

# Securing Public Interest Cybersecurity Researchers in Canadian Universities

Adam Molnar

## Overview

Rooted in democratic ideals, public interest cybersecurity research is essential for understanding the complex relationship between cybersecurity, human rights, and social justice. Universities, with their long tradition of independent inquiry, provide a crucial space for challenging the dominant influence of private industry in shaping our understanding of cybersecurity. Researchers in these institutions are uniquely positioned to generate knowledge that goes beyond profit-driven narratives and encompass a wider range of concerns, including those of civil society organizations, activists, journalists, and marginalized communities. However, researchers employing established computer security methods in public interest cybersecurity work at Canadian universities face their own crisis of the “security of self” due to substantial legal uncertainties surrounding the lawful permissibility of their research. These uncertainties not only threaten the personal and professional security of researchers, but also hinders the ability to contribute to a broader critical understanding of cybersecurity risks, ultimately limiting our collective “security of self” in the digital age.

Building upon Deibert’s (2018) call for a human-centric approach to cybersecurity that prioritizes digital security alongside public interest values, this chapter argues that the legal ambiguities surrounding cybersecurity research in Canadian universities threaten researchers’ ability to conduct meaningful research in the public interest. It examines common methodological practices in this field and their interaction with legal considerations, exploring implications under criminal and copyright law, as well as civil issues like breach of contract and negligence. By scrutinizing potential interpretations of computer security methods under relevant law, the chapter highlights the need to protect researchers and foster an environment conducive to critical knowledge production in human-centred cybersecurity. Ultimately, it poses a series of recommendations for governments to strengthen legal safeguards for public interest cybersecurity research in Canadian universities.

## Introduction

Driven by a commitment to democratic principles and social justice, public interest cybersecurity research plays a vital role in examining the complex interplay between cybersecurity, human rights, and digital security. Universities, with their long tradition of critical independent inquiry, can serve as crucial sites for challenging the dominance of private industry in shaping imaginaries about “who” and “what” constitutes cybersecurity issues. University researchers are uniquely positioned to generate knowledge that diverges from market-driven trends, broadening the narrative of cybersecurity beyond commercial interests to encompass the threats faced by non-profit organizations, activists, journalists, and marginalized communities. This research prioritizes the often-overlooked human element of cybersecurity and privacy threats. However, the Canadian university environment presents significant challenges for researchers seeking to utilize established computer security

methods in public interest cybersecurity research due to considerable legal uncertainty surrounding the permissibility of their work.

Building on Deibert's (2018) call for a "critical cybersecurity approach" that aligns digital security with human-centric, this chapter argues that the legal ambiguities surrounding public interest cybersecurity research in Canadian universities pose a significant threat to researchers. This uncertainty can hinder the production of knowledge about cybersecurity risks that extend beyond narrowly defined commercial interests, ultimately limiting our understanding of the diverse threats faced by individuals and communities in the digital age.

This chapter offers an in-depth analysis of common methodological practices in public interest cybersecurity research and their legal implications. It examines these practices through the lens of relevant Canadian law, including the *Criminal Code*, the *Copyright Act*, and civil law considerations such as breach of contract and negligence. By scrutinizing the potential interpretations of computer security methods under existing statute and case law (where it exists), the chapter provides a thorough examination of the legal risks faced by researchers. Ultimately, it argues that protecting the "human security" of university researchers and fostering a robust environment for critical, independent, human-centred cybersecurity research requires the Canadian government to establish strong legal protections for this vital work.

Section 1 establishes the context for how the cybersecurity industrial complex shapes cybersecurity knowledge, emphasizing the unique contribution that university research can offer in understanding human-centred cybersecurity issues. Section 2 examines the potential threats to this critical research within universities. It introduces computer security methods commonly used in public interest cybersecurity research and analyzes how these methods can be opportunistically interpreted, leading to various legal liabilities for researchers in Canadian institutions, as discussed in Section 3. Section 4 proposes recommendations to protect the "human security" of cybersecurity and privacy researchers at Canadian universities. Overall, this chapter argues that strengthening these protections through robust statutory measures is essential for Canada to advance a comprehensive cybersecurity policy that harnesses the critical potential of university research.

## 1. The University as a Locus for Public Interest Cybersecurity Research

"Cybersecurity," as a body of knowledge and set of practices, is significantly influenced by both state and corporate interests. A primary source of information regarding cybersecurity and threats is derived from commercial threat reporting. Private cybersecurity organizations produce threat intelligence reports that gather and analyze data on cyber risks, ultimately guiding awareness and influencing strategies for securing communication infrastructure.

Commercial threat intelligence reports contain valuable details such as attacker techniques, information about vulnerabilities, and analyses of emerging threats and trends. However, these reports also serve a strategic purpose for the cybersecurity firms that produce them. As Maschmeyer et al. (2021) point out, an entrepreneurial strategy drives the production of these reports, designed to project expertise and bolster reputations to attract clients. This means that threat intelligence is carefully curated to align with profit-maximizing goals of cybersecurity firms, leading to distortions in the overall threat landscape presented.

Commercial threat intelligence reports are powerful cultural artifacts, serving as the primary, and often only, source of data on cyberconflict (Maschmeyer et al., 2021, p. 2). This gives them immense power to define the boundaries of what is known about cyberconflict, constructing narratives that highlight certain actors and

trends while sidelining others. Their influence extends into the political sphere, where these reports, bolstered by perceptions of expertise, significantly shape the perspectives of government policy-makers, industry stakeholders, and even researchers.

What version of “cyberconflict” and “cybersecurity” actors, threats, and vulnerabilities are foregrounded, and which fade to the background or are made invisible altogether? First, according to Maschmeyer et al. (2021, p. 3) and Work (2021), commercial threat intelligence reports primarily focus on cybercrime, economic espionage, and sabotage of critical infrastructure. This focus systematically excludes the range of threats encountered by civil society organizations vital for democracy, such as human rights defenders, journalists, and environmental activists. As a result, these reports primarily reflect the specific security interests of “high-profile victims,” such as government, military, and Fortune 500 companies.

Second, these reports often highlight “high-profile threat actors” often viewed as adversaries of Western/North American interests, like Russia, China, Iran, and North Korea, particularly since threat intelligence firms cater to a largely US audience. This emphasis can obscure the security vulnerabilities generated through US and European cyber operations and their supporting policies.

Third, within this narrow portrayal, producers of commercial threat intelligence reports often emphasize the “unique” or “spectacular,” such as zero-day vulnerabilities or novel attack techniques. This focus on the dramatic can distract from the persistent digital threats faced by less prominent groups. Moreover, these reports tend to frame cyber risks primarily as technological vulnerabilities with technological solutions. This perspective neglects the human and socio-political dimensions of digital threats, overlooking risks that don’t depend on sophisticated tools typically associated with well-resourced nation-state actors. Ultimately, this skewed representation of the threat landscape has real consequences. It influences decision-making, strategy, and resource allocation in cybersecurity, shaping what is, and isn’t, possible in the public interest.

Independent research, less entangled with profit-seeking motives, can more adequately embrace a human-centric approach to cybersecurity (Deibert, 2018). This approach, detached from the imperatives of capital accumulation, prioritizes principles such as fairness, justice, free expression, freedom of association, enabling a critical examination of power dynamics and exploitation. It sheds light on the digital threats faced by marginalized groups such as civil society organizations, human rights advocates, Indigenous communities, and environmental defenders (Deibert, 2018). It also allows for exploration of the gendered dimensions of cyber risks (Harkin et al., 2020) and exposes how private corporations often fail to protect vulnerable groups, focusing instead on product-based solutions (Harkin & Molnar, 2021). Moreover, it can critically examine how the pursuit of “cybersecurity” itself can be used to undermine freedoms and facilitate social control (Deibert et al., 2017).

Universities are vital hubs for pursuing human-centric cybersecurity research in the public interest. While the pervasive influence of neoliberalism within academia often prioritizes applied research, technology transfer, and industry partnerships with an overriding focus on commercial viability, universities still offer a crucial space for conducting research that aligns with broader societal needs and democratic values.

The Citizen Lab at the Munk School of Global Affairs and Public Policy at the University of Toronto provides a compelling example of public interest cybersecurity research. They have a long track record of investigating digital threats targeting civil society organizations, journalists, and political refugees (Citizen Lab, 2023). Employing a multidisciplinary approach, they combine techniques from network measurement, information security, law, and social sciences to expose threats to digital security, human rights, and democracy. For instance, their research into the cybersecurity risks of mercenary spyware has led to the discovery of multiple vulnerabilities in Apple iOS. In another notable project, they investigated information

communication technologies used for content filtering, revealing how vendors sell computer networking devices, commonly known as “middleboxes,” to authoritarian governments to censor content, including material related to LGBTQ+ issues (Dalek et al., 2021).

In the context of corporate accountability research, a key objective is to identify security and privacy risks associated with specific technologies and their impact on democratic freedoms and human rights. This research often involves using established computer science methods to analyze the technical capabilities and data-sharing practices of vendors and their technologies. While these forensic methods are central to building an independent human-centric approach to cybersecurity research, and addressing critical information gaps within the cybersecurity field more broadly, their use is shrouded in legal uncertainty.

To explore this tension further, this chapter will now delve into two common techniques used in this research: reverse engineering and network traffic analysis. By examining these techniques as case studies, we can gain a deeper understanding of the legal challenges faced by researchers working in the public interest. This analysis will encompass the ethical protocols followed when these methods uncover technical vulnerabilities and how these practices intersect with the current legal landscape governing such research, ultimately highlighting the risks posed to researchers.

## 2. The Ubiquitous Use of Computer Security Methods

Computer security and other technical methods often involve observing and analyzing software applications and information communications systems. These techniques are widely used by computer security researchers at universities worldwide to understand how computer systems operate, identify security vulnerabilities, and ultimately improve the security of computer systems and networks. In the context of a public interest and human-centred approach to cybersecurity, these methods can be used to defend vulnerable communities, protect civil liberties, and promote transparency and accountability.

One common technique is reverse engineering (RE), which involves deconstructing a product or technology to learn more about its design, functionality, and underlying code. For digital technologies and computer systems, RE typically involves disassembling or decompiling machine-readable binary code into a more human-readable format, such as a programming language. This allows researchers to analyze software for security flaws, vulnerabilities, or other design and operational features. Researchers often acquire the technology by obtaining a license from the vendor, which may involve agreeing to terms of service.

Another common technique is network traffic analysis, which involves monitoring and analyzing network traffic data to identify anomalies. This technique has various applications in cybersecurity research (and digital research more broadly), such as conducting security audits to determine if an application uses encryption, learning about the server infrastructure of a product or service (including its geographical location), and detecting malware and botnets by identifying abnormal traffic patterns.

Researchers at Canadian universities use these methods to uncover and report vulnerabilities, leading to security updates for major tech companies like Apple and Google (among others), ultimately enhancing the privacy and data security of billions of devices and users worldwide. These researchers adhere to robust ethical obligations, including, obtaining approval from university research ethics boards (REBs) that enforce the Tri-Council Policy Statement (TCPS 2, 2018), where required. Furthermore, researchers also follow rigorous procedural standards, such as coordinated vulnerability disclosure (CVD) programs, which govern the responsible reporting of information about software vulnerabilities discovered during research. To fully assess

the legal implications of these computer security and technical methods and understand the risks researchers face, it is essential to first examine the ethical frameworks that guide this research and how those frameworks are embodied in CVD protocols.

### 3. Coordinated Vulnerability Reporting

Public interest cybersecurity research often employs a CVD policy, a framework for responsibly and promptly reporting security flaws. When researchers acting in good faith discover a software vulnerability, they initiate the CVD process to mitigate potential harm. This typically involves reporting the vulnerability to the software vendor, either directly or through a neutral coordinating party. The vendor then assesses the severity and risk, and typically has a 30- to 60-day window to develop and issue a patch.

However, responsible disclosure extends beyond simply reporting the vulnerability in a carefully managed way. Ethical CVD practices also emphasize minimizing the collection, use, and disclosure of copyrighted material during the course of the research process, limiting what is strictly necessary for proof of concept, as highlighted in cases like *Proctorio v. Linkletter* (2022 BCSC 400, para. 83; 2023 BCCA 160, para. 32). Once the vendor has addressed the vulnerability, researchers may choose to disclose their findings more broadly. This may include reporting to the Canadian Centre for Cyber Security, which plays a similar role in Canada to CERT/CC in the US, particularly if the vulnerability has broader implications for Canadian internet infrastructure. At this final stage, researchers may choose to disseminate their findings through various channels, such as publishing in scholarly journals, presenting at conferences, or contributing to public awareness initiatives.

CVDs is a framework designed to minimize harm by fostering collaboration and transparency between security researchers and vendors. It encourages prompt remediation of vulnerabilities and promotes trust by establishing clear communication channels and timelines. Ideally, CVDs incentivize vendors to enhance the security of their products and services, and ensure researchers adhere to established best-practice standards for vulnerability reporting (Householder et al., 2017).

However, the practical reality of vulnerability disclosure is often more complicated. While CVDs provide ethical research protocols, they don't always guarantee legal protection for researchers. Vendors may favour their own Vulnerability Disclosure Policies (VDPs), which can be unilaterally imposed and vary significantly in their terms and scope. This can create legal uncertainty for researchers, even when adhering to CVD best practices. Some vendors might exploit proactive disclosure by security researchers, using the CVD process as an opportunity to threaten or intimidate them with legal action to prevent or delay public disclosure, often due to concerns about potential liabilities or reputational risk associated with the vulnerability.

Where poorly formulated VDPs can exacerbate legal uncertainty, well-formulated VDPs can mitigate risk by providing explicit and irrevocable authorization for security research. A well-crafted VDP would take careful steps to clarify legal boundaries within various regimes (e.g. criminal, copyright, contract, etc.). Notably, there are multiple efforts currently being made to promote the standardization and adoption of "researcher-friendly" VDPs, including from the National Institute of Standards and Technology (NIST) in the US, the European Union Agency for Cybersecurity (ENISA) in the EU, the Canadian government's aim to formulate a government-wide CVD, and commercial efforts like HackerOne's VDP map and Bugcrowd's disclose.io platform. These initiatives, alongside ongoing advocacy for responsible disclosure practices, are essential for fostering a legal environment that supports public interest cybersecurity research.

Despite the crucial role of CVDs in promoting responsible disclosure, security researchers in Canadian universities often navigate these processes without the support of institutional policies. While researchers generally adhere to ethical guidelines, Canadian universities have largely overlooked the establishment of internal CVD policies to guide research, despite the potential public benefit. This lack of formal guidance could leave researchers more vulnerable to the inconsistencies of externally imposed VDPs, which may offer inadequate protection or impose overly restrictive terms. Even when researchers closely follow CVD protocols and adhere to responsible disclosure practices, they may still face a raft of legal risks stemming from the ambiguous legal landscape surrounding public interest cybersecurity research in Canada.

## 4. Assessing the Legal Risk

### 4.1. Criminal Code

Regarding the *Criminal Code*, if research is conducted within an ethical and controlled environment, the risk of criminal violation should be minimal. Specifically, ss. 342.1(1)(a) and (b) of the *Criminal Code* prohibit, respectively, fraudulently and without colour of right, obtaining any computer service, and intercepting any function of a computer system. These arcane terms are further defined in s. 342.1(2) to mean using any data processing or retrieval functions or observing any functions of a computer program without authorization. The term “colour of right” refers to an honest belief in a legal right to possess or access something, even if that belief is mistaken. While the requirement for fraudulently seems to suggest a subjective element of dishonest intent, Canadian courts have interpreted the *men rea* requirement to be that the computer was “used intentionally, without mistake, with subjective knowledge that the use is unauthorized” (*R. v. McNish*, 2020 ABCA 249, para 58; see also *R. v. Parent*, 2012 QCCA 1653, paras 50; *Manning v. Canada*, File No 0018-C1-00135-01 [CA IRB], paras 53–61). In short, the accused does not have to subjectively believe their use is blameworthy (*McNish*, para 59). Given broad interpretations of unauthorized computer use in Canada under *R. v. Parent*, *R. v. McNish*, and *R. v. Manning*, where the objective standard has largely focused on intentional access with knowledge that it is unauthorized, there is further ambiguity for interpreting university research, even if the intent of the researcher is to responsibly disclose any vulnerabilities discovered.

This is in contrast to the legal landscape in the USA, where the *Computer Fraud and Abuse Act* has been interpreted narrowly by the United States Supreme Court in *van Buren v. United States* (2021, 141 S. Ct. 1648). The Court held that the crime of exceeding authorized access to a computer does not apply to everyday violations of computer use policies. In this case, a police officer was found to have not exceeded his authorized access when he used a police database to look up a license plate number for unofficial purposes in exchange for money (see Mackey & Opsahl, 2021). A vendor VDP, if properly formulated, could clarify the requisite authorization. In any case, provisions under the Canadian *Criminal Code* lack explicit exemptions for independent public interest computer security research. The absence of such exclusions means that authorities possess broad discretion in interpreting certain forms of independent security research, potentially leaving researchers vulnerable due to this ambiguity.

### 4.2. Copyright Act

The *Copyright Act* is often regarded as a delicate balance, aiming to provide protections to copyright owners while simultaneously fostering the creative generation and exchange of ideas and information deemed crucial for a healthy democratic society (*Théberge v. Galerie d'Art du Petit Champlain Inc.*, 2002 SCC 34, at

para 30). While this Act grants copyright owners exclusive rights to control their protected works, it also grants general rights to users and exceptions for specific groups, including educators, journalists, and public interest researchers. Concerning public interest cybersecurity researchers, certain forms of reverse engineering methods may potentially constitute infringing activities. Specifically, these methods may involve making copies of vendors' software programs and bypassing technological protection measures to access software. However, these methods may also fall under certain "user rights" exceptions. User rights, particularly relevant to reverse engineering methods, are delineated in sections related to encryption research (s. 30.62), security (s. 30.63), and fair dealing (ss. 29 and 29.1).

The exception for conducting encryption research is complex. It applies when it is necessary to make a copy of a computer program to conduct the research (s. 30.62 1a), as long as the program was lawfully obtained (s. 30.62.1b), and the researcher notified the owner of the copyrighted material about their intention to conduct the research (s. 30.62.1c). However, the obligation for cybersecurity researchers to inform vendors of their research intentions has exceptions. Notification may be exempted if "the public interest in making the vulnerability or security flaw public without prior notice outweighs the owner's interest in receiving that notice" (s. 30.62[3]). Due to the limited requirement for advanced notification, it is conceivable that vendors could take legal action to impede the research. For public interest cybersecurity researchers, this notification requirement could potentially hinder the meaningful execution and dissemination of independent critical research.

The *Copyright Act* offers a similar exception to copyright infringement for researchers regarding the reproduction of software for security research:

It is not an infringement of copyright for a person to reproduce a work or other subject-matter for the sole purpose, with the consent of the owner or administrator of a computer, computer system or computer network, of assessing the vulnerability of the computer, system or network or of correcting any security flaws. (s. 30.63[1]).

Similar to encryption research, if security researchers want to make public a security vulnerability, they must notify the copyright owner, except if the public interest outweighs giving this notice (s. 30.63[3]). While it appears that researchers making copies of software for public interest cybersecurity research enjoy exceptions under the Act, there is currently no case law that could provide further clarification regarding the definitions and boundaries of "encryption" or "security research."

Sections 30.62 and 30.63 solely exempt the act of reproducing a work—and courts have yet to clarify the scope of the provision. However, the *Copyright Act* also prohibits the circumvention of technological protection measures (TPMs) that "control[] access to a work" (s. 41). Circumventing TPMs might encompass activities such as "descrambling a scrambled work or decrypting an encrypted work," (s. 41 or other actions like "bypassing, removing, deactivating, or impairing the technological protection measure" [s.41]). In the context of reverse engineering (RE), it remains unclear whether circumventing a TPM violates copyright unless authorized by the copyright owner (s. 41.1). However, it is important to note that exceptions to the TPM prohibition, such as those for encryption or security research, may be relevant to reverse engineering activities.

For instance, the circumvention of TPMs doesn't apply to a person conducting encryption research if "it would not be practical to carry out the research without circumventing the technological protection measure" (s. 41.13[1][a]), provided "the person has lawfully obtained the work" (s. 41.13[1][b]), and "the person has informed the owner of the copyright in the work" (s. 41.13[1][c]). Likewise, the prohibition on the circumvention of TPMs doesn't apply to a person conducting security research, granted it's done "with the consent of the owner or administrator of a computer, computer system, or computer network," where the sole

purpose is “assessing the vulnerability of the computer, system, or network or correcting any security flaws” (s. 41.15(1)). These exceptions to anti-circumvention provisions, while vital for guiding security research, introduce authorization requirements that can complicate the conduct of free and fair public interest security research.

Fair dealing exceptions also exist for the purpose of research and education (s. 29). The Supreme Court has established six factors that guide the fair dealing analysis: (1) the purpose of the dealing, (2) the character of the dealing, (3) the quantity or amount of the dealing, (4) whether alternatives to the dealing existed, (5) the nature of the work, and (6) the effect of the dealing on the market for the work (*CCH Canadian Ltd. v. Law Society of Upper Canada*, 2004 SCC 13, at para 53). In the context of university security researchers, the strength of fair dealing exceptions as a defence remains unclear. However, it’s crucial to recognize that conducting encryption or security research often involves circumventing some form of TPM. Fair dealing remains a complex area of law characterized by the absence of clear bright-line rules, particularly in the realm of public interest cybersecurity research. Given this legal ambiguity, it is a matter of subjective interpretation regarding what constitutes fair dealing in the context of public interest cybersecurity research. Again, while not a reliable solution, a vendor’s VDP, if properly formulated, could streamline requirements relating to copyright and fair dealing by providing clear guidance on what types of research are permitted and what conditions must be met.

### 4.3. Contract Law

Terms of Service (ToS) agreements are another source of tension for university researchers using computer security methods. Acquiring access to software for analysis often requires agreeing to a ToS or end-user license agreement (EULA). ToS agreements set out the legal rights, responsibilities, and restrictions between the service provider and end users. While some provisions of ToS have been declared unenforceable, they are binding contracts in Canada. ToS set out the scope of activities relating to what the end user is allowed to do with the software, for example, whether the software can be installed on one or multiple devices or whether the end user is able to make copies of the software. VPD conditions can be incorporated by reference through a ToS or EULA, imposing restrictions on the conditions of disclosure. It is an open question, however, whether these (or other ToS/EULAs) are ultimately enforceable against security researchers entering into a contract of adhesion as a customer (see, e.g. *Century 21 Canada Limited Partnership v. Rogers Communications Inc.*, 2011 BCSC1196, paras 120, 122).

In any case, regarding RE activities to conduct security research, ToS may not expressly mention using the software to undertake RE activities, though in some cases they may even expressly prohibit making copies of software for the purposes of RE. Overall, given the often narrowly defined usage restrictions found in ToS agreements, they introduce legal ambiguity into the production of public interest cybersecurity research. Despite this ambiguity, however, a major limitation is that any software vendor seeking to threaten or intimidate public interest cybersecurity researchers with contract violation must demonstrate damages—which can be challenging—and non-pecuniary damages for harm to their reputation from disclosure of the security vulnerability are rarely awarded. Adhering to coordinated vulnerability disclosure practices can significantly reduce the likelihood of a successful breach of contract claim. This is because vendors typically need to prove they suffered economic damages due to the researcher’s actions. By following responsible disclosure practices, researchers can demonstrate they acted in good faith to minimize any potential harm. While not a guarantee against legal action, this can make it more difficult for vendors to prove they suffered damages, especially when the researcher’s actions are aligned with established best practices. Currently, there are no known cases in Canada where a software company has successfully sued a “good faith” cybersecurity researcher for breach

of contract related to RE for security vulnerability analysis. However, further research should attempt to inquire into the status of unreported cases, settled lawsuits, or documented threats that highlight the potential risks researchers face.

#### 4.4. Anti-SLAPP Motions

If good faith cybersecurity researchers find themselves on the receiving end of litigation that seeks to threaten or intimidate public interest work, potential recourse is available through anti-SLAPP (Strategic Lawsuits Against Public Participation) laws. These laws provide defendants with expedited summary processes for a swift dismissal of a lawsuit. Anti-SLAPP laws vary in application across provinces in Canada. They are currently in force in Ontario, British Columbia, Quebec, and Prince Edward Island. Other provinces, including Alberta, Saskatchewan, Manitoba, New Brunswick, Nova Scotia, and Newfoundland and Labrador, do not yet have anti-SLAPP legislation.

In Ontario, under section 137.1(3) of the *Courts of Justice Act*, the defendant must present a compelling argument to secure a dismissal of the proceeding. Specifically, they must demonstrate that the litigation targets their research as a form of expression connected to the public interest. This includes any form of expression, not just defamation. The plaintiff must also demonstrate that the proceeding has merit, that the defendant lacks a valid defence, and that any resulting harm is a consequence of the expression (s 137.1[4][a] and [b]). A crucial element in the judge's decision is the assessment of the harm inflicted, which must reach a level of severity where allowing the proceeding to continue to outweigh the societal interest in safeguarding the specific expression in question (s 137.1[4][b]). In practical terms, this means that the judge must consider whether the societal value of public interest cybersecurity research, aimed at discovering and mitigating security and privacy risks, outweighs the interests of private sector organizations in being shielded from independent assessment. It's worth noting that, in Canada, anti-SLAPP legislation has not been applied in the context of cybersecurity research. Nevertheless, it is essential to recognize that anti-SLAPP motions have been successful in protecting various legal claims related to the defendant's expressions. Overall, the effectiveness of anti-SLAPP motions as a viable avenue for legal protection in the practice of public interest cybersecurity research remains an open question.

### 5. Securing Research

By shifting the focus from the external cybersecurity landscape affecting the “security of self,” to the conditions governing knowledge production, this chapter underscores the importance of safeguarding researchers who strive to understand and address cyber risks and digital accountability from a human-centred and justice-oriented perspective. These researchers challenge the prevailing information environment on cyber risks, often dominated by narrow economic considerations, and offer crucial insights into the complex interplay between cybersecurity, human rights, and social justice. However, the legal uncertainties surrounding such critical work casts a shadow on the ability to conduct critical research, jeopardizing both current and future efforts to advance knowledge in the public interest. To mitigate these challenges, the chapter proposes the following recommendations:

1. **Establish Clear Legal Protections:** As an interim measure, the Minister of Justice and Attorney General of Canada should immediately issue a non-prosecution directive concerning ss. 342.1 and 430(1.1) of the *Criminal Code* in relation to good-faith security research. This directive would provide immediate relief for researchers facing legal threats or prosecution, aligning with the US Department of

Justice's policy on charging cases under the *Computer Fraud and Abuse Act*, which explicitly discourages prosecution of good-faith security research (see US DOJ, 2022). In the longer term, the government should enact comprehensive legislation that explicitly protects cybersecurity and digital accountability researchers engaged in public interest work. This legislation should clearly define permissible research activities, establish a safe harbour for responsible vulnerability disclosure, and shield researchers from legal threats and repercussions. This could be achieved through a public interest exception in the *Criminal Code* under s. 342.1 (and s. 430[1.1]), and a model security research shield law adopted by provinces to protect responsible security researchers from civil litigation.

2. **Formalize Coordinated Vulnerability Disclosure (CVD) Frameworks:** Promote the widespread adoption of CVD frameworks within Canadian universities as well as the broader cybersecurity community. These frameworks should provide clear guidelines that allow researchers to report vulnerabilities responsibly and without fear of legal repercussion. Further, efforts should be made to standardize VDPs across the industry, potentially through collaboration with standards organizations, to ensure they adequately protect responsible security research.
3. **Enhance Security-Related Exceptions in the *Copyright Act*:** Clarify and strengthen the security research exceptions within the *Copyright Act* to better accommodate the needs of cybersecurity researchers. Ensure these exceptions explicitly cover activities related to vulnerability analysis, including the circumvention of technological protection measures when necessary for security research. To further support these exceptions, policy-makers should explore the possibility of expressly prohibiting private sector vendors from using terms of service to contractually override statutory provisions in the Act that allow fair use exceptions to undertake public interest security research.
4. **Strengthen Anti-SLAPP Legislation:** Expand and enhance anti-SLAPP legislation in all Canadian provinces to offer stronger and more tailored protection for public interest cybersecurity researchers. These laws should provide a robust defence against legal actions designed to intimidate researchers and suppress public interest research.
5. **Support Public Interest Cybersecurity Research:** Increase funding, grants, and other incentives for public interest cybersecurity research programs in Canadian universities. Encourage partnerships between academia, industry, government, and advocacy groups to support research that prioritizes human-centred and justice-oriented approaches to cybersecurity challenges.

Failure to make progress in these areas will undermine the university's essential role in fostering a public interest and human-centred approach to cybersecurity—one that prioritizes human values and justice over the influence of powerful corporate actors and a legal system that can be wielded to serve their interests.

## Acknowledgements

This chapter draws on research supported by the Social Sciences and Humanities Research Council. The author would like to thank Tamir Israel for feedback on parts of an earlier draft of the proposal and an anonymous reviewer for their constructive comments. Any errors or omissions remain the responsibility of the author.

## References

- CCH Canadian Ltd. v. Law Society of Upper Canada*, 2004 SCC 13, [2004] 1 SCR 339
- Century 21 Canada Limited Partnership v. Rogers Communications Inc.*, 2011 BCSC1196
- Citizen Lab (2023). *Citizen Lab Research*. <https://citizenlab.ca/category/research/>
- Copyright Act*, RSC 1985, c. C-42.
- Courts of Justice Act*, RSO 1990, c. C.43.
- Criminal Code*, RSC, 1985, c. C-46.
- Dalek, J., Dumlao, N., Kenyon, M., Poetranto, I., Senft, A., Wesley, C., Filastò, A., Xynou, M., & Bishop, A. (2021). *No Access: LGBTIQ website censorship in six countries*. The Citizen Lab, OutRight Action International, and OONI. <https://citizenlab.ca/2021/08/no-access-lgbtqi-website-censorship-in-six-countries/>
- Deibert, R. J., Gill, L., Israel, T., Legge, C., Poetranto, I., & Singh, A. (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, Ms. Dubravka Šimonović*. The Citizen Lab, Munk School of Global Affairs, University of Toronto. <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>
- Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics & International Affairs*, 32(4), 411–424. DOI: <http://dx.doi.org/10.1017/S0892679418000618>
- Harkin, D., Molnar, A., & Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, media, culture*, 16(1), 33–60. DOI: <http://dx.doi.org/10.1177/1741659018820562>
- Harkin, D., & Molnar, A. (2021). Operating-system design and its implications for victims of family violence: The comparative threat of smart phone spyware for Android versus iPhone users. *Violence against women*, 27(6–7), 851–875. DOI: <http://dx.doi.org/10.1177/1077801220923731>
- Householder, A. D., Wassermann, G., Manion, A., & King, C. (2017). *The CERT guide to coordinated vulnerability disclosure*. Software Engineering Institute.. DOI: <https://doi.org/10.1184/R1/12367340.v1>
- Mackey, A. & Opsahl, K. (2021). Van Buren is a Victory Against Overbroad Interpretations of the CFAA, and Protects Security Researchers. *Electronic Frontier Foundation: Deeplinks Blog*. <https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security>
- Manning v Canada*, (2022) File No 0018-C1-00135-01, (CA IRB)

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. DOI: <http://dx.doi.org/10.1080/19331681.2020.1776658>

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council (2018). *TCPS2. Tri-Council policy statement: Ethical conduct for research involving humans*. <https://ethics.gc.ca/eng/documents/tcps2-2018-en-interactive-final.pdf>

*R v McNish*, (2020) ABCA 249

*R v Parent*, (2012) QCCA 1653

United States Department of Justice (2022). *9–48.000—Computer Fraud and Abuse Act*. <https://www.justice.gov/jm/jm-9-48000-computer-fraud>

Work, J. D. (2020). Evaluating commercial cyber intelligence activity. *International Journal of Intelligence and CounterIntelligence*, 33(2), 278–308. DOI: <https://doi.org/10.1080/08850607.2019.1690877>