Enforcement Cooperation). (2020a). *Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic*. The Hague, Netherlands: Europol.

Europol (European Union Agency for Law Enforcement Cooperation). (2020b). *Internet Organised Crime Threat Assessment*. The Hague, Netherlands: Europol.

Europol (European Union Agency for Law Enforcement Cooperation). (2022). *Cryptocurrencies: Tracing the Evolution of Criminal Finances*. The Hague, Netherlands: Europol.

Evans, M., Kessler, D., Lennon, J., & Ross, S. (2019). US CLOUD Act and International Privacy. Retrieved October 2022, from https://www.dataprotectionreport.com/2019/08/u-s-cloud-act-and-international-privacy/.

Facebook – Meta Transparency Center. (2021). Hate Speech. Retrieved November 2021, from https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook/#content-actioned.

Facebook. (2020a). Preventing Unwanted Contacts and Scams in Messenger. Retrieved April 2022, from https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/.

Facebook. (2020b). Meta: Keeping People Safe and Informed About the Coronavirus. Retrieved July 2021, from https://about.fb.com/news/2020/12/coronavirus/.

Facebook Canada. (2021). *2021 Canadian Election Integrity Initiative: Facebook's Canadian Approach*. Toronto (ON): Facebook Canada.

Facebook Oversight Board. (2019). *Oversight Board Charter*. Menlo Park (CA): Facebook.

Facebook Oversight Board. (2021). *Case Decision 2021-001-FB-FBR*. Menlo Park (CA): Facebook.

Faddoul, M., Chaslot, G., & Farid, H. (2020). A longitudinal analysis of YouTube's promotion of conspiracy videos. *ArXiv*, 2003.03318.

Faife, C. (2022). Security Experts Say New EU Rules Will Damage WhatsApp Encryption. Retrieved May 2022, from https://www.theverge.com/2022/3/28/23000148/eu-dma-damage-whatsapp-encryption-privacy.

Faris, R., Ashar, A., Gasser, U., & Joo, D. (2016). *Understanding Harmful Speech Online*. Vol. No. 2016-21. Cambridge (MA): Berkman Klein Center for Internet and Society at Harvard University.

Farrell, H. & Newman, A. L. (2019). *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton (NJ): Princeton University Press.

FBI (Federal Bureau of Investigation). (2017). Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay. Retrieved August 2021, from https://www.fbi.gov/news/stories/alphabay-takedown.

FBI (Federal Bureau of Investigation). (2022). Science and Technology Branch. Retrieved February 2022, from https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch.

FCAC (Financial Consumer Agency of Canada). (2019). Protection Against Unauthorized Credit and Debit Transactions. Retrieved May 2022, from https://www.canada.ca/en/financial-consumer-agency/services/rights-responsibilities/protection-unauthorized-transactions.html.

Feinberg, A. (2017). This Is the Daily Stormer's Playbook. Retrieved January 2022, from https://www.huffpost.com/entry/daily-stormer-nazi-style-guide_n_5a2ece19e4b0ce3b344492f2.

Fenwick, J. (2021). Twitter Says Online Safety Bill Needs More Clarity. Retrieved November 2021, from https://www.bbc.com/news/uk-politics-59010723.

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York (NY): New York University Press.

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). Precept: A framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, *21*(2), 257-290.

FIN (Department of Finance Canada). (2022). Canada Invokes the Emergencies Act to Limit Funding of Illegal Blockades and Restore Public Order. Retrieved March 2022, from https://www.canada.ca/en/department-finance/news/2022/02/canada-invokes-the-emergencies-act-to-limit-funding-of-illegal-blockades-and-restore-public-order.html.

FINA (Standing Committee on Finance). (2018). *Confronting Money Laundering and Terrorist Financing: Moving Canada Forward*. Ottawa (ON): House of Commons of Canada.

Finklea, K. (2021). *Law Enforcement and Technology: The "Lawful Access" Debate*. Washington (DC): Congressional Research Service.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). (2021a). *Safe Canadians, Secure Economy: Annual Report 2020-2021*. Ottawa (ON): FINTRAC.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). (2021b). What is a Suspicious Transaction Report? Retrieved August 2022, from https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). (2021c). Money Laundering and Terrorist Financing Indicators - Virtual Currency Transactions. Retrieved March 2022, from https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng.

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada). (2022). Mandate. Retrieved March 2022, from https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.

FJA (Office of the Commissioner for Federal Judicial Affairs Canada). (2022). Number of Federally Appointed Judges as of May 1, 2022. Retrieved May 2022, from https://www.fja.gc.ca/appointments-nominations/judges-juges-eng.aspx.

Fletcher, E. (2021). Cryptocurrency Buzz Drives Record Investment Scam Losses. Retrieved March 2022, from https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses.

Forrest, M. (2022). Canada's National Police Force Admits Use of Spyware to Hack Phones. Retrieved October 2022, from https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092.

Frankenfield, J. (2021). Virtual Currency. Retrieved March 2022, from https://www.investopedia.com/terms/v/virtual-currency.asp.

Frankenfield, J. (2022a). Digital Currency. Retrieved August 2022, from https://www.investopedia.com/terms/d/digital-currency.asp.

Frankenfield, J. (2022b). Cryptocurrency Explained With Pros and Cons for Investment. Retrieved August 2022, from https://www.investopedia.com/terms/c/cryptocurrency.asp.

Franks, M. A. (2018). Fearless speech. *First Amendment Law Review, 17*, 294-342.

Fraser, D. (2022). Most Key Participants in Ottawa Convoy Protest Not Yet Charged. Retrieved April 2022, from https://www.cbc.ca/news/canada/ottawa/convoy-protest-police-ottawa-freedom-trucks-occupation-1.6401510.

Freeman Law. (2022). What is a Tumbler, and is Cryptocurrency Tumbling Safe? Retrieved June 2022, from https://freemanlaw.com/what-is-a-tumbler-and-is-cryptocurrency-tumbling-safe/.

Frenkel, S. (2021). The Storming of Capitol Hill Was Organized on Social Media. Retrieved December 2022, from https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html.

Fry, L. W. & Berkes, L. J. (1983). The paramilitary police model: An organizational misfit. *Human Organization*, 42(3), 225-234.

FTC (Federal Trade Commission). (2022). *Social Media a Gold Mine for Scammers in 2021*. Washington (DC): FTC.

Funk, A. (2021). Q&A: Social Media Regulation and the Perils of Section 230 Reform. Retrieved April 2022, from https://freedomhouse.org/article/qa-social-media-regulation-and-perils-section-230-reform.

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security, 2015*(10), 5-12.

Gailey, A. & Haar, R. (2022). The Future of Cryptocurrency: 8 Experts Share Predictions for the Second Half of 2022. Retrieved November 2022, from https://time.com/nextadvisor/investing/cryptocurrency/future-of-cryptocurrency/.

Gallagher, A., Davey, J., & Hart, M. (2020). *The Genesis of a Conspiracy Theory: Key Trends in QAnon Activity Since 2017*. London, United Kingdom: Institute for Strategic Dialogue.

Gallagher, C. (2021). HSE Confirms Data of 520 Patients Published Online. Retrieved July 2022, from https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136.

Garry, A., Walther, S., Rukaya, R., & Mohammed, A. (2021). QAnon conspiracy theory: Examining its evolution and mechanisms of radicalization. *Journal for Deradicalization, 26*, 152-216.

Gaudette, T., Scrivens, R., & Venkatesh, V. (2020). The role of the Internet in facilitating violent extremism: Insights from former right-wing extremists. *Terrorism and Political Violence*, 1-18.

GC (Government of Canada). (1982). *Canadian Charter of Rights and Freedoms*. Ottawa (ON): GC.

GC (Government of Canada). (1985). *Criminal Code R.S.C 1985, c. C-46*. Ottawa (ON): GC.

GC (Government of Canada). (2000a). *Personal Information Protection and Electronic Documents Act*. Ottawa (ON): GC.

GC (Government of Canada). (2000b). *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. Ottawa (ON): GC

GC (Government of Canada). (2010). *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*. Ottawa (ON): GC.

GC (Government of Canada). (2011a). *Internet Child Pornography Reporting Regulations*. Ottawa (ON): GC.

GC (Government of Canada). (2011b). *An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service*. Ottawa (ON): GC.

GC (Government of Canada). (2014). *Bill C-13: An Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*. Ottawa (ON): GC.

GC (Government of Canada). (2018a). *Elections Modernization Act*. Ottawa (ON): GC.

GC (Government of Canada). (2018b). Chair's Statement: Security Ministers' Meeting. Retrieved May 2022, from https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-04-22-security_ministers-ministres_securite.aspx?lang=eng.

GC (Government of Canada). (2019a). Human Rights Treaties. Retrieved September 2022, from https://www.canada.ca/en/canadian-heritage/services/canada-united-nations-system/treaties.html.

GC (Government of Canada). (2019b). Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019: SOR/2019-240. Retrieved August 2022, from https://www.gazette.gc.ca/rp-pr/p2/2019/2019-07-10/html/sor-dors240-eng.html.

GC (Government of Canada). (2019c). Understanding Canada's Anti-Spam Legislation. Retrieved October 2022, from https://fightspam-combattrelepourriel.ised-isde.canada.ca/site/canada-anti-spam-legislation/en/understand-canadas-anti-spam-legislation/understand-canadas-anti-spam-legislation-sub/understanding-canadas-anti-spam-legislation.

GC (Government of Canada). (2019d). *Mutual Legal Assistance in Criminal Matters Act*. Ottawa (ON): GC.

GC (Government of Canada). (2020a). Guide to the Canadian Charter of Rights and Freedoms. Retrieved January 2022, from https://www.canada.ca/en/canadian-heritage/services/how-rights-protected/guide-canadian-charter-rights-freedoms.html#a3.

GC (Government of Canada). (2020b). *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations SOR/2002-184*. Ottawa (ON): GC.

GC (Government of Canada). (2020c). Fact Sheet: Digital Charter Implementation Act, 2020. Retrieved August 2021, from https://www.ic.gc.ca/eic/site/062.nsf/eng/00119.html.

GC (Government of Canada). (2020d). *Canada-United States-Mexico Agreement (CUSMA) - Chapter 19 - Digital Trade*. Ottawa (ON): GC.

GC (Government of Canada). (2021a). Modernizing Canada's Privacy Act. Retrieved February 2022, from https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html.

GC (Government of Canada). (2021b). Legal Definitions of Elder Abuse and Neglect. Retrieved January 2022, from https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/elder-aines/def/p211.html.

GC (Government of Canada). (2021c). When to Verify the Identity of Persons and Entities - Money Services Businesses and Foreign Money Services Businesses. Retrieved February 2022, from https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/client/msb-eng.

GC (Government of Canada). (2021d). Digital Currency. Retrieved September 2022, from https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html#toc4.

GC (Government of Canada). (2021e). Strengthening Canada's Anti-Money Laundering Regime Through Collaboration and Capacity Building. Retrieved June 2022, from https://www.canada.ca/en/public-safety-canada/news/2021/12/strengthening-canadas-anti-money-laundering-regime-through-collaboration-and-capacity-building.html.

GC (Government of Canada). (2021f). *Canada's Anti-Spam legislation (CASL) - Performance Measurement Report 2019-20*. Ottawa (ON): GC.

GC (Government of Canada). (2021g). Discussion Guide. Retrieved August 2021, from https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html.

GC (Government of Canada). (2021h). *Bill C-36, An Act to Amend the Criminal Code and the Canadian Human Rights Act and to Make Related Amendments to Another Act (Hate Propaganda, Hate Crimes and Hate Speech)*. Ottawa (ON): GC.

GC (Government of Canada). (2021i). Technical Paper. Retrieved August 2021, from https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html.

GC (Government of Canada). (2022a). Summary of Session Seven: Connection to Law Enforcement. Retrieved October 2022, from https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/summary-session-seven.html.

GC (Government of Canada). (2022b). CRTC Investigation Targets Dark Web Marketplace Vendors and Administrator. Retrieved May 2022, from https://www.canada.ca/en/radio-television-telecommunications/news/2022/01/crtc-investigation-targets-dark-web-marketplace-vendors-and-administrator.html.

GC (Government of Canada). (2022c). What We Heard: The Government's Proposed Approach to Address Harmful Content Online. Retrieved May 2022, from https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard.html#a1.

GC (Government of Canada). (2022d). Government of Canada Announces Expert Advisory Group on Online Safety. Retrieved April 2022, from https://www.canada.ca/en/canadian-heritage/news/2022/03/government-of-canada-announces-expert-advisory-group-on-online-safety0.html.

GC (Government of Canada). (2022e). Remarks by the Deputy Prime Minister and Minister of Finance Regarding the Emergencies Act. Retrieved March 2022, from https://www.canada.ca/en/department-finance/news/2022/02/remarks-by-the-deputy-prime-minister-and-minister-of-finance-regarding-the-emergencies-act.html.

GC (Government of Canada). (2022f). *2022 Budget: A Plan to Grow Our Economy and Make Life More Affordable*. Ottawa (ON): GC.

Geist, M. (2021a). Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation. Retrieved November 2021, from https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/.

Geist, M. (2021b, August 23). "They Just Seemed Not to Listen to Any of Us" - Cynthia Khoo on the Canadian Government's Online Harms Consultation, *Law Bytes*.

Geist, M. (2021c). *Government of Canada Consultation on the Proposed Approach to Address Harmful Content Online*. Ottawa (ON): University of Ottawa, Faculty of Law.

Geist, M. (2022a). Not Ready for Prime Time: Why Bill C-11 Leaves the Door Open to CRTC Regulation of User Generated Content. Retrieved February 2022, from https://www.michaelgeist.ca/2022/02/not-ready-for-prime-time/.

Geist, M. (2022b). The Groundhog Day Privacy Bill: The Government Waited Months to Bring Back Roughly the Same Privacy Plan?! Retrieved October 2022, from https://www.michaelgeist.ca/2022/06/the-groundhog-day-privacy-bill/.

German Bundestag. (2017). *Act to Improve Enforcement of the Law in Social Networks*. Berlin, Germany: German Bundestag.

Ghaffary, S. (2021). Facebook Will Push you to Read Articles Before you Share Them. Retrieved June 2021, from https://www.vox.com/2021/5/10/22429240/facebook-prompt-users-read-articles-before-sharing.

Ghosh, D. (2021a). Are We Entering a New Era of Social Media Regulation? Retrieved October 2022, from https://hbr.org/2021/01/are-we-entering-a-new-era-of-social-media-regulation.

Ghosh, S. (2021b). Online Misinformation About the US Election Fell 73% After Trump's Social Media Ban. Retrieved December 2022, from https://www.businessinsider.com/misinformation-fell-73-after-trump-was-banned-across-social-media-2021-1.

GIFCT (Global Internet Forum to Counter Terrorism). (2020). *GIFCT Transparency Report July 2020*. Washington (DC): GIFCT.

Gill, L., Israel, T., & Parsons, C. (2018). *Shining a Light on the Encryption Debate: A Canadian Field Guide*. Toronto (ON): The Citizen Lab and The Canadian Internet Policy & Public Interest Clinic.

Gill, L. (2020). *Legal Aspects of Hate Speech in Canada*. Ottawa (ON): Public Policy Forum.

Gilmore, R. (2022). Liberals Say New Online Streaming Bill Won't Hurt Free Speech - But Some Remain Skeptical. Retrieved February 2022, from https://globalnews.ca/news/8592505/online-streaming-bill-c-11-free-speech/.

Global Commission on Internet Governance. (2016). *One Internet*. Waterloo (ON): Centre for International Governance Innovation, Chatham House, The Royal Institute of International Affairs.

Goldfinger, D. (2019). OPP Opens Centre for Cyber Operations. Retrieved February 2022, from https://globalnews.ca/news/5970566/opp-cyber-operations-centre/.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica (CA): RAND Corporation.

Goodwin, J. (2020). Mastercard, Visa and Discover Cut Ties with Pornhub Following Allegations of Child Abuse. Retrieved October 2020, from https://www.cnn.com/2020/12/14/business/mastercard-visa-discover-pornhub/index.html.

Google. (2021). Google Transparency Report: YouTube Community Guidelines Enforcement. Retrieved November 2021, from https://transparencyreport.google.com/youtube-policy/removals?hl=en&channels_by_reason=period.

Gov. of Australia (Government of Australia). (2010). *Australia's Constitution*. Canberra, Australia: Gov. of Australia.

Gov. of Australia (Government of Australia). (2015). *Enhancing Online Safety Act 2015*. Canberra, Australia: Gov. of Australia.

Gov. of Australia (Government of Australia). (2017). *Enhancing Online Safety for Children Amendment Bill 2017*. Canberra, Australia: Gov. of Australia.

Gov. of Australia (Government of Australia). (2018). *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018*. Canberra, Australia: Gov. of Australia.

Gov. of Australia (Government of Australia). (2019). *Sharing of Abhorrent Violent Material Act Fact Sheet*. Canberra, Australia: Gov. of Australia.

Gov. of Germany (Government of Germany). (1998). *German Criminal Code*. Berlin, Germany: Gov. of Germany.

Gov. of MB (Government of Manitoba). (2014). Child Sexual Exploitation. Retrieved October 2022, from https://gov.mb.ca/fs/cfsmanual/1.3.5.html#_Reporting_and_Investigating_1.

Gov. of MB (Government of Manitoba). (2022). *The Child and Family Services Act*. Winnipeg (MB): Gov. of MB.

Gov. of NS (Government of Nova Scotia). (2008). Child Pornography Reporting Act. Retrieved October 2022, from https://nslegislature.ca/sites/default/files/legc/statutes/childpor.htm.

Gov. of NS (Government of Nova Scotia). (2022). *Report on the Review of the Intimate Images and Cyber-Protection Act*. Halifax (NS): Gov. of NS.

Gov. of NZ (Government of New Zealand). (1993). *Films, Videos, and Publications Classification Act 1993*. Wellington, New Zealand: Gov. of NZ.

Gov. of NZ (Government of New Zealand). (2015). *Harmful Digital Communications Act 2015*. Wellington, New Zealand: Gov. of NZ.

Gov. of NZ (Government of New Zealand). (2021). *Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Act 2021*. Wellington, New Zealand: Gov. of NZ.

Gov. of NZ (Government of New Zealand). (2022). *Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Act*. Wellington, New Zealand: Gov. of NZ.

Gov. of QC (Government of Quebec). (1976). *Charter of Human Rights and Freedoms*. Québec (QC): Gov. of QC.

Gov. of QC (Government of Quebec). (1982). *Act respecting Access to Documents held by Public Bodies and the Protection of Personal Information*. Québec (QC): Gov. of QC.

Gov. of QC (Government of Quebec). (1991). *Civil Code of Quebec*. Québec (QC): Gov. of QC.

Gov. of QC (Government of Quebec). (2021). *Bill 64: An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information*. Quebéc (QC): Gov. of QC.

Gov. of the US (Government of the United States). (2018). *Public Law 115-164 (SESTA/FOSTA)*. Washington (DC): Gov. of the US.

Gov. of the US (Government of the United States). (n.d.-a). *18 U.S. Code § 373 - Solicitation to Commit a Crime of Violence*. Washington (DC): Gov. of the US.

Gov. of the US (Government of the United States). (n.d.-b). *18 U.S. Code § 2421A - Promotion or Facilitation of Prostitution and Reckless Disregard of Sex Trafficking*. Washington (DC): Gov. of the US.

Gov. of the US (Government of the United States). (n.d.-c). *18 U.S. Code Chapter 110 - Sexual Exploitation and Other Abuse of Children*. Washington (DC): Gov. of the US.

Gov. of UK (Government of the United Kingdom). (2019). *Online Harms White Paper.* London, United Kingdom: Secretary of State for Digital, Culture, Media & Sport; Secretary of State for the Home Department.

Gov. of UK (Government of the United Kingdom). (2021a). *Online Safety Bill. Explanatory Notes*. London, United Kingdom: Gov. of UK.

Gov. of UK (Government of the United Kingdom). (2021b). *Draft Online Safety Bill*. London, United Kingdom: Gov. of UK.

Gov. of UK (Government of the United Kingdom). (2021c). National Cyber Strategy 2022 Retrieved January 2022, from https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-force.

Gov. of UK (Government of the United Kingdom). (2022). *Online Safety Bill: Factsheet*. London, United Kingdom: Department for Digital, Culture, Media & Sport.

Grant, I. (2015). Intimate partner criminal harassment through a lens of responsibilization. *Osgoode Hall Law Journal, 52*(2), 552-600.

Graves, Z. (2021). The Promise and Perils of Interoperability. Retrieved October 2022, from https://lincolnpolicy.org/2021/the-promise-and-perils-of-interoperability/.

Greene, V. S. (2019). "Deplorable" satire: Alt-right memes, white genocide tweets, and redpilling normies. *Studies in American Humor, 5*(1), 31-69.

Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E., . . . Wilson, R. C. (2021). Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. *The Journals of Gerontology: Series B, 76*(9), 1711-1715.

Grygiel, J. & Brown, N. (2019). Are social media companies motivated to be good corporate citizens? Examination of the connection between corporate social responsibility and social media safety. *Telecommunications Policy, 43*(5), 445-460.

Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences, 117*(27), 15536-15545.

Guliani, N. S. & Shah, N. (2018). The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them. Retrieved April 2022, from https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

Gullo, K. & Rodriguez, K. (2021). EFF to Council of Europe: Flawed Cross Border Police Surveillance Treaty Needs Fixing - Here Are Our Recommendations to Strengthen Privacy and Data Protections Across the World. Retrieved April 2022, from https://www.eff.org/deeplinks/2021/08/eff-council-europe-flawed-cross-border-police-surveillance-treaty-needs-fixing.

Gupta, H. & Taneja, H. (2018). WhatsApp has a Fake News Problem - That Can Be Fixed Without Breaking Encryption. Retrieved July 2021, from https://www.cjr.org/tow_center/whatsapp-doesnt-have-to-break-encryption-to-beat-fake-news.php.

Ha-Redeye, O. (2021). Canadian Courts Assume Jurisdiction over Twitter Defamation. Retrieved April 2022, from https://canliiconnects.org/en/commentaries/73241.

Haggart, B. & Tusikov, N. (2021). How "Free Speech" Kills Internet Regulation Debates: Part Two. Retrieved October 2022, from https://www.cigionline.org/articles/how-free-speech-kills-internet-regulation-debates/.

Hameleers, M., Powell, T. E., Van Der Meer, T. G. L. A., & Bos, L. (2020). A picture paints a thousand lies? The effects and mechanisms of multimodal disinformation and rebuttals disseminated via social media. *Political Communication, 37*(2), 281-301.

Hammond, S. & Ehret, T. (2021). *Cryptos On the Rise*. Eagan (MN): Thomson Reuters.

Hango, D. (2016). *Cyberbullying and Cyberstalking Among Internet Users Aged 15 to 29 in Canada*. Ottawa (ON): Statistics Canada.

Hao, K. (2021). This Is How We Lost Control of Our Faces. Retrieved April 2022, from https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519-536.

Harkin, D. & Whelan, C. (2019). Exploring the implications of 'low visibility' specialist cyber-crime units. *Australian & New Zealand Journal of Criminology, 52*(4), 578-594.

Harmon, E. (2017). Sex Trafficking Experts Say SESTA Is the Wrong Solution. Retrieved March 2022, from https://www.eff.org/deeplinks/2017/10/sex-trafficking-experts-say-sesta-wrong-solution.

Harris, K. (2021). Hundreds Charged Under New Zealand's Harmful Digital Communications Act. Retrieved November 2021, from https://www.nzherald.co.nz/nz/hundreds-charged-under-new-zealands-harmful-digital-communications-act/QA23N4Y4724452UDQKNODTTXXY/.

Harris, T. (2017). How a Handful of Tech Companies Control Billions of Minds Everyday. Retrieved August 2021, from https://www.ted.com/talks/tristan_harris_how_a_handful_of_tech_companies_control_billions_of_minds_every_day?language=en.

Hart, M., Davey, J., Maharasingam-Shah, E., O'Connor, C., & Gallagher, A. (2021). *An Online Environmental Scan of Right-Wing Extremism in Canada*. London, United Kingdom: Institute for Strategic Dialogue.

Hartzog, W. (2018). *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge (MA): Harvard University Press.

Hassan, G., Brouillette-Alarie, S., Alava, S., Frau-Meigs, D., Lavoie, L., Fetiu, A., . . . Rousseau, C. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. *International Journal of Developmental Science*, *12*(1-2), 71-88.

Hatta, M. (2020). Deep web, dark web, dark net: A taxonomy of "hidden" internet. *Annals of Business Administrative Science*, *19*, 277-292.

Haugen, F. (2021). *Statement of Frances Haugen*. Sub-Committee on Consumer Protection, Product Safety, and Data Security: United States Senate Committee on Commerce, Science and Transportation, United States Senate.

HCA (High Court of Australia). (2019). *Comcare v Banerji [2019] HCA 23*. Canberra, Australia: HCA.

Heer, T., Heath, C., Girling, K., & Bugg, E. (2021). *Misinformation in Canada: Research and Policy Options*. Ottawa (ON): Evidence for Democracy.

Heldt, A. (2019). Reading between the lines and the numbers: An analysis of the first NetzDG reports. *Internet Policy Review*, *8*(2), 1-18.

Henry, C. S., Huynh, K. P., & Welte, A. (2018). *2017 Methods-of-Payment Survey Report*. Ottawa (ON): Bank of Canada.

Henry, N. & Powell, A. (2016). Sexual violence in the digital age: The scope and limits of criminal law. *Social & Legal Studies*, *25*(4), 397-418.

Hill, K. (2020). The Secretive Company That Might End Privacy as We Know It. Retrieved October 2022, from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hill, K. (2021). Clearview AI's Facial Recognition App Called Illegal in Canada. Retrieved November 2022, from https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html?

Hillier, L., Jones, T., Monagle, M., Overton, N., Gahan, L., Blackman, J., & Mitchell, A. (2010). *Writing Themselves in 3: The Third National Study on the Sexual Health and Wellbeing of Same Sex Attracted and Gender Questioning Young People*. Vol. 3. Melbourne, Australia: Australian Research Centre in Sex, Health and Society, La Trobe University.

Hitchcock, A., Holmes, R., & Sundorph, E. (2017). *Bobbies on the Net: A Police Workforce for the Digital Age*. London, United Kingdom: Reform.

HMIC (Her Majesty's Inspectorate of Constabulary). (2015). *Real Lives, Real Crime*. London, United Kingdom: HMIC.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2019). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society, 29*(8), 906-921.

Horta Ribeiro, M., Jhaver, S., Zannettou, S., Blackburn, J., Stringhini, G., De Cristofaro, E., & West, R. (2021). Do platform migrations compromise content moderation? Evidence from r/the_donald and r/incels. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW2), 316.

Horwitz, J. & Scheck, J. (2021). Facebook Increasingly Suppresses Political Movements It Deems Dangerous. Retrieved December 2022, from https://www.wsj.com/articles/facebook-suppresses-political-movements-patriot-party-11634937358.

Hours, F. (2022). Clap de fin pour les élèves de la toute première e-promotion de l'école de gendarmerie de Chaumont. Retrieved June 2022, from https://www.gendinfo.fr/actualites/2022/clap-de-fin-pour-les-eleves-de-la-toute-premiere-e-promotion-de-l-ecole-de-gendarmerie-de-chaumont.

House of Commons of Canada. (2021). *Bill C-10. An Act to Amend the Broadcasting Act and to Make Related and Consequential Amendments to Other Acts*. Ottawa (ON): House of Commons of Canada.

House of Commons of Canada. (2022). *Bill C-27: An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts*. Ottawa (ON): House of Commons of Canada.

House of Commons of Canada. (n.d.). Members of Parliament. Retrieved November 2022, from https://www.ourcommons.ca/Members/en/search?parliament=43&province=NT.

HRW (Human Rights Watch). (2018). Germany: Flawed Social Media Law. Retrieved July 2021, from https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice, 13*(1), 81-97.

Huey, L. & Ferguson, L. (2022). *Another Digital Divide: Cybersecurity in Indigenous Communities*. London (ON): Western University.

Hunt, A. (2020). Why Our Online Harm Legislation Isn't Working. Retrieved November 2021, from https://adls.org.nz/Story?Action=View&Story_id=225.

Hutchinson, J., Amarasingam, A., Scrivens, R., & Ballsun-Stanton, B. (2021). Mobilizing extremism online: Comparing Australian and Canadian right-wing extremist groups on Facebook. *Behavioral Sciences of Terrorism and Political Aggression*, 1903064.

Ibrahim, D. (2021). *Trafficking in persons in Canada, 2019*. Ottawa (ON): Canadian Centre for Justice and Community Safety Statistics.

ICO (Information Commissioner's Office). (2022). *Enforcement Notice*. Wilmslow, United Kingdom: ICO.

Igo, S. (2018). *The Known Citizen: A History of Privacy in Modern America*. Cambridge (MA): Harvard University Press.

Ingram, D. (2021). A Tracking Device Made by Apple is Showing up in Suspected Crimes. Retrieved March 2022, from https://www.nbcnews.com/news/apple-airtag-showing-up-crimes-rcna9416.

INHOPE (Association of Internet Hotline Providers). (2020). *Annual Report 2020*. Amsterdam, Netherlands: INHOPE Association.

INTERPOL (International Criminal Police Organization). (2021). *National Cybercrime Strategy Guidebook*. Lyon, France: INTERPOL.

Ipsos & NPR. (2020). *Public Poll Findings and Methodology: More Than 1 in 3 Americans Believe a 'Deep State' is Working to Undermine Trump*. Washington (DC): Ipsos & NPR.

Ipsos. (2021). *Online Harm in Journalism*. Toronto (ON): Ipsos.

IRCC (Immigration, Refugees and Citizenship Canada). (2021a). What Kinds of Fraud Should Newcomers to Canada Watch out for? Retrieved November 2021, from https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/newcomers.html.

IRCC (Immigration, Refugees and Citizenship Canada). (2021b). I Received Threats from Someone Who Says They Are from the Immigration Department. Is it a Scam? Retrieved February 2022, from https://www.cic.gc.ca/english/helpcentre/answer.asp?qnum=1218&top=31.

ISED (Innovation, Science and Economic Development Canada). (2019). *Canada's Digital Charter in Action: A Plan by Canadians for Canadians*. Ottawa (ON): ISED.

ITV News. (2020). Thousands of Digital Devices Awaiting Analysis by Police Investigators. Retrieved May 2022, from https://www.itv.com/news/2020-04-22/thousands-of-digital-devices-awaiting-analysis-by-police-investigators.

IWF (Internet Watch Foundation). (2020). The Annual Report 2020: 2020 Trends and Data. Retrieved August 2021, from https://annualreport2020.iwf.org.uk/trends.

Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S., & Kaufmann, Z. (2021). *Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online*. Washington (DC): Wilson Center, Science and Technology Innovation Program.

Jeney, P. (2015). *Combatting Child Sexual Abuse Online*. Brussels, Belgium: European Parliament.

Jolley, D., Douglas, K. M., Leite, A. C., & Schrader, T. (2019). Belief in conspiracy theories and intentions to engage in everyday crime. *British Journal of Social Psychology, 58*(3), 534-549.

Jolley, D., Meleady, R., & Douglas, K. M. (2020). Exposure to intergroup conspiracy theories promotes prejudice which spreads across groups. *British Journal of Psychology, 111*(1), 17-35.

Jolley, D. & Paterson, J. L. (2020). Pylons ablaze: Examining the role of 5G COVID-19 conspiracy beliefs and support for violence. *British Journal of Social Psychology*, *59*(3), 628-640.

Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does media literacy help identification of fake news? Information literacy helps, but other literacies don't. *American Behavioral Scientist*, *65*(2), 371-388.

Jones, M. L. & Kaminski, M. E. (2021). An American's guide to the GDPR. *Denver Law Review*, *98*(1), 93-128.

Judson, E. (2022). *The Online Safety Bill: Demos Position Paper*. London, United Kingdom: Demos.

JUS (Department of Justice Canada). (2010). Elder Abuse - Financial Fraud by Strangers. Retrieved January 2022, from https://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/eldfr-ainfr/eldfr-ainfr.html.

JUS (Department of Justice Canada). (2012). *A Handbook for Police and Crown Prosecutors on Criminal Harassment*. Ottawa (ON): JUS.

JUS (Department of Justice Canada). (2019). Legislative Background: An Act to Amend the Criminal Code, the Youth Criminal Justice Act and Other Acts and to Make Consequential Amendments to Other Acts, as Enacted (Bill C-75 in the 42nd Parliament). Retrieved March 2022, from https://www.justice.gc.ca/eng/rp-pr/csj-sjc/jsp-sjp/c75/p2.html.

JUS (Department of Justice Canada). (2020). *Evaluation of the Investigative Powers for the 21st Century Initiative*. Ottawa (ON): JUS.

JUS (Department of Justice Canada). (2021). What is Human Trafficking? Retrieved March 2022, from https://www.justice.gc.ca/eng/cj-jp/tp/what-quoi.html.

JUST (Standing Committee on Justice and Human Rights). (2019). *Taking Action to End Online Hate: Report of the Standing Committee on Justice and Human Rights, 42nd Parliament, 1st Session*. Ottawa (ON): House of Commons of Canada.

Justiz Online. (2022). Gericht entscheidet über Eilanträge von Google und Meta: Netzwerkdurchsetzungsgesetz verstößt teilweise gegen Unionsrecht. Retrieved April 2022, from https://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/05_01032022/index.php.

Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J., & Kompatsiaris, I. (2016). OSINT and the Dark Web. In B. Akhgar, P. S. Bayerl & F. Sampson (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation*. Cham, Switzerland: Springer International Publishing Ag.

Kan, M. (2020). Pornhub Purges 10 Million Videos After Losing Credit Card Support. Retrieved October 2020, from https://www.pcmag.com/news/pornhub-purges-10-million-videos-after-losing-credit-card-support.

Kanstrén, T. (2021). Mapping Ring Signatures and Stealth Addresses in Monero. Retrieved August 2022, from https://medium.com/coinmonks/mapping-ring-signatures-and-stealth-addresses-in-monero-a5543a434684.

Karadeglija, A. (2022). Regulating Cryptocurrency Under Emergencies Act Not as Clear as Freeland Suggests. Retrieved March 2022, from https://nationalpost.com/news/politics/regulating-cryptocurrency-under-emergencies-act-not-as-clear-as-freeland-suggests.

Karasavva, V. & Noorbhai, A. (2021). The real threat of deepfake pornography: A review of Canadian policy. *Cyberpsychology, Behavior, and Social Networking*, *24*(3), 203-209.

Keatinge, T., Carlisle, D., & Keen, F. (2018). *Virtual Currencies and Terrorist Financing: Assessing The Risks and Evaluating Responses*. Brussels, Belgium: European Parliament.

Keller, D. (2021). Empirical Evidence of Over-Removal by Internet Companies Under Intermediary Liability Laws: An Updated List. Retrieved November 2021, from http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

Kendrick, L. (2012). *Speech, Intent and the Chilling Effect*. Vol. No. 2012-37: Public Law and Legal Theory Research Paper Series. Charlottesville (VA): University of Virginia School of Law.

Kenyon, M. (2021). Bill C-11 Explained. Retrieved July 2021, from https://citizenlab.ca/2021/04/bill-c-11-explained/.

Kerr, I. & McGill, J. (2007). Emanations, snoop dogs and reasonable expectations of privacy. *Criminal Law Quarterly*, *52*(3), 392-431.

Kerr, I. & Barrigar, J. (2012). Privacy, Identity and Anonymity. In K. Ball, K. Haggerty & D. Lyon (Eds.), *International Handbook of Surveillance Studies*. London, United Kingdom: Routledge.

Ketchum, A. (2020). *Report on the State of Resources Provided to Support Scholars Against Harassment, Trolling, and Doxxing While Doing Public Media Work and How University Media Relations Offices/Newsrooms Can Provide Better Support*. Montréal (QC): Medium.

Kethineni, S. & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review*, *30*(3), 325-344.

Khan, I. (2021). *Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Vol. A/HRC/47/25. Geneva, Switzerland: United Nations Human Rights Council.

Khan, R. & Ali Hakami, T. (2022). Cryptocurrency: Usability perspective versus volatility threat. *Journal of Money and Business*, *2*(1), 16-28.

Khoo, B., Phan, R. C. W., & Lim, C. H. (2021). Deepfake attribution: On the source identification of artificially generated images. *WIREs Data Mining and Knowledge Discovery*.

Khoo, C., Robertson, K., & Deibert, R. (2019). *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*. Toronto (ON): Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto.

Khoo, C. (2021). *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence*. Toronto (ON): Women's Legal Education & Action Fund.

Kiedrowski, J., Melchers, R.-F., Ruddell, R., & Petrunik, M. (2015). *The Civilianization of Police in Canada*. Ottawa (ON): Public Safety Canada.

Klonick, K. (2018). The New Governors: The people, rules, and processes governing online speech. *Harvard Law Review, 131*, 1598-1670.

Klonick, K. (2020). The Facebook Oversight Board: Creating an independent institution to adjudicate online free expression. *The Yale Law Journal, 129*(2418), 2418-2499.

Klosowski, T. (2020). Facial Recognition Is Everywhere. Here's What We Can Do About It. Retrieved April 2022, from https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

Koczerginski, M. (2021). Cyber Justice: Ontario Court Recognizes New Tort of Internet Harassment. Retrieved June 2022, from https://mcmillan.ca/insights/cyber-justice-ontario-court-recognizes-new-tort-of-internet-harassment/.

Koepke, L., Weil, E., Janardan, U., Dada, T., & Harlan, Y. (2020). *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*. Washington (DC): Upturn.

Kong, J., Ip, J., Huang, C., & Lin, K. (2021). *One Year of Racist Attacks: Anti-Asian Racism Across Canada One Year into the COVID-19 Pandemic*. Toronto (ON): Chinese Canadian National Council Toronto Chapter.

Kostelac, C. A. (2008). *The Changing Face of Police Organizations: Trends in Civilianization*. Tempe (AZ): Arizona State University.

Kowalski, M. (2002). *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics*. Ottawa (ON): Statistics Canada.

Krasodomski-Jones, A. (2021). *The Liberal Democratic Internet - Five Models for a Digital Future*. London, United Kingdom: Digital Policy Lab, Institute for Strategic Dialogue.

Kratz, M. (2018). 514-BILLETS Pays $100,000 - CASL Still Being Enforced After Critical Reviews. Retrieved May 2022, from http://www.slaw.ca/2018/05/25/514-billets-pays-100000-casl-still-being-enforced-after-critical-reviews/.

Kratz, M. (2019). Digital Intermediaries Can Be Responsible for Unknown CASL Violations - New CRTC Guidance on S.9 Anti-Spam Compliance. Retrieved May 2022, from http://www.slaw.ca/2019/01/24/digital-intermediaries-can-be-responsible-for-unknown-casl-violations-new-crtc-guidance-on-s-9-anti-spam-compliance/.

Kratz, M. (2020). CRTC Enforces CASL in Case of Malware Distribution. Retrieved May 2022, from http://www.slaw.ca/2020/01/03/crtc-enforces-casl-in-case-of-malware-distribution/.

Krishnamurthy, V., Lenner, A. L., Sali, M., van Houden, V., Crothers, S., Nguyen, J., . . . Horton, B. (2020). *CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States*. Ottawa (ON): Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa (CIPPIC).

Krishnamurthy, V., Schmidt, D., & Lehr, A. (2021). Cybersecurity and Human Rights: Understanding the Connection. In J. Andrew & F. Bernard (Eds.), *Human Rights Responsibilities in the Digital Age: States, Companies and Individuals* (1 ed.). Oxford, United Kingdom: Hart Publishing.

Kristof, N. (2020). The Children of Pornhub. Retrieved December 2022, from https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html.

Kukutai, T. & Taylor, J. (2016). *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australia: ANU Press.

Laidlaw, E. & Young, H. (2017). *Internet Intermediary Liability in Defamation: Proposals for Statutory Reform*. Toronto (ON): Law Commission of Ontario.

Laidlaw, E. (2019). *Mapping Current and Emerging Models of Intermediary Liability*. Calgary (AB): University of Calgary.

Laidlaw, E. & Young, H. (2020). Creating a revenge porn tort for Canada. *Supreme Court Law Review, 2020*, 147-187.

Laidlaw, E. (2021a). The Future of the Tort of Privacy: Is Alberta's Lag Its Opportunity to Lead? Retrieved March 2022, from https://nationalmagazine.ca/en-ca/articles/law/opinion/2021/the-future-of-the-tort-of-privacy.

Laidlaw, E. (2021b). *Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows*. Calgary (AB): Global Affairs Canada.

Lam, S., Ferlatte, O., & Salway, T. (2019). Cyberbullying and health: A preliminary investigation of the experiences of Canadian gay and bisexual adult men. *Journal of Gay & Lesbian Social Services, 31*(3), 332-357.

Landau, S. (2011). *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. Cambridge (MA): MIT Press.

Landau, S. (2017). *Listening In: Cybersecurity in an Insecure Age*. Grand Rapids (MI): Yale University Press.

Lane, A. M. (2022). Crypto Theft is on the Rise. Here's How the Crimes Are Committed, and How You Can Protect Yourself. Retrieved March 2022, from https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027.

Lang, H. (2022). Major Cryptocurrency Firms Launch New Coalition to Promote Market Integrity. Retrieved February 2022, from https://www.theglobeandmail.com/business/international-business/article-major-cryptocurrency-firms-launch-new-coalition-to-promote-market/.

Langlois, S. & Sauvageau, F. (2021). La désinformation et les médias sociaux, le couple qui inquiète. Retrieved December 2022, from https://www.ledevoir.com/opinion/idees/594300/la-desinformation-et-les-medias-sociaux-le-couple-qui-inquiete.

LCJC (Standing Committee Legal and Constitutional Affairs). (2017). *Delaying Justice is Denying Justice: An Urgent Need to Address Lengthy Court Delays in Canada*. Ottawa (ON): Senate of Canada.

LCO (Law Commission of Ontario). (2020). *Defamation Law in the Internet Age*. Toronto (ON): LCO.

Le Pennec, G., Fiedler, I., & Ante, L. (2021). Wash trading at cryptocurrency exchanges. *Finance Research Letters, 43*, 101982.

Leinwand, J. (2018). Expanding Our Policies on Voter Suppression. Retrieved August 2022, from https://about.fb.com/news/2018/10/voter-suppression-policies/.

Lemstra, M., Rogers, M., Redgate, L., Garner, M., & Moraros, J. (2011). Prevalence, risk indicators and outcomes of bullying among on-reserve First Nations youth. *Canadian Journal of Public Health, 102*(6), 462-466.

Leonardi, P. M. & Vaast, E. (2016). Social Media and Their Affordances for Organizing: A Review and Agenda for Research. *Academy of Management Annals, 11*(1), 150-188.

Leslie, D. (2020). *Understanding Bias in Facial Recognition Technologies*. London, United Kingdom: The Alan Turing Institute.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 1-17.

Leuprecht, C. (2019). *Where to Draw the Blue Line: How Civilians and Contractors Can Let Police Do The Policing*. Ottawa (ON): Macdonald-Laurier Institute.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change, 67*, 3-20.

Library of Congress. (2021). Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech. Retrieved November 2021, from https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/.

Liebhardt, J. (2008). Australia Rallies to "Stop the Clean Feed." Retrieved February 2022, from https://globalvoices.org/2008/12/11/australia-rallies-to-stop-the-clean-feed/.

LII (Legal Information Institute). (n.d.). Tort. Retrieved March 2022, from https://www.law.cornell.edu/wex/tort#:~:text=A%20tort%20is%20an%20act%20or%20omission%20that,in%20fact%20that%20an%20individual%20suffers.%201%20Overview.

Lin, S., Hernandez, S., & Castleman, T. (2022). Accused Pelosi Attacker David DePape Spread QAnon, Other Far-Right, Bigoted Conspiracies. Retrieved November 2022, from https://www.latimes.com/california/story/2022-10-28/pelosi-attack-suspect-david-depape-shared-conspiracy-theories.

Ling, J. & Pearson, J. (2016). Exclusive: Canadian Police Obtained Blackberry's Global Decryption Key. Retrieved October 2022, from https://www.vice.com/en/article/kz9kaa/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how.

Ling, J. (2022). Was it Really about Vaccine Mandates - or Something Darker? The Inside Story of the Convoy Protests. Retrieved December 2022, from https://www.thestar.com/news/canada/2022/03/19/was-it-really-about-vaccine-mandates-or-something-darker-the-inside-story-of-the-convoy-protests.html.

Little, S. (2022). Exclusive: Mountie Who Worked Amanda Todd Case Speaks for First Time. Retrieved November 2022, from https://globalnews.ca/news/9050914/amanda-todd-officer-speaks/.

Llansó, E. J. (2020). No amount of "AI" in content moderation will solve filtering's prior-restraint problem. *Big Data & Society*, *7*(1), 2053951720920686.

Louie, D. W. (2017). Social media and the sexual exploitation of Indigenous girls. *Girlhood Studies*, *10*(2), 97-113.

Loveluck, B. (2020). The many shades of digital vigilantism: A typology of online self-justice. *Global Crime*, *21*(3-4), 213-241.

Lucock, C. & Black, K. (2009). Anonymity and Law in Canada. In I. Kerr, V. Steeves & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. New York (NY): Oxford University Press.

Lukings, M. & Lashkari, A. H. (2022a). *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance* (1 ed.). Cham, Switzerland: Springer Cham.

Lukings, M. & Lashkari, A. H. (2022b). *Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective*. Cham, Switzerland: Springer Nature.

Lyons, K. (2021). Clearview's Facial Recognition Tech is Illegal Mass Surveillance, Canada Privacy Commissioners Say. Retrieved November 2022, from https://www.theverge.com/2021/2/4/22266055/clearview-facial-recognition-illegal-mass-surveillance-canada-privacy.

Mac, R. & Hill, K. (2021). Are Apple AirTags Being Used to Track People and Steal Cars? Retrieved December 2022, from https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html.

Macaulay, K. (2021). How Is Canada Addressing Non-Consensual Intimate Image Distribution? Retrieved November 2022, from https://www.mcgill.ca/definetheline/article/how-canada-addressing-non-consensual-intimate-image-distribution.

MacCarthy, M. (2022). What U.S. Policymakers Can Learn from the U.K.'s Online Safety Bill. Retrieved June 2022, from https://www.brookings.edu/blog/techtank/2022/05/19/what-u-s-policymakers-can-learn-from-the-u-k-s-online-safety-bill/.

MacDonald, M. (2021). The Double Exploitation of Deepfake Porn. Retrieved January 2022, from https://thewalrus.ca/the-double-exploitation-of-deepfake-porn/.

Macguire, E. (2020). Anti-Asian Hate Continues to Spread Online Amid COVID-19 Pandemic. Retrieved December 2022, from https://www.aljazeera.com/news/2020/4/5/anti-asian-hate-continues-to-spread-online-amid-covid-19-pandemic.

Mackey, J. (2012). Privacy and the Canadian media: Developing the new tort of "intrusion upon seclusion" with Charter values. *Western Journal of Legal Studies*, 2(1), 3.

Madiega, T. (2020). *Reform of the EU Liability Regime for Online Intermediaries*. Brussels, Belgium: European Parliamentary Research Service.

Madiega, T. (2021). *Digital Services Act*. Brussels, Belgium: European Parliamentary Research Service.

Malone, M. (2021). *Canadian Businesses Need Better Tools to Report Cybercrime*. Ottawa (ON): Institute for Research on Public Policy.

Maras, M.-H. & Alexandrou, A. (2018). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof, 23*(3), 255-262.

Martin, A. (2021). What is the Online Safety Bill and Why are Some People Worried About it? Retrieved November 2021, from https://news.sky.com/story/what-is-the-online-safety-bill-and-why-are-some-people-worried-about-it-12437427.

Marwick, A. & Lewis, R. (2017). *Media Manipulation and Disinformation Online*. New York (NY): Data & Society Research Institute.

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics, 18*(1), 1-20.

Masoodi, M. J. & Rand, A. (2021). *Why Canada Must Defend Encryption*. Toronto (ON): Ryerson University's Cybersecure Policy Exchange.

Matthes, J., Schmuck, D., & von Sikorski, C. (2021). In the eye of the beholder: A case for the visual hostile media phenomenon. *Communication Research*, 00936502211018596.

Mazowita, B. & Vézina, M. (2014). *Police-Reported Cybercrime in Canada, 2012*. Ottawa (ON): Statistics Canada.

McClelland, C. (2021). Data Brokers Are Tracking You — and Selling the Info. Retrieved May 2022, from https://financialpost.com/technology/data-brokers-are-tracking-you-and-selling-the-info.

McFarlane, G. (2021). How Facebook (Meta), Twitter, Social Media Make Money From You. Retrieved October 2022, from https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx#toc-the-bottom-line.

McGuire, M. R. (2017). Technology Crime and Technology Control: Contexts and History. In M. R. McGuire & T. J. Holt (Eds.), *The Routledge Handbook of Technology, Crime and Justice*. Abingdon, United Kingdom: Routledge.

Mckim, N. (2021). Greens Reject Online Safety Bill. Retrieved November 2021, from https://greensmps.org.au/articles/greens-reject-online-safety-bill.

McMillan. (2018). What Can The Law Do About 'Deepfake'? Retrieved April 2022, from https://mcmillan.ca/insights/what-can-the-law-do-about-deepfake/.

McMillan. (2021). Bill 64 Enacted: Québec's Modern Privacy Regime. Retrieved April 2022, from https://mcmillan.ca/insights/bill-64-enacted-quebecs-modern-privacy-regime/.

McNamee, M. S. (2021). HSE Cyber-Attack: Irish Health Service Still Recovering Months After Hack. Retrieved May 2022, from https://www.bbc.com/news/world-europe-58413448.

Mcquigge, M. (2018). Airbnb Rentals Being Used for Alleged Human Trafficking: Toronto Police. Retrieved May 2022, from https://www.theglobeandmail.com/news/toronto/airbnb-rentals-being-used-for-alleged-human-trafficking-toronto-police/article38066008/.

MediaSmarts. (n.d.). Responses and Solutions in the Classroom. Retrieved January 2022, from https://mediasmarts.ca/online-hate/responses-solutions.

Merrill, J. B. & Oremus, W. (2021). Five Points for Anger, One for a 'Like': How Facebook's Formula Fostered Rage and Misinformation. Retrieved January 2022, from https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/.

Meyer, C. (2021). Canada Looks at Australia's Experience Regulating Social Media. Retrieved July 2021, from https://www.thestar.com/news/canada/2021/02/02/canada-looks-at-australias-experience-regulating-social-media.html.

Ministère de l'Intérieur. (2019). Un insigne militaire pour valoriser les gendarmes docteurs. Retrieved June 2022, from https://www.gendarmerie.interieur.gouv.fr/pjgn/actus/un-insigne-militaire-pour-valoriser-les-gendarmes-docteurs.

Misitzis, L. (2021, July 2). There. I Fixed It., *This American Life*.

Mizrahi, S. (2018). Ontario's new invasion of privacy torts: Do they offer monetary redress for violations suffered via the Internet of Things? *Western Journal of Legal Studies*, *8*(1), 3.

Molla, R. (2021). Right-Wing Extremists' Favorite New Platform Is So Dangerous. Retrieved September 2022, from https://www.vox.com/recode/22238755/telegram-messaging-social-media-extremists.

Monk, B., Mitchell, J., Frank, R., & Davies, G. (2018). Uncovering Tor: An examination of the network structure. *Security and Communication Networks*, 4231326.

Moonshot CVE. (2021). *Redirect Method Canada: Final Report*. London, United Kingdom: Moonshot CVE.

Moreau, G. (2021a). *Police-Reported Crime Statistics in Canada, 2020*. Ottawa (ON): Statistics Canada.

Moreau, G. (2021b). *Police-Reported Hate Crime in Canada, 2019*. Ottawa (ON): Statistics Canada.

Mortensen, M. & Neumayer, C. (2021). The playful politics of memes. *Information, Communication & Society*, 24(16), 2367-2377.

Müller, K. & Schwarz, C. (2020a). From hashtag to hate crime: Twitter and anti-minority sentiment. *SSRN*, 3149103

Müller, K. & Schwarz, C. (2020b). Fanning the flames of hate: Social media and hate crime. *SSRN*, 3082972.

Mullins, S. J. (2013). "Global Jihad": The Canadian experience. *Terrorism and Political Violence*, *25*(5), 734-776.

Musharbash, Y. (2021). *The Globalization of Far-Right Extremism: An Investigative Report*. West Point (NY): Combating Terrorism Center.

NACCC (North American Cyber Classification Compendium). (2021a). *Cyber Classification Compendium*. Vol. 21.09 Ottawa (ON): Cybercrime Support Network, Canadian Association of Chiefs of Police, E-Crimes Cyber Council.

NACCC (North American Cyber Classification Compendium). (2021b). *North American Cyber Classification Compendium Infographic*. Ottawa (ON): Cybercrime Support Network, Canadian Association of Chiefs of Police, E-Crimes Cyber Council.

Nakashima, E. & Gellman, B. (2015). As Encryption Spreads, U.S. Grapples With Clash Between Privacy, Security. Retrieved April 2014, from https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html?postshare=531428699926574.

NCMEC (National Center for Missing & Exploited Children). (2021). COVID-19 and Missing & Exploited Children. Retrieved August 2021, from https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children.

NeedHelpNow.ca. (2022). Removing Pictures/Videos. Retrieved January 2022, from https://www.needhelpnow.ca/app/en/removing_pictures.

Negreiro, M. (2020). *Curbing the Surge in Online Child Abuse: The Dual Role of Digital Technology in Fighting and Facilitating its Proliferation*. Brussels, Belgium: European Parliament.

Nesbitt, M. & Hansen, T. (2021). Enforcing Canadian Security Laws through Criminal Prosecutions during a Pandemic: Lessons from Canada's COVID-19 Experience. In L. West, T. Juneau & A. Amarasingam (Eds.), *Stress Tested: The COVID-19 Pandemic and Canadian National Security*. Calgary (AB): University of Calgary Press.

Netsafe. (2021). What is the HDCA? Retrieved July 2021, from https://www.netsafe.org.nz/what-is-the-hdca/.

New Zealand Police. (2021). *New Zealand Police Expert Panel on Emergent Technologies. Terms of Reference*. Wellington, New Zealand: New Zealand Police.

New Zealand Police. (2022). Advisory Panel on Emergent Technologies. Retrieved April 2022, from https://www.police.govt.nz/about-us/programmes-and-initiatives/police-use-emergent-technologies/advisory-panel-emergent.

Newton, C. (2019). The Trauma Floor: The Secret Lives of Facebook Moderators in America. Retrieved April 2022, from https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona.

Newton, C. (2020). Everything You Need to Know About Section 230. Retrieved November 2021, from https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation.

Nisker, J. (2006). PIPEDA: A constitutional analysis. *Canadian Bar Review, 85*(2), 317-343.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford (CA): Stanford Law Books.

NLCA (Court of Appeal of Newfoundland and Labrador). (2019). *Re: Section 487.02 of the Criminal Code, 2019 NLCA 6*. St. John's (NL): NLCA.

Nobles, M., Reyns, B. W., Fox, K., & Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly, 31*(6), 986-1014.

Nogrady, B. (2021). Scientists under attack. *Nature, 598*, 250-253.

Nordal, S. (2013). *Privacy as a Social Concept*. Calgary (AB): University of Calgary.

Northcott, P. (2021). Civilian Investigators Coming to RCMP. Retrieved February 2022, from https://www.rcmp-grc.gc.ca/en/gazette/civilian-investigators-coming-rcmp?h=.

Northcott, P. (2022). RCMP Training Officers on Cryptocurrency. Retrieved September 2022, from https://www.rcmp-grc.gc.ca/en/gazette/rcmp-training-officers-cryptocurrency.

Norton Rose Fulbright. (2012). Rights of Action for Breach of Privacy in Canada. Retrieved April 2022, from https://www.mondaq.com/canada/corporate/175580/rights-of-action-for-breach-of-privacy-in-canada.

Nosák, D. (2021). The DSA Introduces Important Transparency Obligations for Digital Services, but Key Questions Remain. Retrieved June 2022, from https://cdt.org/insights/the-dsa-introduces-important-transparency-obligations-for-digital-services-but-key-questions-remain/.

Novak, M., Grier, J., & Gonzales, D. (2019). New Approaches to Digital Evidence and Acquisition and Analysis. Retrieved May 2022, from https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

NSF (National Science Foundation). (2019). Facial Recognition Software Has a Gender Problem. Retrieved April 2022, from https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=299486.

NSIRA (National Security and Intelligence Review Agency). (2019a). *Review of the CSIS-RCMP Relationship in a Region of Canada through the Lens of an Ongoing Investigation*. Ottawa (ON): NSIRA.

NSIRA (National Security and Intelligence Review Agency). (2019b). *Review of the Canadian Security Intelligence Service's (CSIS) Internal Security Branch*. Ottawa (ON): NSIRA.

NSPCC (National Society for the Prevention of Cruelty to Children). (2020). Instagram Most Recorded Platform Used in Child Grooming Crimes During Lockdown. Retrieved September 2022, from https://www.nspcc.org.uk/about-us/news-opinion/2020/instagram-grooming-crimes-children-lockdown.

NSSC (Supreme Court of Nova Scotia). (2015). *Crouch v. Snell, 2015 NSSC 340*. Halifax (NS): NSSC.

NSWP (Global Network of Sex Work Projects). (2018). *The Impact of Anti-Trafficking Legislation and Initiatives on Sex Workers*. Edinburgh, United Kingdom: NSWP.

NWAC (Native Women's Association of Canada). (2014). *Sexual Exploitation and Trafficking of Aboriginal Women and Girls: Literature Review and Key Informant Interviews*. Gatineau (QC): NWAC.

O'Connor, C. (2021). *Gaming and Extremism: The Extreme Right on Twitch*. London, United Kingdom: Institute for Strategic Dialogue.

O'Regan, M. (2019). Airbnb Must Face the Facts: Human Trafficking and Modern Slavery Happen in Rented Accommodation. Retrieved May 2022, from https://news.airbnb.com/expanding-our-efforts-to-combat-human-trafficking/.

OAIC (Office of the Australian Information Commissioner). (2021). Clearview AI Breached Australians' Privacy. Retrieved October 2022, from https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy.

OECD (Organisation for Economic Co-operation and Development). (2020a). *Combatting COVID-19 Disinformation on Online Platforms*. Paris, France: OECD.

OECD (Organisation for Economic Co-operation and Development). (2020b). *Current Approaches to Terrorist and Violent Extremist Content Among the Global Top 50 Online Content-Sharing Services*. Paris, France: OECD.

OECD (Organisation for Economic Co-operation and Development). (2021). *Data Portability, Interoperability and Digital Platform Competition*. Paris, France: OECD.

Ofcom. (2020). Ofcom to Regulate Harmful Content Online. Retrieved July 2021, from https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/ofcom-to-regulate-harmful-content-online#:~:text=The%20Government%20has%20decided%20to,benefits%20of%20being%20online%20safely.

OHCHR (United Nations Human Rights Office of the High Commissioner). (2021). Special Rapporteur on the Right to Privacy. Retrieved January 2022, from https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701-1777.

Olser. (n.d.). CASL Compliance: More than Spam. Understanding Canada's Anti-Spam Law. Retrieved May 2022, from https://www.osler.com/en/resources/in-focus/casl-compliance-more-than-spam-understanding-canada-s-anti-spam-law.

Olteanu, A., Castillo, C., Boy, J., & Varshney, K. R. (2018). *The Effect of Extremist Violence on Hateful Speech Online*. Paper presented at Proceedings of the Twelfth International AAAI Conference on Web and Social Media, Palo Alto (CA).

ONCA (Court of Appeal for Ontario). (2012). *Jones v. Tsige 2012 ONCA 32*. Toronto (ON): ONCA.

ONCJ (Ontario Court of Justice). (2021). *R. v. Hurren, 2021 ONCJ 148*. Ottawa (ON): ONCJ.

OnlyFans. (2020). *Privacy Policy*. London, United Kingdom: OnlyFans.

ONSC (Ontario Superior Court of Justice). (2016). *Doe 464533 v. D. (N.), 2016 ONSC 541*. Toronto (ON): ONSC.

ONSC (Ontario Superior Court of Justice). (2019). *Yenovkian v. Gulian, 2019 ONSC 7279*. Toronto (ON): ONSC.

ONSC (Ontario Superior Court of Justice). (2021). *Caplan v. Atas, 2021 ONSC 670*. Toronto (ON): ONSC.

OPC (Office of the Privacy Comissioner of Canada). (2011). Data at Your Fingertips Biometrics and the Challenges to Privacy. Retrieved April 2022, from https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/.

OPC (Office of the Privacy Commissioner of Canada). (2016a). How the OPC Protects and Promotes Privacy. Retrieved August 2021, from https://www.priv.gc.ca/en/about-the-opc/what-we-do/mm/.

OPC (Office of the Privacy Commissioner of Canada). (2016b). Online Reputation: What Are They Saying about Me? Retrieved April 2022, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/.

OPC (Office of the Privacy Commissioner of Canada). (2017a). Enforcement of PIPEDA. Retrieved May 2022, from https://priv.gc.ca/biens-assets/compliance-framework/en/index.

OPC (Office of the Privacy Commissioner of Canada). (2017b). Interpretation Bulletin: Commercial Activity. Retrieved October 2022, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/.

OPC (Office of the Privacy Commissioner of Canada). (2018). Summary of Privacy Laws in Canada. Retrieved July 2021, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

OPC (Office of the Privacy Commissioner of Canada). (2019a). *2018-2019 Survey of Canadians on Privacy*. Ottawa (ON): OPC.

OPC (Office of the Privacy Commissioner of Canada). (2019b). The *Privacy Act* in Brief. Retrieved July 2021, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_brief/.

OPC (Office of the Privacy Commissioner of Canada). (2019c). PIPEDA in Brief. Retrieved October 2022, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

OPC (Office of the Privacy Commissioner of Canada). (2020a). Privacy in a Pandemic. Retrieved May 2022, from https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201920/ar_201920/.

OPC (Office of the Privacy Commissioner of Canada). (2020b). Questions and Answers - Bill 64. Retrieved April 2022, from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/qa_20200924/.

OPC (Office of the Privacy Commissioner of Canada). (2021a). *Projecting Our Values Into Laws: Laying the Foundation for Responsible Innovation*. Gatineau (QC): OPC.

OPC (Office of the Privacy Commissioner of Canada). (2021b). *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020*. Gatineau (QC): OPC.

OPC (Office of the Privacy Commissioner of Canada). (2021c). RCMP's Use of Clearview AI's Facial Recognition Technology Violated Privacy Act, Investigation Concludes. Retrieved May 2022, from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/.

OPC (Office of the Privacy Commissioner of Canada). (2021d). *Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*. Ottawa (ON): OPC.

OPC (Office of the Privacy Commissioner of Canada). (2022). Privacy Education for Kids. Retrieved May 2022, from https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/.

OSC (Ontario Securities Commission). (2022). Canadian Securities Regulators Expect Commitments from Crypto Trading Platforms Pursuing Registration. Retrieved September 2022, from https://www.osc.ca/en/news-events/news/canadian-securities-regulators-expect-commitments-crypto-trading-platforms-pursuing-registration.

Osipovich, A. (2021). Upstart Peer-to-Peer Crypto Exchanges Take Aim at Coinbase. Retrieved April 2022, from https://www.wsj.com/articles/upstart-peer-to-peer-crypto-exchanges-take-aim-at-coinbase-11621848601.

Owen, T., Loewen, P., Ruths, D., Bridgman, A., Gorwa, R., MacLellan, S., . . . Zhilin, O. (2019). *Digital Democracy Project: Research Memo #3 - Polarization and its Discontents*. Ottawa (ON): Public Policy Forum.

Paikin, S. (2020, May 13). How Extremists Are Exploiting COVID-19, *The Agenda*.

Palmer, D. (2021). Businesses Don't Know How to Manage VPN Security Properly - and Cyber Criminals Are Taking Advantage. Retrieved October 2022, from https://www.zdnet.com/article/many-organisations-dont-know-how-to-manage-vpn-security-properly-and-cyber-criminals-are-taking-advantage/.

Paris, B. & Donovan, J. (2019). *Deepfakes and Cheap Fakes*. New York (NY): Data & Society.

Parker, S. (2021). *The North American Cyber Classification Compendium*. Vol. Spring/Summer 2021. Ottawa (ON): Canadian Police Chief Magazine.

Parsons, C. (2016). Pleading the Case: How the RCMP Fails to Justify Calls for New Investigatory Powers. Retrieved February 2022, from https://christopher-parsons.com/pleading-the-case-how-the-rcmp-fails-to-justify-calls-for-new-investigatory-powers/.

Parsons, C. & Molnar, A. (2018). Government surveillance accountability: The failures of contemporary Canadian interception reports. *Canadian Journal of Law and Technology, 16*(1), 4.

Parsons, C. (2019). Canada's New and Irresponsible Encryption Policy. Retrieved August 2021, from https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/.

Parsons, C. (2022). Lawful Access Returns: Online Harms and Warrantless Access to Subscriber and Transmission Data. Retrieved April 2022, from https://christopher-parsons.com/lawful-access-returns-online-harms-and-warrantless-access-to-subscriber-and-transmission-data/.

Parsons, P. (2021). Prosecutor Shortage Puts 1,200 Court Cases at Risk, Says Alberta Crown Attorneys' Association. Retrieved April 2022, from https://www.cbc.ca/news/canada/edmonton/alberta-crown-prosecutor-shortage-1.6255359.

Patil, S. (2019). *Partnering for Prosperity: India-Canada Collaboration to Curb Digital Black Markets*. Waterloo (ON): Centre for International Governance Innovation and Gateway House.

Pavlounis, D., Johnston, J., Brodsky, J., & Brooks, P. (2022). *The Digital Media Literacy Gap: How to Build Widespread Resilience to False and Misleading Information Using Evidence-Based Classroom Tools*. Toronto (ON): CIVIX Canada.

Pearson, J. & Ling, J. (2016). Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages. Retrieved February 2022, from https://www.vice.com/en/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada.

Pennell, D., Campbell, M., Tangen, D., & Knott, A. (2022). Should Australia have a law against cyberbullying? Problematising the murky legal environment of cyberbullying from perspectives within schools. *The Australian Educational Researcher, 49*, 827-844.

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2), 2017.2012.2692.

Penney, J. (2019a). Chilling effects and transatlantic privacy. *European Law Journal, 25*, 122-139.

Penney, J. (2019b). Privacy and legal automation: The DMCA as a case study. *Stanford Technology Law Review, 22*(2), 412-486.

Penney, J. (2020). Online Abuse, Chilling Effects, and Human Rights. In E. Dubois & F. Martin-Bariteau (Eds.), *Citizenship in a Connected Canada: A Policy and Research Agenda*. Ottawa (ON): University of Ottawa Press.

Penney, J. (2022). Understanding chilling effects. *Minnesota Law Review, 106*(3), 1451-1530.

Pennycook, G., Bear, A., Collins, E. T., & Rand, D. G. (2020). The implied truth effect: Attaching warnings to a subset of fake news headlines increases perceived accuracy of headlines without warnings. *Management Science, 66*(11), 4944-4957.

Pennycook, G., Epstein, Z., Mosleh, M., Arechar, A. A., Eckles, D., & Rand, D. G. (2021). Shifting attention to accuracy can reduce misinformation online. *Nature, 592*(7855), 590-595.

Perrigo, B. (2022). Inside Facebook's African Sweatshop. Retrieved April 2022, from https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/.

Perrin, W., Woods, L., & Walsh, M. (2021). Secretary of State's Powers and the Draft Online Safety Bill. Retrieved November 2021, from https://www.carnegieuktrust.org.uk/blog-posts/secretary-of-states-powers-and-the-draft-online-safety-bill/.

Perry, B. & Scrivens, R. (2016). Uneasy alliances: A look at the right-wing extremist movement in Canada. *Studies in Conflict & Terrorism, 39*(9), 819-841.

Pew Research Center. (2017). *Online Harassment 2017*. Washington (DC): Pew Research Center.

Pfefferkorn, R. (2020). The EARN IT Act: How to Ban End-to-End Encryption without Actually Banning It. Retrieved April 2022, from https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it.

Pfefferkorn, R. (2022). Content-oblivious trust and safety techniques: Results from a survey of online service providers. *Journal of Online Trust and Safety, 1*(2), jots.v1i2.14.

PHAC (Public Health Agency of Canada). (2019). *Canada: A Pathfinding Country. Canada's Road Map to End Violence Against Children*. Ottawa (ON): PHAC.

Plan International. (2020a). *Free to be Online?: Girls' and Young Women's Experiences of Online Harassment*. Surrey, United Kingdom: Plan International.

Plan International. (2020b). Abuse and Harassment Driving Girls Off Facebook, Instagram and Twitter. Retrieved August 2021, from https://plan-international.org/news/2020-10-05-abuse-and-harassment-driving-girls-facebook-instagram-and-twitter.

Police1 BrandFocus Staff. (2018). Analyze and Share Digital Evidence Faster with a Tool Developed by and for Police. Retrieved May 2022, from https://www.police1.com/police-products/investigation/computer-digital-forensics/articles/analyze-and-share-digital-evidence-faster-with-a-tool-developed-by-and-for-police-3Z5uUyAYZ1MQwXWJ/.

Pollino, M. A. (2021). Turning points from victim to survivor: An examination of sexual violence narratives. *Feminist Media Studies*, 14680777.14682021.12006260.

Popham, J., McCluskey, M., Ouellet, M., & Gallupe, O. (2020). Exploring police-reported cybercrime in Canada: Variation and correlates. *Policing: An International Journal, 43*(1), 35-48.

Pornhub. (2020). The Latest on Our Commitment to Trust and Safety. Retrieved October 2020, from https://www.pornhub.com/blog/the-latest-on-our-commitment-to-trust-and-safety.

Pornhub. (2022). Non-Consensual Content Policy. Retrieved March 2022, from https://help.pornhub.com/hc/en-us/articles/360041719433-Non-Consensual-Content-Policy.

Porter, J. (2021). Apple Scrubs Controversial CSAM Detection Feature from Webpage But Says Plans Haven't Changed. Retrieved October 2022, from https://www.theverge.com/2021/12/15/22837631/apple-csam-detection-child-safety-feature-webpage-removal-delay.

Posetti, J., Bontchev, K., & Shabbir, N. (2022). *The Chilling: Assessing Big Tech's Response to Online Violence Against Women Journalists*. Paris, France: UNESCO.

Posner, R. (2007). *United States vs. Garcia*. Madison (WI): United States Court of Appeals, Seventh Circuit.

Powell, A. & Henry, N. (2018). Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives. *Policing and Society, 28*(3), 291-307.

Powell, T. E., Boomgaarden, H. G., De Swert, K., & de Vreese, C. H. (2015). A clearer picture: The contribution of visuals and text to framing effects. *Journal of Communication, 65*(6), 997-1017.

PrevNet. (2014). *Cyber Bullying and How it is Affecting Canadian Youth*. Kingston (ON): Queen's University.

Price, M. (2022). Mastercard, Visa Suspend Ties with Ad Arm of Pornhub Owner MindGeek. Retrieved October 2022, from https://www.reuters.com/business/finance/mastercard-visa-suspend-ties-with-ad-arm-pornhub-owner-mindgeek-2022-08-04/.

Prichard, J., Wortley, R., Watters, P. A., Spiranovic, C., Hunn, C., & Krone, T. (2022). Effects of automated messages on internet users attempting to access 'barely legal' pornography. *Sexual Abuse, 34*(1), 106-124.

Proctor, J. (2020). The Difficult History of Prosecuting Hate in Canada. Retrieved July 2021, from https://www.cbc.ca/news/canada/british-columbia/racists-attacks-court-hate-crimes-1.5604912.

Project Arachnid. (2022). Shield by Project Arachnid. Retrieved February 2022, from https://www.projectarachnid.ca/en/#shield.

PS (Public Safety Canada). (2017a). Five Country Ministerial 2017: Joint Communiqué. Retrieved October 2022, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/index-en.aspx.

PS (Public Safety Canada). (2017b). *2017 Public Report on the Terrorist Threat to Canada*. Ottawa (ON): PS.

PS (Public Safety Canada). (2019a). *2018 Public Report on the Terrorist Threat to Canada*. Ottawa (ON): PS.

PS (Public Safety Canada). (2019b). Government of Canada Announces Initiatives to Address Violent Extremist and Terrorist Content Online. Retrieved November 2021, from https://www.canada.ca/en/public-safety-canada/news/2019/06/government-of-canada-announces-initiatives-to-address-violent-extremist-and-terrorist-content-online.html.

PS (Public Safety Canada). (2020). International Statement: End-To-End Encryption And Public Safety. Retrieved February 2022, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2020-jnt-sttmnt-ncrptn-pblc-sfty/index-en.aspx.

PS (Public Safety Canada). (2021a). Cyberbullying Can Be Against the Law. Retrieved August 2021, from https://www.canada.ca/en/public-safety-canada/campaigns/cyberbullying/cyberbullying-against-law.html.

PS (Public Safety Canada). (2021b). Five Country Ministerial. Retrieved September 2021, from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-en.aspx.

PS (Public Safety Canada). (2021c). Human Trafficking. Retrieved August 2021, from https://www.canada.ca/en/public-safety-canada/campaigns/human-trafficking.html.

Pyrik, J. (2021). The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). In S. Carvin, T. Juneau & C. Forcese (Eds.), *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community.* Toronto (ON): University of Toronto Press.

Qarri, A. (2022). Canada Must Reform Competition and Privacy Policy Together to Protect Consumers. Retrieved June 2022, from https://policyoptions.irpp.org/magazines/february-2022/canada-must-reform-competition-and-privacy-policy-together-to-protect-consumers/.

Rakheja, H. (2021). Despite Privacy Fears, Aadhaar-Linked Facial Recognition Used For Covid-19 Vaccines. Retrieved April 2022, from https://inc42.com/buzz/despite-privacy-fears-facial-recognition-used-for-covid-19-vaccines/.

Raman-Wilms, M. & Curry, B. (2021). What is Bill C-10 and Why Are the Liberals Planning to Regulate the Internet? Retrieved July 2021, from https://www.theglobeandmail.com/politics/article-what-is-bill-c-10-and-why-are-the-liberals-planning-to-regulate-the/.

Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications, 186*, 115742.

RCMP (Royal Canadian Mounted Police). (2014). *Cybercrime: An Overview of Incidents and Issues in Canada*. Ottawa (ON): RCMP.

RCMP (Royal Canadian Mounted Police). (2018). RCMP Warn of Social Media Extortion Scam Targeting Youths. Retrieved February 2022, from https://www.rcmp-grc.gc.ca/en/news/2018/rcmp-warn-social-media-extortion-scam-targeting-youths.

RCMP (Royal Canadian Mounted Police). (2019). Fraud Schemes Targeting New Canadians. Retrieved November 2021, from https://www.rcmp-grc.gc.ca/en/news/2019/fraud-schemes-targeting-new-canadians.

RCMP (Royal Canadian Mounted Police). (2020a). The Connected RCMP. Retrieved February 2022, from https://www.rcmp-grc.gc.ca/en/connected-rcmp.

RCMP (Royal Canadian Mounted Police). (2020b). RCMP FSOC Target Dark Web Drug Trafficking Operation. Retrieved August 2021, from https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=2100&languageId=1&contentId=63303.

RCMP (Royal Canadian Mounted Police). (2020c). The National Cybercrime Coordination Unit. Retrieved February 2022, from https://www.rcmp-grc.gc.ca/en/national-cybercrime-coordination-unit.

RCMP (Royal Canadian Mounted Police). (2021a). Cybercrime Defined. Retrieved October 2021, from https://www.rcmp-grc.gc.ca/en/cybercrime-defined.

RCMP (Royal Canadian Mounted Police). (2021b). New Cybercrime and Fraud Reporting System. Retrieved October 2021, from https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system.

RCMP (Royal Canadian Mounted Police). (2021c). Impacts and Consequences of Bullying and Cyberbullying. Retrieved July 2022, from https://www.rcmp-grc.gc.ca/en/bullying/impacts-and-consequences-bullying-and-cyberbullying.

RCMP (Royal Canadian Mounted Police). (2021d). The National Cybercrime Coordination Unit (NC3). Retrieved February 2022, from https://www.rcmp-grc.gc.ca/en/nc3.

RCMP (Royal Canadian Mounted Police). (2021e). Response to the Report by the Office of the Privacy Commissioner into the RCMP's use of Clearview AI. Retrieved June 2022, from https://www.rcmp-grc.gc.ca/en/news/2021/response-the-report-the-office-the-privacy-commissioner-the-rcmps-use-clearview-ai.

RCMP (Royal Canadian Mounted Police). (2022a). Sample Warrant. Retrieved October 2022, from https://www.ourcommons.ca/content/Committee/441/ETHI/WebDoc/WD11922842/11922842/RoyalCanadianMountedPolice-Authorization-e.pdf.

RCMP (Royal Canadian Mounted Police). (2022b). Q&A With an Expert in Electronic Surveillance on the Challenges and Opportunities of Collecting Evidence. Retrieved October 2022, from https://www.rcmp-grc.gc.ca/en/gazette/qa-an-expert-electronic-surveillance-the-challenges-and-opportunities-collecting-evidence?fe=undefined&wbdisable=true.

Reed, C. (2007). Taking Sides on Technology Neutrality. *SCRIPT-ed*, *4*(3), 263-284.

Reep-van den Bergh, C. M. & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*, 5.

Reporters Without Borders. (2018). The Network Enforcement Act Apparently Leads to Excessive Blocking of Content. Retrieved November 2021, from https://rsf.org/en/news/network-enforcement-act-apparently-leads-excessive-blocking-content.

Reuters. (2022). German Court Rules Against Online Hate-Speech Law. Retrieved April 2022, from https://www.reuters.com/world/europe/german-court-rules-against-online-hate-speech-law-2022-03-01/.

Rice, E. S., Haynes, E., Royce, P., & Thompson, S. C. (2016). Social media and digital technology use among Indigenous young people in Australia: A literature review. *International Journal for Equity in Health*, *15*(1), 81.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York (NY): Farrar, Straus and Giroux.

Ridgeway, G. (2018). Policing in the Era of Big Data. *Annual Review of Criminology, 1*, 401-419.

Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. *NIJ Journal, 280*(January), 1-10.

Roberts, S. T. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media* (1 ed.). New Haven (CT): Yale University Press.

Robertson, A. (2021). Facebook is Shutting Down Its Face Recognition Tagging Program. Retrieved April 2022, from https://www.theverge.com/2021/11/2/22759613/meta-facebook-face-recognition-automatic-tagging-feature-shutdown.

Robertson, K., Khoo, C., & Song, Y. (2020). *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*. Toronto (ON): The Citizen Lab.

Robinson, N. & Whittaker, J. (2020). Playing for Hate? Extremism, terrorism, and videogames. *Studies in Conflict & Terrorism*, 1057610X.1052020.1866740.

Rogers, R. (2020). Deplatforming: Following extreme internet celebrities to Telegram and alternative social media. *European Journal of Communication, 35*(3), 213-229.

Rohlfing, S. (2015). Hate on the Internet. In N. Hall, A. Corb, P. Giannasi & J. G. D. Grieve (Eds.), *The Routledge International Handbook on Hate Crime*. Abingdon, United Kingdom: Routledge.

Romano, A. (2018). A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as we Know it. Retrieved September 2018, from https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

Roose, K. (2021). What Is QAnon, the Viral Pro-Trump Conspiracy Theory? Retrieved December 2022, from https://www.nytimes.com/article/what-is-qanon.html.

Rottweiler, B. & Gill, P. (2020). Conspiracy beliefs and violent extremist intentions: The contingent effects of self-efficacy, self-control and law-related morality. *Terrorism and Political Violence, 34*(7), 1485-1504.

Saliba, J. (2021). My Technology Can…Speed Up Digital Evidence Processing. Retrieved May 2022, from https://www.policemag.com/613434/my-technology-can-speed-up-digital-evidence-processing.

Samsung. (2021). Evolving for the Better: SmartThings Ecosystem Gives Galaxy Users Better Control Over Their Connected Devices. Retrieved October 2022, from https://www.samsungmobilepress.com/press-releases/evolving-for-the-better-smartthings-ecosystem-gives-galaxy-users-better-control-over-their-connected-devices?path=%2Fpressreleases%2Fevolving-for-the-better-smartthings-ecosystem-gives-galaxy-users-better-control-over-their-connected-devices.

Samsung. (n.d.). Galaxy SmartTag. Retrieved October 2022, from https://www.samsung.com/ca/mobile-accessories/galaxy-smarttag-black-ei-t5300bbegca/.

Sandle, P. (2022). UK Ditches Ban on 'Legal but Harmful' Online Content in Favour of Free Speech. Retrieved December 2022, from https://www.reuters.com/world/uk/uk-ditches-ban-legal-harmful-online-content-favour-free-speech-2022-11-28/.

Sap, M., Card, D., Gabriel, S., Choi, Y., & Smith, N. A. (2019). *The Risk of Racial Bias in Hate Speech Detection.* Paper presented at the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy.

Scassa, T. (2018). Enforcement Powers Key to PIPEDA Reform. Retrieved October 2022 from https://policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/.

Scassa, T. (2020). A Human Rights-Based Approach to Data Protection in Canada. In E. Dubois & F. Martin-Bariteau (Eds.), *Citizenship in a Connected Canada: A Research and Policy Agenda*. Ottawa (ON): University of Ottawa Press.

Scassa, T. (2021). Data Mobility (Portability) in Canada's Bill C-11. Retrieved November 2021, from https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=338:data-mobility-portability-in-canadas-bill-c-11&Itemid=80.

Scassa, T. (2022a). Anonymization and De-Identification in Bill C-27. Retrieved October 2022, from http://teresascassa.ca/index.php?option=com_k2&view=item&id=356:anonymization-and-de-identification-in-bill-c-27&Itemid=80.

Scassa, T. (2022b). Bill C-27's Take on Consent: A Mixed Review. Retrieved October 2022, from http://teresascassa.ca/index.php?option=com_k2&view=item&id=355:bill-c-27%E2%80%99s-take-on-consent-a-mixed-review&Itemid=80.

Scassa, T. (2022c). Data Sharing for Public Good: Does Bill C-27 Reflect Lessons Learned from Past Public Outcry? Retrieved October 2022, from https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=357:data-sharing-for-public-good-does-bill-c-27-reflect-lessons-learned-from-past-public-outcry?&Itemid=80&tmpl=component&print=1.

SCC (Supreme Court of Canada). (1990a). *Canada (Human Rights Commission) v. Taylor [1990] 3 SCR 892*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (1990b). *R. v. Keegstra [1990] 3 SCR 697*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (1995). *Hill v. Church of Scientology of Toronto [1995] 2 SCR 1130*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2011). *Bou Malhab v. Diffusion Métromédia CMR inc. [2011] 1 SCR 214*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2014a). *Wakeling v. United States of America, 2014 SCC 72*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2014b). *R. v. Spencer, 2014 SCC 43*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2016a). *Royal Bank of Canada v. Trang, 2016 SCC 50*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2016b). *R. v. Jordan, 2016 SCC 27*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2021). *Sherman Estate v. Donovan, 2021 SCC 25*. Ottawa (ON): SCC.

SCC (Supreme Court of Canada). (2022). Docket 40269. Andrei Bykovets v. His Majesty the King. Retrieved October 2022, from https://www.scc-csc.ca/case-dossier/info/dock-regi-eng.aspx?cas=40269).

Scheck, J., Purnell, N., & Horwitz, J. (2021). Facebook Employees Flag Drug Cartels and Human Traffickers: The Company's Response is Weak, Documents Show. Retrieved December 2022, from https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953.

Schiebinger, L., Klinge, I., Sánchez de Madariaga, I., Paik, H. Y., Schraudner, M., & Stefanick, M. (2021). Facial Recognition: Analyzing Gender and Intersectionality in Machine Learning. Retrieved September 2022, from https://genderedinnovations.stanford.edu/methods/gender.html.

Schöpfel, J. (2019). Grey Literature and Professional Knowledge Making. In L. Börjesson & I. Huvila (Eds.), *Research Outside The Academy: Professional Knowledge-Making in the Digital Age*. Cham, Switzerland: Springer International Publishing.

Schwartz, B., Adeler, M., Myschyshyn, M., & Walichnowski, R. (2021). Ethical and legal obligations of lawyers to consider cybersecurity. *Asper Review of International Business and Trade Law, 21*, 25-57.

Scott-Railton, J., Campo, E., Marczak, B., Razzak, B. A., Anstis, S., Böcü, G., . . . Deibert, R. (2022). CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. Retrieved May 2022, from https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

Scrivens, R., Davies, G., & Frank, R. (2020). Measuring the evolution of radical right-wing posting behaviors online. *Deviant Behavior, 41*(2), 216-232.

SECU (Standing Committee on Public Safety and National Security). (2021). *Systemic Racism in Policing in Canada*. Ottawa (ON): House of Commons of Canada.

SECU (Standing Committee on Public Safety and National Security). (2022a). *The Rise of Ideologically Motivated Violent Extremism in Canada - 44th Parliament, 1st Session*. Ottawa (ON): House of Commons of Canada.

SECU (Standing Committee on Public Safety and National Security). (2022b). *44th Parliament, 1st Session, Number 012*. Ottawa (ON): House of Commons of Canada.

Seering, J., Wang, T., Yoon, J., & Kaufman, G. (2019). Moderator engagement and community development in the age of algorithms. *New Media & Society, 21*(7), 1417-1443.

Selim, G. (2019). *Mass Violence, Extremism, and Digital Responsibility: Testimony of George Selim Senior Vice President for National Programs ADL (Anti-Defamation League) at a Hearing Before the Senate Committee on Commerce, Science and Transportation*. Washington (DC): The United States Senate.

Shahani, A. (2014). Smartphones are Used to Stalk, Control Domestic Abuse Victims. Retrieved 2022, from https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications, 9*, 4787.

Sheils, C. (2021). Enter The Deep and Dark Web If You Dare (And Get Ready For A Surprise). Retrieved February 2022, from https://digital.com/online-privacy/deep-dark-web/.

Shin, J., Jian, L., Driscoll, K., & Bar, F. (2018). The diffusion of misinformation on social media: Temporal pattern, message, and source. *Computers in Human Behavior, 83*, 278-287.

Short, E., Brown, A., Pitchford, M., & Barnes, J. (2017). Revenge porn: Findings from the harassment and revenge porn (HARP) survey - preliminary results. *Annual Review of Cybertherapy and Telemedicine, 15*, 161-166.

Shute, R., Vernon, E., Verastegui-Sanchez, M., Dix, M., & Planty, M. (2021). *Landscape Study of Digital Tools to Identify, Capture, and Analyze Digital Evidence in Technology-Facilitated Abuse Cases*. Research Triangle Park (NC): U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Siminovic, D. (2017). *Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on Violence Against Women, its Causes and Consequences*. Toronto (ON): Citizen Lab, Munk School of Global Affairs, University of Toronto.

Simonite, T. (2018). Photo Algorithms ID White Men Fine - Black Women, Not So Much. Retrieved April 2022, from https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/.

Simple Rate. (2021). Credit Card Fraud Statistics in Canada 2021. Retrieved July 2022, from https://www.simplerate.ca/credit-card-fraud-statistics-canada/.

Singh, A. (2015). Hacking Team Leak Highlights Citizen Lab Research. Retrieved April 2022, from https://citizenlab.ca/2015/08/hacking-team-leak-highlights-citizen-lab-research/.

Sly, S. & Wheeler, T. (2022). An Education-Based Approach to Curbing CSAM Production. Retrieved April 2022, from https://www.brookings.edu/techstream/an-education-based-approach-to-curbing-csam-production/.

Smith, T. (2021a). Cryptocurrency Regulations Around the World. Retrieved February 2022, from https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122.

Smith, D. (2021b). Here's What Died on the Order Paper. Retrieved May 2022, from https://www.nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2021/here-s-what-died-on-the-order-paper.

Sobowale, J. (2021). A New Era for Crypto. Retrieved February 2022, from https://www.nationalmagazine.ca/en-ca/articles/legal-market/regulatory/2021/a-new-era-for-crypto.

Solomon, H. (2022). Canadian Internet Providers Must Block Bad Botnets, Says Regulator. Retrieved October 2022, from https://www.itworldcanada.com/article/canadian-internet-providers-must-block-bad-botnets-says-regulator/490160.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*, 1087-1156.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477-560.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge (MA): Harvard University Press.

Solove, D. J. (2015). The Meaning and Value of Privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge, United Kingdom: Cambridge University Press.

Spencer, D. C., Ricciardelli, R., Ballucci, D., & Walby, K. (2020). Cynicism, dirty work, and policing sex crimes. *Policing: An International Journal, 43*(1), 151-165.

Starr, P. (2005). *The Creation of the Media: Political Origins of Modern Communications*. New York (NY): Basic Books.

StatCan (Statistics Canada). (2001). The Daily: Household Internet Use Survey. Retrieved May 2022, from https://www150.statcan.gc.ca/n1/daily-quotidien/010726/dq010726a-eng.htm.

StatCan (Statistics Canada). (2018). Language Highlight Tables, 2016 Census. Retrieved April 2022, from https://www12.statcan.gc.ca/census-recensement/2016/dp-pd/hlt-fst/lang/Table.cfm?Lang=E&T=31&Geo=00&SP=1&view=2&age=1&rl=1.

StatCan (Statistics Canada). (2020a). Canadians Spend More Money and Time Online During Pandemic and Over Two-Fifths Report a Cyber Incident. Retrieved August 2020, from https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.htm.

StatCan (Statistics Canada). (2020b). Police Resources in Canada, 2019. Retrieved October 2022, from https://www150.statcan.gc.ca/n1/pub/85-002-x/2020001/article/00015-eng.htm.

StatCan (Statistics Canada). (2021a). *Canadian Internet Use Survey, 2020*. Ottawa (ON): StatCan.

StatCan (Statistics Canada). (2021b). Police-Reported Cybercrime, by Cyber-Related Violation, Canada (Selected Police Services). Retrieved August 2021, from https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000101.

StatCan (Statistics Canada). (2021c). *Cybercrime: Changes to the Uniform Crime Reporting Survey (UCR 2.4)*. Ottawa (ON): StatCan.

StatCan (Statistics Canada). (2022). Incident-Based Crime Statistics, by Detailed Violations, Canada, Provinces, Territories, Census Metropolitan Areas and Canadian Forces Military Police. Retrieved October 2022, from https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510017701&pickMembers%5B0%5D=1.1&pickMembers%5B1%5D=2.257&cubeTimeFrame.startYear=2010&cubeTimeFrame.endYear=2021&referencePeriods=20100101%2C20210101.

Stecula, D. A. & Pickup, M. (2021). Social media, cognitive reflection, and conspiracy beliefs. *Frontiers in Political Science, 3*, 62.

Steeves, V. (2009). Reclaiming the Social Value of Privacy. In I. Kerr, V. Steeves & C. Lucock (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. New York (NY): Oxford University Press.

Stigall, M. & Choo, K.-K. R. (2021). Digital Forensics Education: Challenges and Future Opportunities. In K.-K. R. Choo, T. Morris, G. Peterson & E. Imsand (Eds.), *National Cyber Summit (NCS) Research Track* (Vol. 310). Cham, Switzerland: Springer.

Stoddart, J. (2004). Developing a Canadian Approach to Privacy - Office of the Privacy Commissioner of Canada. Retrieved June 2022, from https://www.priv.gc.ca/en/opc-news/speeches/2004/sp-d_041119/.

Stoddart, J. (2007). The Charter @ 25. Retrieved May 2022, from https://www.priv.gc.ca/en/opc-news/speeches/2007/sp-d_070216/.

Stoltz, M., Crocker, A., & Schmon, C. (2022). The EU Digital Markets Act's Interoperability Rule Addresses an Important Need, but Raises Difficult Security Problems for Encrypted Messaging. Retrieved May 2022, from https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises.

Strawhun, J., Adams, N., & Huss, M. T. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims*, *28*(4), 141-156.

Suares, W. (2019). Experts Advise Protecting Yourself Against Stalking in the Digital Age. Retrieved October 2022, from https://okcfox.com/news/local/stalking-in-the-digital-age.

Sullivan, D. (2021). Giving Kids and Teens More Control Over Their Images in Search. Retrieved October 2022, from https://blog.google/products/search/giving-kids-and-teens-more-control-over-their-images-search/.

Swartz, K. (2021). Mapping Out How Decentralised Exchanges Can be Regulated. Retrieved February 2022, from https://www.regulationasia.com/mapping-out-how-decentralised-exchanges-can-be-regulated/.

Swire-Thompson, B. & Lazer, D. (2020). Public health and online misinformation: Challenges and recommendations. *Annual Review of Public Health*, *41*, 433-451.

Talbot, M. (2021). Canadian Civil Liberties Association has 'serious concerns' about CCTV Expansion in Ontario. Retrieved August 2021, from https://toronto.citynews.ca/2021/07/13/cctv-cameras-privacy-ontario/.

Tanner, S. & Campana, A. (2020). "Watchful citizens" and digital vigilantism: A case study of the far right in Quebec. *Global Crime*, *21*(3-4), 262-282.

Taylor, S. (2017). More Inmates in Sask.'s Jails, Shortage of Crown Prosecutors in Regina. Retrieved April 2022, from https://www.cbc.ca/news/canada/saskatchewan/saskatchewan-justice-ministry-extra-costs-1.4441589.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, *33*(5), 890-911.

Tenove, C., Tworek, H. J. S., & McKelvey, F. (2018). *Poisoning Democracy: How Canada Can Address Harmful Speech Online*. Ottawa (ON): Public Policy Forum.

Tenove, C. & Tworek, H. (2019). Online disinformation and harmful speech: Dangers for democratic participation and possible policy responses. *Journal of Parliamentary & Political Law, 13*, 215-232.

Tenove, C. & Tworek, H. (2020). *Trolled on the Campaign Trail: Online Incivility and Abuse in Canadian Politics*. Vancouver (BC): University of British Columbia's Centre for the Study of Democratic Institutions.

Terrill, R. J. (2013). *World Criminal Justice Systems. A Comparative Survey.* Waltham (MA): Anderson Publishing.

The Canadian Press. (2021). Canadian Companies Hit by Ransomware Attacks Pay Almost $500,000 on Average to Perpetrators, Survey Finds. Retrieved May 2022, from https://www.theglobeandmail.com/business/article-canadian-companies-hit-by-ransomware-attacks-pay-almost-500000-on/.

The eQuality Project. (n.d.). How Do Administrative & Regulatory Law Respond to Tech-Facilitated Violence? Retrieved April 2022, from https://www.equalityproject.ca/resources/legal-briefs-answering-your-questions-about-cyberbullying-law/legal-briefs-how-do-administrative-regulatory-law-respond-to-cyberviolence/#_ftn2.

The Tor Project. (2022). Users: Relay Users. Retrieved September 2022, from https://metrics.torproject.org/userstats-relay-country.html.

Theocharis, Y., Cardenal, A., Jin, S., Aalberg, T., Hopmann, D. N., Strömbäck, J., . . . Štětka, V. (2021). Does the platform matter? Social media and COVID-19 conspiracy theory beliefs in 17 countries. *New Media & Society*, 14614448211045666.

Therrien, D. (2021a). Examining the Canadian Competition Act in the Digital Era. Retrieved June 2022, from https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_sen-ont_211221/.

Therrien, D. (2021b). The Future of Privacy Law Reform in Canada: Remarks at the IAPP Canada Privacy Symposium 2021. Retrieved May 2022, from https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210526/.

Thiessen, B., LaRoche, A., & Lee, J. (2021). Tort of 'Public Disclosure of Private Facts' Recognized in Alberta in 'Revenge Porn' Case. Retrieved May 2022, from https://www.osler.com/en/resources/regulations/2021/tort-of-public-disclosure-of-private-facts-recognized-in-alberta-in-revenge-porn-case.

Thompson, E. (2022). Convoy Protest Could Change the Way Money is Monitored, Says Watchdog Agency. Retrieved March 2022, from https://www.cbc.ca/news/politics/truck-convoy-fundraiser-gofundme-1.6346639.

Thompson, S. & Lyon, D. (2021). Pixies, Pop-Out Intelligence, and Sandbox Play: The New Analytic Model and National Security Surveillance in Canada. In D. Lyon & D. Murakami Wood (Eds.), *Big Data Surveillance and Security Intelligence: The Canadian Case*. Vancouver (BC): University of British Columbia Press.

Tile. (2022). Tile's Scan and Secure Feature Addresses Unwanted Tracking. Retrieved October 2022, from https://www.tile.com/en-us/blog/tile-introduces-scan-and-secure-feature-unwanted-tracking-safety.

Tile. (n.d.). How Tile Works. Retrieved October 2022, from https://www.tile.com/en-CA/how-it-works.

Titley, G., Keen, E., & Foldi, L. (2014). *Starting Points for Combatting Hate Speech Online*. Strasbourg, France: Council of Europe, Youth Division.

TMU (Toronto Metropolitan University). (2022). Cybersecurity, Data Protection and Digital Forensics. Retrieved June 2022, from https://continuing.torontomu.ca/public/category/courseCategoryCertificateProfile.do?method=load&certificateId=170590.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131-148.

TPSB (Toronto Police Services Board). (2022). Use of Artifical Intelligence Technology. Retrieved June 2022, from https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

Triggs, G. (2019). Why an Australian Charter of Rights is a Matter of National Urgency. Retrieved January 2022, from https://theconversation.com/why-an-australian-charter-of-rights-is-a-matter-of-national-urgency-121411.

Tripp, H. (2019). All sex workers deserve protection: How FOSTA/SESTA overlooks consensual sex workers in an attempt to protect sex trafficking victims. *Penn State Law Review, 124*(1), Article 6.

Trudel, P. (2021). Fausses nouvelles et réseaux sociaux. In C. Hervé & M. Stanton-Jean (Eds.), Éthique, intégrité scientifique et fausses nouvelles. Paris, France: Dalloz.

Tsekouras, P. (2021). Apple Tracking Devices Being Used in Thefts of High-End Cars in York Region: Police. Retrieved March 2022, from https://toronto.ctvnews.ca/apple-tracking-devices-being-used-in-thefts-of-high-end-cars-in-york-region-police-1.5690819.

Tsui, J. (2020). Why Gender-Neutral Facial Recognition Will Change How We Look at Technology. Retrieved April, 2022, from https://www.technologynetworks.com/informatics/articles/why-gender-neutral-facial-recognition-will-change-how-we-look-at-technology-332962.

Tunney, C. (2022). Federal Government Invokes Emergencies Act for First Time Ever in Response to Protests, Blockades. Retrieved April 2022, from https://www.cbc.ca/news/politics/trudeau-premiers-cabinet-1.6350734.

Twitter. (2021a). An Update Following the Riots in Washington, DC. Retrieved November 2021, from https://blog.twitter.com/en_us/topics/company/2021/protecting--the-conversation-following-the-riots-in-washington--.

Twitter. (2021b). Our Range of Enforcement Options. Retrieved August 2021, from https://help.twitter.com/en/rules-and-policies/enforcement-options.

Tworek, H. & Leerssen, P. (2019). *An Analysis of Germany's NetzDG Law.* Philadelphia (PA): Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression.

Tworek, H. (2020). *How a Public Health Approach Could Help Curb the Infodemic.* Waterloo (ON): Centre for International Governance Innovation.

Tworek, H. (2021a). History Explains Why Global Content Moderation Cannot Work. Retrieved March 2022, from https://www.brookings.edu/techstream/history-explains-why-global-content-moderation-cannot-work/.

Tworek, H. (2021b). Fighting hate with speech law: Media and German visions of democracy. *The Journal of Holocaust Research, 35*, 106-122.

Tworek, H. (2022). *Authorities Were Warned about Extremist Fundraising Online but Did Not Seem to Hear.* Waterloo (ON): Centre for International Governance Innovation.

Tworek, H. & Wanless, A. (2022). Time for Transparency From Digital Platforms, But What Does That Really Mean? Retrieved March 2022, from https://www.lawfareblog.com/time-transparency-digital-platforms-what-does-really-mean.

U.K. Parliament (Parliament of the United Kingdom). (2022a). *Online Safety Bill.* London, United Kingdom: House of Commons.

U.K. Parliament (Parliament of the United Kingdom). (2022b). *Online Safety Bill [As Amended on Report].* London, United Kingdom: House of Commons.

U.S. House of Representatives. (2018). *Allow States and Victims to Fight Online Sex Trafficking Act of 2017.* Washington (DC): U.S. House of Representatives.

Ullmann, S. & Tomalin, M. (2020). Quarantining online hate speech: Technical and ethical perspectives. *Ethics and Information Technology, 22*, 69-80.

UN (United Nations). (1948). *Universal Declaration of Human Rights.* Paris, France: United Nations General Assembly.

UN (United Nations). (1966). *International Covenant on Civil and Political Rights.* Vol. 999. Paris, France: United Nations General Assembly.

UN (United Nations). (2007). *United Nations Declaration on the Rights of Indigenous Peoples.* Paris, France: United Nations General Assembly.

UN HRC (United Nations Human Rights Council). (2011a). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue.* Geneva, Switzerland: UN.

UN HRC (United Nations Human Rights Council). (2011b). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework.* Geneva, Switzerland: UN.

UN News (United Nations News). (2020). Online Predators Put Millions of Children at Risk During COVID-19 Pandemic Shutdown. Retrieved August 2021, from https://news.un.org/en/story/2020/04/1061742.

UNESCO (United Nations Educational, Scientific and Cultural Organization). (2018). Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training. Retrieved June 2022, from https://en.unesco.org/fightfakenews.

United States Congress. (2018). *CLOUD Act*. Washington (DC): United States Congress.

United States Congress. (2022). *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022*. Washington (DC): United States Congress.

UNODC (United Nations Office on Drugs and Crime). (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. Vienna, Austria: United Nations.

Uscinski, J. E. & Parent, J. M. (2014). Who Are the Conspiracy Theorists? In J. E. Uscinski & J. M. Parent (Eds.), *American Conspiracy Theories*. New York (NY): Oxford University Press.

Vaccari, C. & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1), 2056305120903408.

Van Cauwenberghe, C. (2015). Canada: Amendments to PIPEDA Give Financial Institutions New Artillery in Fighting Financial Abuse. Retrieved October 2022, from https://www.mondaq.com/canada/financial-services/438616/amendments-to-pipeda-give-financial-institutions-new-artillery-in-fighting-financial-abuse.

Van Puyvelde, D., Coulthart, S., & Hossain, M. S. (2017). Beyond the buzzword: Big data and national security decision-making. *International Affairs, 93*(6), 1397-1416.

Velásquez, N., Leahy, R., Johnson Restrepo, N., Lupu, Y., Sear, R., Gabriel, N., . . . Johnson, N. F. (2021). Online hate networks spreads malicious COVID-19 content outside the control of individual social media platforms. *Scientific Reports, 11*, 11549.

Vidal-Tomás, D. (2022). Which cryptocurrency data sources should scholars use? *International Review of Financial Analysis, 81*, 102061.

Vigderman, A. & Turner, G. (2022). 2022 VPN Usage Statistics. Retrieved October 2022, from https://www.security.org/vpn/statistics/.

Vincent, J. (2020). Twitter is bringing its 'Read Before you Retweet' Prompt to All Users. Retrieved June 2021, from https://www.theverge.com/2020/9/25/21455635/twitter-read-before-you-tweet-article-prompt-rolling-out-globally-soon.

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research, 17*(2), 183-194.

von Sikorski, C. (2021). Visual polarisation: Examining the interplay of visual cues and media trust on the evaluation of political candidates. *Journalism, 23*(9), 1900-1918.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151.

Wachter, S. & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review, 2019*(2), 494-620.

Wagner, A. (2022). Tolerating the trolls? Gendered perceptions of online harassment of politicians in Canada. *Feminist Media Studies, 22*(1), 32-47.

Waldman, A. E. (2018). *Privacy as Trust: Information Privacy for an Information Age*. New York (NY): Cambridge University Press.

Walker, J. (2018). *Hate Speech and Freedom of Expression: Legal Boundaries in Canada*. Ottawa (ON): Library of Parliament.

Waller, I. & Anderson, A. (2021). Quantifying social organization and political polarization in online platforms. *Nature, 600*(7888), 264-268.

Walter, M., Kuktai, T., Carroll, S. R., & Rodriguez-Lonebear, D. (2020). *Indigenous Data Sovereignty and Policy*. London, United Kingdom: Routledge.

Wanamaker, K. (2019). *Profile of Canadian Businesses who Report Cybercrime to Police: The 2017 Canadian Survey of Cyber Security and Cybercrime*. Ottawa (ON): Public Safety Canada.

Wang, J., Nansel, T. R., & Iannotti, R. J. (2011). Cyber bullying and traditional bullying: Differential association with depression. *Journal of Adolescent Health, 48*(4), 415-417.

Watson, C. & Huey, L. (2020). Technology as a source of complexity and challenge for special victims unit (SVU) investigators. *International Journal of Police Science & Management, 22*(4), 419-427.

Weaver, N. (2021). The Ransomware Problem Is a Bitcoin Problem. Retrieved June 2022, from https://www.lawfareblog.com/ransomware-problem-bitcoin-problem.

Weimann, G. (2016). Terrorist migration to the dark web. *Perspectives on Terrorism, 10*(3), 40-44.

Wells, R. (2019). The Trauma of Revenge Porn. Retrieved December 2022, from https://www.nytimes.com/2019/08/04/opinion/revenge-porn-privacy.html.

Wells, R. (n.d.-a). Bekah Wells Attorney-at-Law. Retrieved February 2022, from https://www.bekahwells.com/.

Wells, R. (n.d.-b). Women Against Cyberrape. Retrieved February 2022, from https://www.womenagainstcyberrape.com/.

West, L. & Forcese, C. (2020). Twisted into knots: Canada's challenges in lawful access to encrypted communications. *Common Law World Review, 49*(3-4), 182-198.

Westlake, B., Bouchard, M., & Frank, R. (2012). *Comparing Methods for Detecting Child Exploitation Content Online.* Paper presented at European Intelligence and Security Informatics Conference, Odense, Denmark.

Willey, J. (2018). Houston Woman Says Ex Used 'Tile' Device to Stalk Her Repeatedly. Retrieved October 2022, from https://abc13.com/houston-woman-harassment-high-tech-device-stalking/3719155/.

Williams, M. L., Burnap, P., Javed, A., Liu, H., & Ozalp, S. (2020). Hate in the machine: Anti-black and anti-muslim social media posts as predictors of offline racially and religiously aggravated crime. *British Journal of Criminology, 60*(1), 93-117.

Williams, T. (2017). Backpage's Sex Ads are Gone. Child Trafficking? Hardly. Retrieved December 2022, from https://www.nytimes.com/2017/03/11/us/backpage-ads-sex-trafficking.html.

Windwehr, S. & York, J. C. (2020). Facebook's Most Recent Transparency Report Demonstrates the Pitfalls of Automated Content Moderation. Retrieved November 2021, from https://www.eff.org/deeplinks/2020/10/facebooks-most-recent-transparency-report-demonstrates-pitfalls-automated-content.

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus, 109*(1), 121-136.

Winter, J. (2019). FBI Document Warns Conspiracy Theories Are a New Domestic Terrorism Threat. Retrieved November 2021, from https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cubnl0aW1lc%E2%80%A6.

Wright, J. M., Chun, W. H. K., Clarke, A., Herder, M., & Ramos, H. P. (2022). *Protecting Expert Advice for the Public: Promoting Safety and Improved Communications*. Ottawa (ON): Royal Society of Canada.

Yar, M. & Drew, J. (2019). Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales. *International Journal of Cyber Criminology, 12*(2), 578-594.

YouTube. (2019). Continuing Our Work to Improve Recommendations on YouTube. Retrieved November 2021, from https://blog.youtube/news-and-events/continuing-our-work-to-improve/.

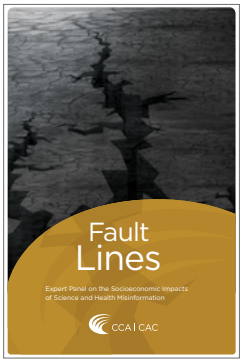
YRP (York Regional Police). (2021). Vehicle Theft Warning and Prevention Tips. Retrieved January 2022, from https://www.yrp.ca/en/Modules/News/index.aspx?newsId=167fa5b3-3583-431d-8cc0-91e49aee3bff.

Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA Forum, 20*(4), 567-583.

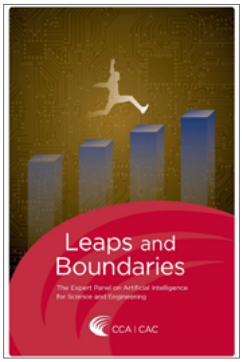
Zimmer, K. (2022). *Utilizing the Courts for an Online Reputational Scrub, and the Potential Emergence of a Right to Be Forgotten in Canada*. Vancouver (BC): Continuing Legal Education Society of British Columbia.

CCA Reports of Interest

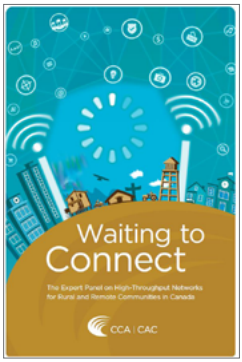
The assessment reports listed below are accessible through the CCA's website (www.cca-reports.ca):



Fault Lines (2023)

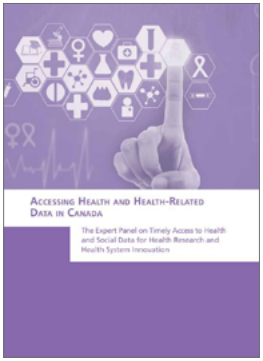


Leaps and Boundaries (2022)

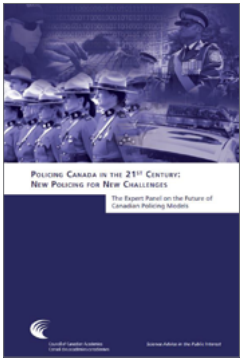


Waiting to Connect (2021)

Toward Peace, Harmony, and Well-Being: Policing in Indigenous Communities (2019)



Accessing Health and Health-Related Data in Canada (2015)



Policing Canada in the 21st Century: New Policing for New Challenges (2014)

CCA Board of Directors*

*As of March 1, 2023

CCA Scientific Advisory Committee*

David Castle (Chair), Professor, School of Public Administration and Gustavson School of Business, University of Victoria; Researcher in Residence, Office of the Chief Science Advisor to the Prime Minister of Canada (Victoria, BC)

Maydianne C. B. Andrade, Professor, Biological Sciences, University of Toronto Scarborough; President, Canadian Black Scientists Network (Toronto, ON)

Peter Backx, FRSC, Professor, Department of Biology, and Canada Research Chair in in Cardiovascular Biology, York University (Toronto, ON)

Kyle Bobiwash, Assistant Professor and Indigenous Scholar, Department of Entomology, University of Manitoba (Winnipeg, MB)

Stephanie E. Chang, Professor, School of Community and Regional Planning and Institute for Resources, Environment and Sustainability, University of British Columbia (Vancouver, BC)

Jackie Dawson, Canada Research Chair in Environment, Society and Policy, and Associate Professor, Department of Geography, University of Ottawa (Ottawa, ON)

Colleen M. Flood, FRSC, FCAHS, Director, Centre for Health Law, Policy and Ethics; Professor, Faculty of Law (Common Law Section), University of Ottawa (Ottawa, ON)

Digvir S. Jayas, O.C., FRSC, FCAE, Distinguished Professor and Vice-President (Research and International), University of Manitoba (Winnipeg, MB)

Malcolm King, FCAHS, Scientific Director, Saskatchewan Centre for Patient-Oriented Research, University of Saskatchewan (Saskatoon, SK)

Chris MacDonald, Associate Professor; Director, Ted Rogers Leadership Centre; Chair, Law and Business Department; Ted Rogers School of Management, Toronto Metropolitan University (Toronto, ON)

Nicole A. Poirier, FCAE, President, KoanTeknico Solutions Inc. (Beaconsfield, QC)

Louise Poissant, FRSC, Scientific Director of Fonds de recherche du Québec – Société et culture (Montréal, QC)

Jamie Snook, Executive Director, Torngat Wildlife Plants and Fisheries Secretariat (Happy Valley-Goose Bay, NL)

David A. Wolfe, Professor of Political Science, University of Toronto Mississauga; Co-Director, Innovation Policy Lab, Munk School of Global Affairs and Public Policy, University of Toronto (Toronto, ON)

*As of March 1, 2023

Council of Canadian Academies | Conseil des académies canadiennes

180 Elgin Street, Suite 1401
Ottawa ON K2P 2K3
Tel: 613 567-5000
www.cca-reports.ca