National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

The Need to Legally Protect CSIS Employees From Doxings

Ms Nicole Fleming

JCSP 50

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Exercise Solo Flight – Exercice Solo Flight

The Need to Legally Protect CSIS Employees From Doxing

Ms Nicole Fleming

THE NEED TO LEGALLY PROTECT CSIS EMPLOYEES FROM DOXING

1. Introduction

The employee Code of Conduct at the Canadian Security Intelligence Service (CSIS or 'the Service') states their mission is to "protect Canada's national security interests and the safety of Canadians".[1] In order to do so, many CSIS employees[2] willingly embrace the fact they must interact with, and collect information from persons who are suspected of terrorist activities or who engage in espionage.[3] There is unquestionable risk in meeting face-to-face with those who may be terrorists or spies. As a result, CSIS intelligence officers have training and procedures in place to mitigate the varying hazards they encounter. Today, however, these collectors of intelligence have a new peril at hand, one which comes in online spaces. Increasingly, they are at risk of harm due to the non-consensual release of their personal information online, a phenomenon known as *doxing*.[4] The following reality-based (but fictional) scenario illustrates what could happen.

> CSIS intelligence officer Jane Jones must interview Fred Flanders, suspected of having vital knowledge about a potential terrorist attack.[5] Jones attempts to set an interview appointment with Flanders, without success. Due to the seriousness of the potential attack, Jones and a colleague, Sally Smith, assess it is necessary to visit Flanders at his home, with the aim of setting up a longer meeting. When they knock, he answers the door. After they offer their first names and identify themselves as CSIS employees, Flanders immediately takes their photographs with his smartphone. He shuts the door and rapidly posts their images to a social media service. He advises fellow ideologues to be on the lookout for 'Jane' and 'Sally' and to post any information in the 'chat' about their whereabouts.
>
> Later, a subscriber to the chat discreetly takes photos of Jones – and her license plate – while she is refueling her car at a gas station near her residence. With these, chat members use online searching/hacking tools to find and publish Jones' full name and residential address. Harassment ensues, both online and at her home. Another member of the chat performs an online image search[6] and discovers the social media page of Smith's nephew. This was because the image

---

[1] Canadian Security Intelligence Service, *Code of Conduct* (Canada: Government of Canada, 2021), 4.
[2] Not all employees of CSIS actively collect intelligence; many members work in critical support areas such as finance, information technology and policy analysis. (https://www.canada.ca/en/security-intelligence-service/corporate/csis-jobs.html, accessed 5 May 2024)
[3] *CSIS Act*, 3. Section 2 (a-c) includes the following definitions of threats to the security of Canada: espionage or sabotage; "clandestine or deceptive" foreign influenced activities "detrimental to the interests of Canada"; and acts of serious violence "for the purpose of achieving a political, religious or ideological" goal.
[4] Section 2 of this essay will provide a more detailed definition of doxing.
[5] Drawing on the more formal language of the *CSIS Act*, this is also known as an act of serious violence motivated by ideology, politics or religion.
[6] A search of google.ca on 5 May 2024 of the terms *image search* reveals a plethora of results, including these sites offering the service: Google, TinEye, SmallSEOTools, Duplichecker, DNSChecker, Yahoo, Yandex and PimEyes.

> search found Smith in a group photo from a family gathering, and which was innocently posted without her knowledge. As a result, the chat members hurl virtual abuse at Smith's nephew and threaten him with real-world harm. Moreover, the doxing has an adverse effect on Jones' and Smith's ability to further interview and investigate the potential terrorist attack. With their names and faces proliferating online, they can no longer discreetly interact with persons in this ideological milieu.[7]

In this scenario, the intelligence officers took steps to mitigate the risk of meeting with someone potentially connected to terrorism. For example, they did not go alone to the subject's residence and they identified themselves only by their first names. Nonetheless, the simple use of photos, social media collaboration and online searching/hacking techniques led to real-world threats and harassment. There is no way to prevent this; at least not one that would allow intelligence officers to live in the same cities where they work. Even more disconcerting is the harm it caused to Canadian interests by impeding the ability of CSIS to investigate a threat to national security.

This essay argues that Canada requires legislative change in order to provide a visible deterrent against the doxing of intelligence service employees, and this will counter the harm doxing causes to Canadian security interests. First, it will define what doxing is. Next, it will describe the duty of CSIS intelligence collectors to put themselves in harm's way. Then, it will describe Canadian legislation and demonstrate that although there are legal tools available, they do not provide an easily explained, tangible method of countering or deterring this type of doxing. It will next address the topic of freedom of expression with regards to the Canadian Charter of Rights and Freedoms, and shine a light on how the federal government can undertake certain limiting actions when necessary. Following this are three examples of how other countries legally protect their intelligence employees, with the goal of showing potential methods by which the problem could be managed in Canada. Finally, the essay will address the fact that the moral lens through which doxing is viewed varies greatly and is wholly dependent on the experiences and biases of those involved. It ultimately will conclude that in Canada, the doxing of intelligence employees is unacceptable, and that a legal deterrent is not only achievable, it is a national security necessity.

2. What is doxing

The concept of doxing (also spelt doxxing or d0xing[8]) is an online phenomenon and this essay will rely on Douglas' definition: "the intentional public release onto the

---

[7] Although the example is fictitious, it is drawn from various facets of the author's 27-year career in the realm of public safety and national security. Additionally, it is beyond the scope of the essay to include a complete listing of employee safety/risk mitigation strategies used by intelligence collectors. It is also beyond the scope of the essay to document the numerous potential reasons why the fictional interview subject reacted as he did, though sections 2 and 7 will touch on the motivations of those who dox.

[8] David M. Douglas, "Doxing: A Conceptual Analysis," *Ethics and Information Technology* 18, no. 3 (2016), 199. On page 1652 of their article, Li and Whitworth use a similar definition, with more nuance: "Doxing refers to the public exposure of private documents and information *without consent* and with the intent to humiliate, *harass*, intimidate, punish *and/or blackmail* targets, or *condemn certain actions and ideas*. [emphasis added]"

Internet of personal information about an individual by a third party, often with the intent to humiliate, *threaten, intimidate*, [emphasis added] or punish the identified individual".[9] As additional context to this definition, Jaccoud, Molnar and Aebi state doxing can be viewed as a mechanism which fosters "social cohesion within large social groups" and simultaneously serves as a means for "controlling deviant behaviours".[10] Those who use it in this way justify their behavior by focusing on the "reprehensible" nature of the doxing target and exposing that the target is affiliated to a particular group.[11] This can be either a connection to a social grouping or a government.

In one of the few Canadian legal decisions to touch specifically on the criminal aspects of doxing, Judge Janzen stated in 2015 that the *doxer*[12] acquires identifiable information about a person from social media sites or via a hack into private systems. In their ruling, Janzen also stated that in addition to distress and shame, the personal information released via doxing "can be used by others to facilitate identity theft and fraud. The threat to publish private information can also be used by the person who holds the information for extortion and blackmail purposes".[13]

3. Putting themselves in harm's way

As employees of the Service, those who collect intelligence are required to enter a variety of environments to acquire what the Government of Canada (GoC) needs. These environments encompass real-world and online spaces which contain a plethora of ideologies and motivations, as well as the equally varied individuals who espouse them. Some of these spaces have the concept of violence as a foundational aspect,[14] with a portion of this violence aimed at the state and those acting on the state's behalf. Additionally, CSIS employees investigate hostile activities[15] from some foreign states with regards to espionage and sabotage, cyber-threats as well as foreign interference.[16] For those who participate in threat activities that are counter to Canadian security interests, doxing is a powerful tool that can impede the efforts of CSIS collectors. In acknowledging this, it is also important to underscore that CSIS employees do not move in these spaces due to their own whim or curiosity. They do so because it is necessary for the Service to acquire, evaluate and circulate information relevant to threats to national

---

[9] Douglas, "Doxing: A Conceptual Analysis," 199.
[10] Lachlan Jaccoud, Lorena Molnar and Marcelo F. Aebi, "Antifa's Political Violence on Twitter: A Grounded Theory Approach," *European Journal on Criminal Policy and Research* 29, no. 3 (2023), , 496 and 497.
[11] Jaccoud, Molnar and Aebi, "Antifa's Political Violence on Twitter: A Grounded Theory Approach," 503.
[12] For ease of reading, this essay will periodically use the terms *doxer* and *doxee*, respectively, to denote the individuals doing the doxing and those on the receiving end of the act.
[13] *R. V. B.L.A., 2015 BCPC 203,* 3 (paragraph 3). See also page 13 of this essay for more on this case.
[14] CSIS Public Report 2022, 24.
[15] For an example of what a hostile act by a foreign intelligence service can include, a review of media coverage surrounding the poisoning of Sergei Skripal is illustrative.
[16] CSIS Public Report 2022, 20-21.

security to the GoC. *But for*[17] this requirement, it is much less likely that CSIS employees would encounter individuals or entities seeking to dox them.

As noted earlier, there is no way to completely protect oneself against doxing when one must interact with hostile threat actors, but identity management for the purpose of employee safety is a common consideration for intelligence services.[18] Therefore, while no specific details are publicly available, it is logical to conclude that CSIS employees have a full range of internal procedures[19] for identity management. These, however, are not enough when it comes to online tools like image searches or hacked database material that are readily available to knowledgeable threat actors.

Although CSIS employees are not police officers, they are considered *peace officers*[20] in a legal sense. As well, the professions are similar in that their members must work in environments that are riskier than many Canadians will normally encounter. Intelligence collectors meet face-to-face with individuals suspected of involvement in acts of serious violence and also with persons suspected of working for hostile foreign intelligence services. In doing so, they put themselves into harm's way for the benefit of a safer, more secure Canada. As noted in a 2000 Ontario Court of Appeal decision relating to the attempted murder of four police officers, "attacks upon … officers who are doing their duty are attacks on the rule of law and on the safety and well-being of the community as a whole".[21] While much less serious than attempted murder, doxing a CSIS member to prevent them from doing their job can be considered an attack on the state which employs them. Therefore, the state has a duty to protect those employees in order to protect itself. Implementing legislation which directly names CSIS members as a category of employee requiring additional safeguards from doxing is a reasonable means of providing this protection.

---

[17] This specific phrase references the "But-for-Test," , https://www.law.cornell.edu/wex/but-for_test. This is a "a test commonly used in both tort law and criminal law to determine actual causation. The test asks, "but for the existence of X, would Y have occurred?"'

[18] For example, intelligence collectors in the United Kingdom make use of *false personas* online. From: Home Office, *Covert Human Intelligence Sources Revised Code of Practice* (United Kingdom, 2022), 27.

[19] For an indirect Canadian example, testimony at a public inquiry indicated two CSIS employees had their identities *anonymized* in transcripts. From: *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions - Public Hearing Volume 10 (Thursday April 4, 2024)*, 240.

[20] Section 20 (1) of the *CSIS Act* states: "The Director and employees have, in performing the duties and functions of the Service under this Act, the same protection under the law as peace officers have in performing their duties and functions as peace officers." From: *CSIS Act,* 31.

[21] Ontario Court of Appeal, R v. McArthur, 27 February 2004, docket C13278, paragraph 49. This decision relates to an extremely violent incident involving a bank robbery and exchanges of gunfire between the defendant and police officers. Nonetheless, the sentiment expressed in this decision can be considered applicable to the work performed by CSIS collectors.

4. The legal situation surrounding doxing in Canada

There is no Canadian federal legislation[22] which mentions the word doxing[23] and this includes the *Criminal Code* (the *CC*), the *Privacy Act*, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*[24], the *Security of Information Act (SOIA)* and the *CSIS Act*.[25] Therefore, lacking specific mention of the term it is necessary to assess whether any of these acts have provisions which could be applicable to the concept. For this essay's purpose, it will first focus on the *CSIS Act* and the *SOIA* as these are two pieces of legislation which directly deal with intelligence matters. It will then move to the *CC*, and conclude with discussion of Bill C-63, a piece of draft legislation about online harms that recently had its first reading.

The CSIS Act, Section 18: Offence To Disclose Identity

This section regulates the requirement to protect the identity of CSIS employees engaged in *covert operational activities*. On first reading, the words *offence to disclose identity* seem to indicate the section may cover the concept of doxing. Therefore, a closer look is necessary:

> (1) Subject to subsection (2), no person shall knowingly disclose any information that they obtained or *to which they had access in the course of the performance of their duties and functions under this Act* [emphasis added] or their participation in the administration or enforcement of this Act and from which could be inferred the identity of an employee who was, is or is likely to become engaged *in covert operational activities of the Service* [emphasis added] or the identity of a person who was an employee engaged in such activities.[26]

When read in full, it is clear this portion of the *CSIS Act* does not relate to doxing, i.e.: members of the general public revealing the identities or personal details of CSIS employees online. Instead, it places a clear responsibility on the shoulders of CSIS employees with regards to protecting the identities of their colleagues who were, are or

---

[22] It is beyond the scope of this essay to include discussion of civil remedies, i.e. torts. The Merriam-Webster Dictionary definition of tort is: "a wrongful act other than a breach of contract for which relief may be obtained in the form of damages or an injunction". Torts stand in contrast with criminal law and, as such exploration of the potential remedies offered via this pathway is too large to undertake here.

[23] Spelling variants of *doxing* also did not reveal any results. Search performed on 20 April 2024 at https://laws.justice.gc.ca/Search/Advanced.aspx.

[24] By virtue of their titles, the *Privacy Act* and the *PIPEDA* initially appeared to have a connection to the concept of doxing, as they are aimed at protecting privacy and personal information from unauthorized release. When reading the purpose section of each, however, it is immediately clear the goal of these acts is to protect personal and private information which is in the hands of federal government entities (for the *Privacy Act*), or held by private commercial entities (for the *PIPEDA*).

[25] On 6 May 2024, the House of Commons of Canada gave first reading to Bill C-70, an "Act respecting countering foreign interference". If passed, it will amend several pieces of legislation, including the *CSIS Act*, the *SOIA* and the *CC*. For instance, the SOIA's title will change to the *Foreign Interference and Security of Information Act*. Given that C-70's first reading was in close proximity to this essay's due date, the author was unable to review and assess whether amendments were relevant to this essay's thesis. (https://www.parl.ca/Content/Bills/441/Government/C-70/C-70_1/C-70_1.PDF)

[26] *CSIS Act* (Canada: Minister of Justice, 2023), 27.

are likely to work in covert operations at CSIS.[27] For this essay, this is defined as those who engage in intelligence collection activities.[28] This is with regards to its "role to investigate activities suspected of constituting threats to the security of Canada and to report on these to the" GoC.[29] Section 18 (1) acknowledges that by virtue of their employment, those working inside CSIS not only have information that could harm Canadian interests as covered by the *SOIA*, but also possess that which could potentially harm their colleagues. In an indication of the serious potential consequences of this activity, section 18 (3) clearly indicates that in some circumstances, an indictable offence may be the appropriate consequence for this activity.[30]

The CSIS Act, Section 12.1: Measures To Reduce Threats

At first glance, this part of the *CSIS Act* also appears to have potential applicability against doxing. Again, a closer look is needed.

> 12.1 (1) If there are reasonable grounds to believe that *a particular activity constitutes a threat to the security of Canada* [emphasis added], the Service may take measures, within or outside Canada, to reduce the threat.
>
> (2) The measures shall be *reasonable and proportional in the circumstances* [emphasis added], having regard to the nature of the threat, the nature of the measures, *the reasonable availability of other means to reduce the threat* [emphasis added] and the reasonably foreseeable effects on third parties, including on their right to privacy.
>
> ….
>
> (3.2) The Service *may take measures under subsection (1) that would limit a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms only if a judge* [emphasis added], on an application made under section 21.1, issues a warrant authorizing the taking of those measures.[31]

Although a full review of section 12.1 is beyond the scope of this paper, examination of specific phrases within is worthwhile. For instance, taking *measures to reduce the threat* could provide CSIS the capacity to counter doxing of employees involved in covert operational activities. If an employee of CSIS is collecting intelligence, logic indicates they are doing so as part of the Service's efforts to investigate a *particular activity* [that] *constitutes a threat to the security of Canada*. If this employee is doxed as a result of their efforts to collect intelligence on the threat, it is also

---

[27] The *CSIS Act* does not provide a definition of the term "covert operational activities of the Service".
[28] These activities are found in section 12(1), 15(1) and 16(1) of the *CSIS Act*.
[29] *CSIS Website* (Canada, 2023).
[30] This has not been tested in court. Searches at www.canlii.org/en did not reveal any cases that relate to section 18(1-3) of the *CSIS Act.* CanLII's website states it is the Canadian Legal Information Institute and it is a non-profit organization that has as its mandate "to provide efficient and open online access to judicial decisions and legislative documents" and "its collection is generally complete for cases decided after 2001". (accessed 20 April 2024)
[31] *CSIS Act*, 23-25.

reasonable to believe that the act of doxing is connected to the larger threat. If this test is met, then CSIS may take *reasonable and proportional* means to reduce the threat from doxers. This is only if there are no other ways to accomplish the same ends that have *reasonable availability*. As will be demonstrated in upcoming sections of this essay, however, there are other pieces of federal legislation that could be brought to bear on this situation, some of which are both more available and more reasonably brought to bear.

Moreover, it is unlikely CSIS could use threat reduction measures against employee doxing without also limiting the ability of the doxer to express themselves online. Given that freedom of expression is deemed fundamental in the Canadian Charter of Rights and Freedoms,[32] using measures to reduce the threat in this fashion are likely to be assessed as limiting. With this in mind, it would then become necessary for CSIS to seek a warrant from a judge of the Federal Court to undertake such an act. As such, this method seems less than reasonably available (even impractical), given that other legal pathways are available and which do not use the scarce resources of the Federal Court[33]. These potential alternate routes are the *SOIA* and the *CC*.

The SOIA: Prejudice to the Safety or Interest of the State

The goal of the *SOIA* is to criminalize "information-related conduct that may be harmful to Canada, such as spying, economic espionage and foreign-influenced threats or violence".[34] As doxing is connected to information, this essay will explore the *SOIA's* potential ability to protect CSIS employees. Section 3 (1)(i) states that "a purpose is prejudicial to the safety or interests of the State if a person… impairs or threatens the capabilities of the … [GoC] in relation to security and intelligence".[35] If a CSIS employee is doxed and this impairs the ability of the employee to investigate threats to national security, it is logical to conclude that this will impede overall GoC capacity relating to intelligence. It could be argued it is absurd to state that impeding the ability of a single CSIS employee via doxing would harm Canada's overall security efforts. This argument is negated, however when one considers the specialized nature of CSIS work.[36] This is particularly the case for the time it takes to train an employee[37] in intelligence collection techniques, and to also become proficient in their use. When these unique capabilities are

---

[32] Minister of Justice, *Constitution Act, 1982* (Canada, 2021), Part I, Canadian Charter of Rights and Freedoms, section 2 (b). See also Section 5 of this essay for more on the Charter.

[33] There are 43 judges on the Federal Court, including the Chief Justice and the Associate Chief Justice. (https://www.fct-cf.gc.ca/en/pages/about-the-court/members-of-the-court, accessed on 2 May 2024) This is contrasted with the 749 who are federally appointed judges at Courts of Kings Bench, provincial Supreme Courts and Superior Courts across Canada. (https://www.fja.gc.ca/appointments-nominations/judges-juges-eng.aspx accessed 2 May 2024.)

[34] Department of Justice, *Addressing Foreign Interference* (Canada, 2023), 2.

[35] Minister of Justice, *Security of Information Act* (Canada: Minister of Justice, 2023), 3-5.

[36] For example, a search at Google.ca revealed no Canadian post-secondary educational streams which focus on *intelligence collection techniques.* There were several, however, relating to intelligence analysis. (Search performed on 4 May 2024 at https:www.google.ca and using the search terms: "canadian post-secondary study intelligence collection".)

[37] CSIS, *Applying for a Job at CSIS: Frequently Asked Questions*, 2020), 17 and 22. Intelligence officers have a three-year probationary period.

combined with the Service's small size,[38] it is easily inferred there are few such employees who have the capacity to skillfully perform intelligence collection by eliciting information from people. Therefore, impeding the capacity of a CSIS employee to collect intelligence will have far-reaching harmful effects, including those which would be felt at the national level.

The SOIA: Foreign-influenced or Terrorist-influenced Threats Or Violence

Next, Section 20 (1) of the *SOIA* outlines offences that come from this type of harm, including those which are threats or violence linked to foreign entities or to a terrorist group.[39]

> 20 (1) Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign entity or a terrorist group, induces or attempts to induce, by threat, accusation, menace or violence, any person to do anything or to cause anything to be done
>
> (a) that is for the purpose of increasing the capacity of a foreign entity or a terrorist group *to harm Canadian interests* [emphasis added]; or
>
> (b) that is *reasonably likely to harm Canadian interests* [emphasis added].
>
> (2) A person commits an offence under subsection (1) whether or not the threat, accusation, menace or violence occurred in Canada.
>
> (3) Every person who commits an offence under subsection (1) *is guilty of an indictable offence* [emphasis added] and is liable to *imprisonment for life* [emphasis added].[40]

This section of the *SOIA* is also relevant for its potential use in protecting CSIS employees from doxing. If the doxing occurred as a result of CSIS efforts to collect information on these threats, it logically follows the activity is connected to the larger threat to Canada. In the act of doxing, it is possible that a threat actor would wish to cause others to do things and that these things would increase the capacity of a foreign entity or terrorist group to damage the national interest.

The challenge with using the *SOIA* and the offence as described in 20 (3), however, is twofold: a lack of explicit deterrence and a dearth of reasonableness and proportionality. Due to the fact there is no explicit mention of either CSIS or doxing in the SOIA, the explicit deterrence aspect is missing. Furthermore, the *SOIA* offers only

---

[38] CSIS has approximately 3,300 employees nationwide. "Canadian Security Intelligence Service (CSIS) - the People of CSIS," , accessed Oct. 6, 2023, https://www.canada.ca/en/security-intelligence-service/corporate/transparency/briefing-material/2021-transition-binder/people-of-csis.html.

[39] Please note that Section 20 of the *SOIA* is subject to proposed changes within Bill C-70, which was given first reading on 6 May 2024. Notably, the bill adds wording to the *SOIA* about the concept of foreign-influenced or terrorist-influenced *intimidation.* Please also see page 14 of this essay for additional information about intimidation and the *CC*.

[40] *Security of Information Act*, 18.

indictable convictions as punishment. While this essay is arguing for a means by which to produce a preventative effect via legal consequences for those who dox CSIS employees, it also acknowledges there is context to each offence. It is conceivable that an employee may be doxed out of fear, or some other non-nefarious reason. As such, having an indictable offence as the only punishment is neither reasonable nor proportional. Therefore, while use of the *SOIA* is a more practical method than that which is provided via threat reduction measures in the *CSIS Act*, its lack of proportionality also causes it to fail as an overall solution.

Criminal Code: Criminal Harassment, Uttering Threats and Intimidation

Section 183 (a-k)[41] of the *CC* contains more than 100 categories of offences, from high treason to counselling misrepresentation as it pertains to the *Immigration and Refugee Protection Act (IRPA).* Due to such variety, an examination of all offences which may be potentially relevant to doxing is beyond the scope of this essay. This section will examine only three of these categories – criminal harassment, uttering threats and intimidation – and their definitions within the *CC*.

Criminal harassment (section 264). This section applies to behaviours on the part of one person that are likely to cause another person "reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them" and includes "engaging in threatening conduct directed at the other person or any member of their family".[42] Searches for the term *doxing* at the website of the Canadian Legal Information Institute (CanLII)[43] revealed only one criminal verdict. The defendant pled guilty to "nine counts of criminal harassment, eight counts of public mischief, four counts of extortion, one count of uttering a threat and one count of breach of a recognisance."[44] Deeper reading of the decision reveals the criminal harassment counts were directly related to doxing.[45]

Uttering threats of assault causing bodily harm (section 264.1). This section discusses the offence of knowingly threatening to harm or kill another person; it also notes that this can include threats to property and even to animals.[46] Central to doxing is concept of revealing personal information about a person with the intent of threatening some kind of harm. As such, this section of the *CC* could be applicable to a scenario involving a CSIS employee.

Intimidation (section 423). This section deals with instances where one person "who, wrongfully and without lawful authority" does something for the "purpose of

---

[41] *Criminal Code* (Canada: Minister of Justice, 2024), 235-244.
[42] *Criminal Code*, 236, Section 1-2.
[43] For more information on CanLII, please see footnote 28.
[44] *R. V. B.L.A., 2015 BCPC 203,* page 5, para. 8 In this instance, the defendant's doxing acts were also intermingled with another online act, *swatting*.
[45] *R. V. B.L.A., 2015 BCPC 203*. The sections of the decision relevant to doxing pertain to the criminal harassment of Victims #1, #9, #13, #16, #17, #18, #19, #20, #21 and #23.
[46] *Criminal Code*, 328, Section 1.

compelling another person to abstain from doing anything that he or she has a lawful right to do, or to do anything that he or she has a lawful right to abstain from doing".[47]

Subsections of 423.1 discuss the concepts of illegal intimidation pertaining to the impediment of the administration of justice, which has as its goal the provocation of a state of fear in either: a) the general public; b) anyone participating in the justice system (e.g. a juror or witness etc.) in order to impede them in the performance of their duties; and c) journalists informing the public about criminal organizations. Section 423.2 (1) brings intimidation regarding health care into the picture, both for those seeking health services and for those providing them. Doxing can be viewed as a form of intimidation. This intimidation may be aimed at stopping an employee from performing their duties and functions as articulated in the *CSIS Act*. As such, this portion of the *CC* is also potentially useful with regards to doxing.

Although all three portions of the *CC* could be made relevant against those who would dox CSIS intelligence collectors, it is only section 423 that explicitly recognizes certain categories of society require additional protection. By singling out justice system participants, journalists or those who provide health care, the *CC* establishes that some individuals need to be specifically defended due to their work categories – those who are involved in different ways and means of protecting the public. Naming a particular category of profession provides an easily referenced deterrence factor. As such, CSIS employees would benefit from this type of categorization, either within the *CC* or elsewhere in federal law.

The Online Harms Act

Bill C-63, "An Act to enact the Online Harms Act*"* (C-63), is in draft format and had its first reading in February 2024. Its goal is to create "stronger online protections for children and better safeguard everyone in Canada from online hate and other types of harmful content."[48] One of the ways it aims to achieve this is by more explicitly defining types of harmful online content. Three such definitions are: content that foments hatred, content that foments violence and content that foments violent extremism or terrorism. For hatred, C-63 is clear to limit what is considered hatred by stipulating that "content does not express detestation or vilification solely because it expresses disdain or dislike or it discredits, humiliates, hurts or offends."[49] For violence, it states this is "content that actively encourages a person to commit — or that actively threatens the commission of — an act of physical violence against a person or an act that causes property damage".[50] For violent extremism or terrorism, the clarifying language is extensive, stating this is content which:

> …encourages a person to commit — or that actively threatens the commission of — for a political, religious or ideological purpose, an act of physical violence

---

[47] *Criminal Code*, 472-474, Sections 423, 423.1 and 423.2.
[48] Canadian Heritage, *Backgrounder, Online Harms Act* (Canada.ca, 2024), 1.
[49] *Bill C-63 (an Act to Enact the Online Harms Act) (First Reading)* (Minister of Justice, 2024), 2 and 6, section 2 (1) and section 2 (3).
[50] *Bill C-63 (an Act to Enact the Online Harms Act) (First Reading)*, 2, section 2(1).

> against a person or an act that causes property damage, with the intention of intimidating or denouncing the public or any section of the public or of compelling a person, government or domestic or international organization to do or to refrain from doing any act, and that, given the context in which it is communicated, could cause a person to commit an act that could cause
>
> (a) serious bodily harm to a person;
>
> (b) a person's life to be endangered; or
>
> (c) a serious risk to the health or safety of the public or any section of the public.[51]

Given that C-63's language is aimed at the online space, doxing activities will almost certainly be captured within. While promising, it is unknown how these draft definitions may evolve. As well, C-63 is aimed at all Canadians and does not recognize the specific risk-related aspects of the duties and functions of CSIS employees. Finally, C-63 reserves its harshest consequences for operators of social media services and not for those posting the content. As such, it may not provide the deterrence factor nor the tools needed to protect CSIS employees – and by extension Canada's ability to collect intelligence on threats to national security.

This entire section's purpose was to highlight some key pieces of Canadian legislation that are potentially relevant for protecting CSIS employees from doxing. It has demonstrated there are many laws which could be made applicable in this situation. What it has also shown is that none of these laws is easily pointed to as a means of discouraging the doxing of an intelligence collector. Additionally, there is limited jurisprudence relating to doxing in Canada.[52] When the newness of doxing is coupled with a lack of express language about it in Canadian legislation, this means it is not easy to articulate possible legal repercussions. This is particularly the case with regards to deterring those who may be eager to dox a CSIS employee.

5. Canada's Charter of Rights and Freedoms

At odds with the state's obligation to protect a group of government employees is the overarching need to respect fundamental freedoms expressed in Canada's Charter of Rights and Freedoms, as laid out in the *Constitution Act, 1982*. Section 2 of the Charter states "[e]veryone has the following fundamental freedoms", which include peaceful assembly and association, conscience and religion as well as "freedom of thought, belief, opinion and *expression* [emphasis added], including freedom of the press and other media of communication".[53] The freedoms and rights articulated in the Charter are, however,

---

[51] *Bill C-63 (an Act to Enact the Online Harms Act) (First Reading)*, 2, section 2(1).
[52] A search of CanLII holdings (canlii.org) on 2 May 2024 revealed nine cases which mentioned *doxing*. As noted earlier, only one of these was within the realm of criminal law: R. V. B.L.A. 2015, BCPC 203.
[53] *The Constitution Acts 1867 to 1982* (Canada, 2021), 47.

"subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".[54]

In Canada, a method of demonstrably justifying the reasonable limits is outlined in what has come to be known as the *Oakes test*.[55] It asks two questions of those considering laws that may have a limiting effect on rights and freedoms within the Charter. The first and most important asks "is the objective sufficiently important to justify limiting a Charter right?"[56] Next, the test demands that there be proportionality between the limit and the method of attaining it.[57] It is critical that these considerations be brought forward early, at the policy development stage,[58] and that they are not performative or "mechanistic" in nature.[59] As such, any legislation which is aimed at transparently deterring the doxing of CSIS intelligence collectors must take into consideration the Oakes test. For instance, C-63 directly speaks to the need to respect freedom of expression in Canada, while simultaneously protecting the ability of Canadians to participate fully in public discourse online "without being hindered by harmful content".[60] As such, C-63 drafters took into consideration the distinct requirement for "legislation … [to be] drafted more carefully [by Parliament], and more consciously of the principles which attempt to respect the interests of individuals and groups alike".[61]

6. Other countries' protections

Having established that CSIS employees are often required to put themselves in the path of those who may wish to dox them and that Canada does not have legislation in place to protect against this, this essay now explores what other countries do. It will discuss examples from Australia, the Netherlands and the United States (the US), with the goal of illustrating some possible legislative avenues that Canada could explore.

Australia

The legislation governing the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS) offers a deterrence factor to those who would, without authorization, publish the identities of employees. For both agencies, the penalty is imprisonment for 10 years.[62] The Attorney-General must approve

---

[54] *The Constitution Acts 1867 to 1982*, 47, Section 1.
[55] Department of Justice, *Charterpedia - Section 1 Reasonable Limits* (Canada, 2022), 5.
[56] *Charterpedia - Section 1 Reasonable Limits*, 6.
[57] *Charterpedia - Section 1 Reasonable Limits*, 6. For this second requirement in the Oakes test, it also takes into consideration: a) the need to have a rational link between the item being limited and the reason for the limit; b) that the limit is no more than is reasonably necessary; and c) there must be a "final balancing", in that "there must be proportionality between the deleterious and salutary effects of the law".
[58] *Charterpedia - Section 1 Reasonable Limits*, 19.
[59] *Charterpedia - Section 1 Reasonable Limits*, 6.
[60] *Bill C-63 (an Act to Enact the Online Harms Act) (First Reading)*, 9, section 9 (c-d).
[61] Michael A. Johnston, "Section 1 and the Oakes Test: A Critical Analysis," *National Journal of Constitutional Law* 26, no. 1 (Nov 1, 2009), 109.
[62] *Australian Security Intelligence Organisation Act 1979* (Australia: Office of Parliamentary Counsel, Canberra, 2023), 271 (section 92). See also *Intelligence Services Act 2001* (Australia: Office of Parliamentary Counsel, Canberra, 2023), 95 (section 41). Section 92 of the *ASIO Act* was tested and upheld

any use of these provisions before going to court. By the placement of these legal consequences inside the foundational legislation for Australian intelligence collection, it is clear the government wishes to provide enhanced protections for these employees, although the word *doxing* is not specifically mentioned. While Australia has a Westminster-style government and its population total is somewhat similar to Canada's,[63] there is a key difference in their legal systems. Australia has "no …[federal or constitutional] legislation enshrining a general right to freedom of expression".[64] Instead, protection of the concept is limited and comes from the United Nations General Assembly's *International Covenant on Civil and Political Rights (ICCPR)*.[65] While Australia signed the ICCPR in 1972 and ratified it in 1982, it "has never adopted it into domestic law".[66] This makes it easier for Australia, in contrast to Canada, to use legislative methods that can be interpreted as an impediment to freedom of expression.

Netherlands

In January 2024,[67] the Netherlands passed legislation which made it illegal to "use personal data for harassment purposes".[68] The legislation indicates that harassment purposes are those having the "aim of instilling fear in that other person, causing severe disturbances to that other person or seriously hindering that person in the performance of his or her duties or profession".[69] If found guilty, the doxer's punishment ranges from fines to imprisonment, with maximums of up to EUR 22,500[70] or two years in jail. If the doxee is someone in a specific profession, the maximum jail time is harsher. These professions include journalists, mayors and police officers.[71] As such, it is clear the Netherlands wishes to provide additional protections to those assessed to be at particular

---

in R.v. Benbrika & Ors (Ruling No 26) [2008] VSC (21 May 2008). A review of AustLII databases revealed there have been no legal tests of section 41 of the *Intelligence Services Act 2001*. Note that AustLII is Australia's online free-access resource for Australian legal information.

[63] The Australian Bureau of Statistics estimated the country's population was 26,638,554 people on June 30, 2023. (https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/latest-release). Statistics Canada estimated Canada's population at 40,528,396 on October 1, 2023. (https://www150.statcan.gc.ca/n1/daily-quotidien/231219/dq231219c-eng.htm).

[64] *Right to Freedom of Opinion and Expression - Public Sector Guidance Sheet* (Australia: Australian Government), 6.

[65] Section 19 of the *ICCPR* states the freedom to have an opinion is absolute and that freedom of expression allows for the ability to "seek, receive and impart information of all kinds" and that the freedom also comes with duties and responsibilities." From: *Freedom of Information, Opinion and Expression* (Australia: Australia Human Rights Commission, c), 1.

[66] Joint Standing Committee on Foreign Affairs, Defence and Trade, *Interim Report - Legal Foundations of Religious Freedom in Australia* (Canberra: Parliament of the Commonwealth of Australia, 2017), 6.

[67] Jennifer Beckett, "The Government Wants to Criminalise Doxing. It May Not Work to Stamp Out Bad Behaviour Online," *theconversation.*com, 2024.

[68] Ministry of Justice and Security, *Use of Personal Data for the Objective of Harassment to Become Criminal Offence*, (Government of the Netherlands, 2023), 1. This legislation has not yet been tested in court.

[69] *Use of Personal Data for the Objective of Harassment to Become Criminal Offence*, 2.

[70] On 4 May 2024, the Bank of Canada's exchange rate page stated the average exchange rate for the past year was: 1 Euro = 1.46 CA dollar; as such this fine would be approximately $32850.00 Canadian. (from https://www.bankofcanada.ca/rates/exchange/daily-exchange-rates-lookup/)

[71] *Use of Personal Data for the Objective of Harassment to Become Criminal Offence*, 2. The other professions listed are: politicians, lawyers and judges.

risk. Like Australia, the system of constitutional law in the Netherlands is different than Canada's. Both have constitutions which enshrine freedom of expression, the right to privacy and the right to equal treatment. In the Netherlands, however, the courts cannot review legislation to see "whether it is compatible with the Constitution and then declare it unlawful if it is not".[72] This difference allows the Netherlands more leeway than that which is found in Canada when passing legislation which limits freedom of expression.

The US

The US shields intelligence service employees via the *Intelligence Identities Protection Act (IIPA).* This federal law gives jail time to those who reveal the identities of persons who work in covert intelligence collection. Its creators stated that while they took freedom of expression rights seriously:

> [T]o expose their identities repeatedly…serves no legitimate purpose. It does not alert to abuses; it does not further civil liberties; it does not enlighten public debate; and it does not contribute one iota to the goal of an educated and informed electorate. Instead, it *reflects a total disregard for the consequences that may jeopardize the lives and safety of individuals and damage the ability of the United States to safeguard the national defense* [emphasis added].[73]

For the most part, the *IIPA* pertains to intelligence collectors who are active outside of the US, but it also includes certain members of the Federal Bureau of Investigation (FBI) who work inside its borders.[74] It breaks down the penalties for divulging this information into two categories: that which is done by persons who have authorized access, and those who do not. Those with authorized access to classified information can be sentenced to up to 10 years in prison; those without can be sentenced to up to three years. Fines are applicable for both scenarios. Those who do not have authorized access will face punishment only "if they participated in a pattern of activity designed to discover and reveal the identities of covert agents and have reason to believe that such disclosure will harm U.S. intelligence operations."[75]

The US legal system is different from that of Canada, as are the constitutional rights attributed to freedom of speech, the First Amendment. The US has firmly entrenched the idea that governments in the US cannot regulate "content-based and/or viewpoint-based language even if the language amounts to offensive communication … [which] applies not only to hate speech but also to other intimidating and/or threatening conversations … online".[76] As such, when there are transgressions American law focusses on regulating activities, not speech itself.[77] If the GoC were to emulate the

---

[72] Ministry of the Interior and Kingdom Relations, *Constitution and Charter,* (Government of the Netherlands), 1-2.
[73] Jennifer K. Elsea, *CRS Report for Congress - Intelligence Identities Protection Act* (United States of America: Congressional Research Service, 2013), 5.
[74] Elsea, *CRS Report for Congress - Intelligence Identities Protection Act*, 2-3.
[75] Elsea, *CRS Report for Congress - Intelligence Identities Protection Act*, 3-4.
[76] Lisa Bei Li, "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting," *Federal Communications Law Journal* 70, no. 3 (2018), 320.
[77] Li, "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting," 320.

IIPA's goal of deterring this specific action, it may be able balance its requirement to honour Canadians' freedom to express themselves and, at the same time, be able to protect its intelligence collectors.

This review of legislation which protects intelligence employees in other countries demonstrates there are methods by which CSIS collectors may be shielded from doxing. It also establishes that due to differing legal regimes, each country has had to find its own path towards compromise as it pertains to the requirement to protect these employees and to simultaneously uphold constitutional freedoms, such as freedom of expression.

7. A moral grey zone

There is more to deterring the doxing of CSIS employees than formulating and then enacting legislation. There is also a moral component that comes from the fact that doxing is connected to the concepts of public denunciation/shaming, as well as to the power imbalance between the state and its citizens.

Walking hand-in-hand with doxing and public shaming is the concept of *vigilantism*. Even in medieval times, there were effective community-based techniques used to publicly denounce someone (e.g. the *stocks* and the *pillory*[78]) as a means of controlling undesirable behaviour.[79] When writing about a modern methodology, *digital vigilantism* (DV)[80], Trottier defines it this way:

> DV is a form of mediated and coordinated action. Its point of departure is moral outrage or a general sense of offence taking, typically towards an act that has been captured and transmitted via mobile devices and through social platforms. In response to this offence taking, users seek to render a targeted individual (or category of individual) visible through information sharing practices such as assembling and publishing their personal details ('doxing').[81]

The lens through which one views an act of DV is important. It can be argued that making visible someone's so-called bad behavior is a potentially corrective and relatively harmless measure. This would be in the case of making public the shoddy vehicle parking practices of some urban residents.[82] This is in stark contrast, however, to the damaging

---

[78] "wikipedia.org" states the *stocks* are "feet restraining devices … used as a form of corporal punishment and public humiliation". The online reference platform states the *pillory* is a wooden or metal device "erected on a post with holes for securing the head and hands". Definitions accessed 15 April 2024.
[79] Daniel Trottier, "Denunciation and Doxing: Towards a Conceptual Model of Digital Vigilantism," *Global Crime* 21, no. 3-4 (2020), 197.
[80] Daniel Trottier, "Digital Vigilantism as Weaponisation of Visibility," *Philosophy & Technology* 30, no. 1 (2017), 59. Trottier uses Les Johnston's 1996 six elements of vigilantism as a framework for his discussion of the topic. It has six elements: 1) the act is planned and premeditated; 2) it is not performed by police or state actors; 3) those involved view themselves as exercising the right to self-protection within a specific place; 4) it threatens the use of force; 5) it surfaces when the normal order of things is seen to be under threat; and 6) asserts security of both the one and the many by promising that the established "system of order will prevail".
[81] Trottier, "Digital Vigilantism as Weaponisation of Visibility," 57.
[82] Trottier, "Digital Vigilantism as Weaponisation of Visibility," 62.

impact of being falsely named and shamed, as was the case for those wrongly targeted in the 2013 Boston bombing manhunt.[83] Doxing individuals who are involved in sexual assault can be viewed by some as a means of improving society, such as the *#metoo* movement.[84] Doxing members of the government can be viewed by others as bad, such as the doxing of public health officials during the COVID-19 pandemic.[85] Therefore, doxing needs to be viewed as a neutral tool and its use covers a great deal of potentially nebulous moral ground.

As an example of this moral morass, large-scale doxing activities occurred in 2019 and were used against the state, particularly law enforcement and security officials. When large numbers of ideologically/politically motivated people responded to a legislative amendment on the part of the government[86], they used doxing as a means to strike back. They used a variety of social media services, including the Telegram application,[87] to expose the private or personal information of police officers, such as where the officers lived. They eventually doxed the families of the officers, with slogans indicating that the doxers were "extending punishment to your family and children". Viewed through a Canadian lens, the doxing of police officers and their families is likely to be deemed reprehensible by numerous people. Many Canadians have confidence in their police services[88] and view them as stalwart members of a group "rooted also in the defence of civility and community, in treating people fairly … and in being aligned and responsive to local needs and issues".[89]

Canadian perceptions of these 2019 doxing incidents would likely change upon learning that they occurred in Hong Kong and were part of mass protests against the local government, backed by China. The doxing was in response to proposed amendments to extradition legislation where "[a]nyone in Hong Kong, including permanent citizens and foreign visitors, could be accused of having violated the Chinese laws and extradited to China".[90] Canadian media reported on the response of Canadians to the protest activities,

---

[83] Trottier, "Digital Vigilantism as Weaponisation of Visibility," 69.
[84] Trottier, "Digital Vigilantism as Weaponisation of Visibility," 199.
[85] Rita V. Burke et al., "A Qualitative Analysis of Public Health Officials' Experience in California during COVID-19: Priorities and Recommendations," *Frontiers in Public Health* 11 (September 13, 2023), 2.
[86] Yao-Tai Li and Katherine Whitworth, "Data as a Weapon: The Evolution of Hong Kong Protesters' Doxing Strategies," *Social Science Computer Review* 41, no. 5 (2023), 1650.
[87] Li and Whitworth, "Data as a Weapon: The Evolution of Hong Kong Protesters' Doxing Strategies," 1654. This article states Telegram is a "not-for-profit, encrypted, cloud-based messaging app that combines SMS and email. It distinguishes itself from other platforms such as Facebook and Google by emphasizing its commitment to privacy, and is therefore popular among protesters to share information and organize activities".
[88] It is necessary to recognize that many Canadians who are Black, Indigenous and People of Colour (BIPOC) fear police and do their utmost avoid any interaction with them. This due to a variety of past and present incidents where BIPOC Canadians assess they have been victims of racism at the hands of law enforcement. Additional context and views can be found in *The Skin We're In* by Desmond Cole, published by Penguin Random House Canada, 2020.
[89] J. Jackson and B. Bradford, "What is Trust and Confidence in the Police?" *Policing : A Journal of Policy and Practice* 4, no. 3 (2010), 247-248.
[90] This was in response to an incident from February 2018, when "a young man from Hong Kong murdered his girlfriend in Taiwan. Although he was arrested in Hong Kong, he could not be extradited to Taiwan because there was no extradition agreement …. to plug this loophole, the HKSAR [Special Administrative

with many viewing them as a justifiable tactic when faced with overwhelming state power. Some comments were: “Stand tall brave people of Hong Kong. You fight for your god-given [sic] human rights. The world is watching” and “The people of Hong Kong treasure their freedoms and will stand up for them”.[91]

In response, the Hong Kong government approved amendments to the Personal Data (Privacy) Ordinance in 2021 in order to counter doxing of police and government officials. These amendments made “the disclosure of personal data without consent, with *an intent to cause psychological harm*, a criminal offence in Hong Kong that can be punishable by up to a HK$1 million dollar fine and 5 years in jail”.[92] To those sympathetic to Hong Kong protestors, this legislative change is likely viewed as too harsh. For Hong Kong security officials and their families, the change is likely seen as a positive one.

8. Conclusion

It must be acknowledged that doxing is part of “the digital realm [which] fosters an environment where individuals can be convicted without a trial and without guarantees for the accused, such as the presumption of innocence”.[93] In terms of this essay, it means there is a need to protect intelligence collectors from being convicted and then punished through doxing. Another necessary acknowledgement, however, is that “moral legitimacy of doxing” exists in “that it seeks to change the asymmetrical power relations [of the populace] with the state and the police”.[94] For Canadians, moral legitimacy takes one form via freedom of expression, and which is established as a constitutional necessity. The friction between these two concepts is evident, and yet a compromise remains essential.

Via its review of Canadian acts and legislation as well as international examples, this essay has demonstrated that such compromises can happen. The Charter states Canadians have fundamental freedoms; however, there are reasonable limits to these freedoms as long as they can be demonstrably justified. Bill C-63, the draft online harms act, provides a concrete example of reasonable limits and how to justify them via clear legal meaning; i.e., stating that disdain or dislike will not be considered hate even if it humiliates or offends. There are also laws which protect specific categories of people

---

Region] government proposed to amend the Fugitive Offenders Ordinance and the Mutual Legal Assistance in Criminal Matters Ordinance.” From: Thomas Yun-tong Tang and Michelle W. T. Cheng, "The Politicization of Everyday Life: Understanding the Impact of the 2019 Anti-Extradition Law Amendment Bill Protests on Pro-Democracy Protesters' Political Participation in Hong Kong," *Critical Asian Studies* 54, no. 1 (2022), 135.

[91] Shannon Busta, "From the Comments: 'Stand Tall, Brave People of Hong Kong.' Readers Respond to Protests and China's Retreat on Extradition Bill," *The Globe and Mail* 17 June, 2019.

[92] Li and Whitworth, "Data as a Weapon: The Evolution of Hong Kong Protesters’ Doxing Strategies," 1653. Previously, the data disclosure offence in the PDPO was linked to an intent to “obtain financial gain or cause financial loss to the data subject.” Also, $1-million HK dollars is approximately $172,600.00 Canadian; based on the yearly average exchange rate between the HK dollar and the CA dollar from the Bank of Canada. (https://www.bankofcanada.ca/rates/exchange/currency-converter/ accessed 6 May 2024)

[93] Jaccoud, Molnar and Aebi, "Antifa’s Political Violence on Twitter: A Grounded Theory Approach," 510.

[94] Li and Whitworth, "Data as a Weapon: The Evolution of Hong Kong Protesters’ Doxing Strategies," 1653.

from acts of intimidation, as is the case with the *CC* providing special protection for those with responsibilities linked to the criminal justice or healthcare systems.

When it comes to the national interest of Canada, this paper has established that there can be no impairment or threat to the key state capabilities of security and intelligence. This essay has demonstrated that doxing CSIS intelligence collectors has a demonstrably harmful effect on Canada's overall national security efforts. Although there are many ways to impose consequences for doxing under current federal laws, none are easily pointed to as a clear deterrent. This essay has shown this is particularly the case when doxing is used to impede the work of intelligence employees. Therefore, in order to shield those who work to keep Canada secure through intelligence collection, there must be legislative change.

BIBLIOGRAPHY

Australian Security Intelligence Organisation Act 1979. Australia: Office of Parliamentary Counsel, Canberra, 2023.

Bill C-63 (an Act to Enact the Online Harms Act) (First Reading) Minister of Justice, 2024. https://www.parl.ca/Content/Bills/441/Government/C-63/C-63_1/C-63_1.PDF accessed 17 April 2024.

"Canadian Security Intelligence Service (CSIS) - the People of CSIS." https://www.canada.ca/en/security-intelligence-service/corporate/transparency/briefing-material/2021-transition-binder/people-of-csis.html accessed Oct. 6, 2023.

The Constitution Acts 1867 to 1982. Canada: 2021.

Criminal Code. Canada: Minister of Justice, 2024.

CSIS Act. Canada: Minister of Justice, 2023.

CSIS Website. Canada: 2023. https://www.canada.ca/en/security-intelligence-service.html accessed 20 April 2024

Freedom of Information, Opinion and Expression. Australia: Australia Human Rights Commission. https://humanrights.gov.au/our-work/rights-and-freedoms/freedom-information-opinion-and-expression accessed on 24 April 2024.

Intelligence Services Act 2001. Australia: Office of Parliamentary Counsel, Canberra, 2023.

Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions - Public Hearing Volume 10, Thursday April 4, 2024. https://foreigninterferencecommission.ca/public-hearings/day-10-april-4 accessed on 29 April 2024.

Right to Freedom of Opinion and Expression - Public Sector Guidance Sheet. Australia: Australian Government. https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/right-freedom-opinion-and-expression accessed on 24 April 2024.

"wikipedia.org." – definitions of *stocks* (https://en.wikipedia.org/wiki/Stocks) and *pillory* (https://en.wikipedia.org/wiki/Pillory) accessed on 15 April 2024.

Beckett, Jennifer. "The Government Wants to Criminalise Doxing. It May Not Work to Stamp Out Bad Behaviour Online." *theconversation.com,* 2024.

https://theconversation.com/the-government-wants-to-criminalise-doxing-it-may-not-work-to-stamp-out-bad-behaviour-online-223546 accessed 15 April 2024.

Burke, Rita V., Anna S. Distler, Timothy C. McCall, Emma Hunter, Shruti Dhapodkar, Larissa Chiari-Keith, and Aaron A. Alford. "A Qualitative Analysis of Public Health Officials' Experience in California during COVID-19: Priorities and Recommendations." *Frontiers in Public Health* 11, (September 13, 2023): 1-10.

Busta, Shannon. "From the Comments: 'Stand Tall, Brave People of Hong Kong.' Readers Respond to Protests and China's Retreat on Extradition Bill." *The Globe and Mail,* 17 June, 2019. https://www.proquest.com/blogs-podcasts-websites/comments-stand-tall-brave-people-hong-kong/docview/2382316393/se-2 accessed 16 April 2024.

Canadian Heritage. *Backgrounder, Online Harms Act* Canada.ca, 2024. https://www.canada.ca/en/canadian-heritage/news/2024/02/backgrounder--government-of-canada-introduces-legislation-to-combat-harmful-content-online-including-the-sexual-exploitation-of-children.html accessed 17 April 2024.

Canadian Security Intelligence Service. *Code of Conduct*. Canada: Government of Canada, 2021. https://www.canada.ca/en/security-intelligence-service/corporate/csis-jobs/code-of-conduct.html accessed 9 September 2023.

Cornell Law School. "But-for-Test." https://www.law.cornell.edu/wex/but-for_test accessed 4 May 2024.

CSIS. *Applying for a Job at CSIS: Frequently Asked Questions* 2020. https://www.canada.ca/en/security-intelligence-service/corporate/csis-jobs/faq.html#faq10 accessed 4 May 2024.

CSIS. *CSIS Jobs*. https://www.canada.ca/en/security-intelligence-service/corporate/csis-jobs.html, accessed 5 May 2024.

Department of Justice. *Addressing Foreign Interference*. Canada: 2023. https://www.justice.gc.ca/eng/cons/fi-ie/pdf/Addressing_foreign_interference.pdf and https://www.justice.gc.ca/eng/cons/fi-ie/ accessed 20 April 2024.

Department of Justice. *Charterpedia - Section 1 Reasonable Limits*. Canada: 2022. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art1.html accessed 30 April 2024.

Douglas, David M. "Doxing: A Conceptual Analysis." *Ethics and Information Technology* 18, no. 3 (2016): 199-210.

Elsea, Jennifer K. *CRS Report for Congress - Intelligence Identities Protection Act*. United States of America: Congressional Research Service, 2013.

Home Office. *Covert Human Intelligence Sources Revised Code of Practice*. United Kingdom: 2022. https://assets.publishing.service.gov.uk/media/63985c2fe90e077c2e1ce84c/Revised_CHIS_Code_of_Practice_December_2022_FINAL.pdf accessed 1 May 2024.

Jaccoud, Lachlan, Lorena Molnar, and Marcelo F. Aebi. "Antifa's Political Violence on Twitter: A Grounded Theory Approach." *European Journal on Criminal Policy and Research* 29, no. 3 (2023): 495-513.

Jackson, J. and B. Bradford. "What is Trust and Confidence in the Police?" *Policing : A Journal of Policy and Practice* 4, no. 3 (2010): 241-248.

Johnston, Michael A. "Section 1 and the Oakes Test: A Critical Analysis." *National Journal of Constitutional Law* 26, no. 1 (Nov 1, 2009): 85.

Joint Standing Committee on Foreign Affairs, Defence and Trade. *Interim Report - Legal Foundations of Religious Freedom in Australia*. Canberra: Parliament of the Commonwealth of Australia, 2017.

R. v. Benbrika & Ors (Ruling No 26) [2008] VSC 452 (Judge J. Bongiorno, Supreme Court of Victoria at Melbourne, 21 May 2008). https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2008/452.html. accessed 28 May 2024.

R. v. B.L.A., 2015 BCPC 203 (Judge P. Janzen, Provincial Court of British Columbia 2015). https://canlii.ca/t/gk3rx accessed on 2 May 2024.

Li, Lisa Bei. "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting." *Federal Communications Law Journal* 70, no. 3 (2018): 317-328.

Li, Yao-Tai and Katherine Whitworth. "Data as a Weapon: The Evolution of Hong Kong Protesters' Doxing Strategies." *Social Science Computer Review* 41, no. 5 (2023): 1650-1670.

Minister of Justice. *Constitution Act, 1982*. Canada: 2021.

Minister of Justice. *Security of Information Act*. Canada: Minister of Justice, 2023.

Ministry of Justice and Security. *Use of Personal Data for the Objective of Harassment to Become Criminal Offence* Government of the Netherlands, 2023. https://www.government.nl/latest/news/2023/07/12/use-of-personal-data-for-the-objective-of-harassment-to-become-criminal-offence# accessed 28 April 2024.

Ministry of the Interior and Kingdom Relations. *Constitution and Charter* Government of the Netherlands. https://www.government.nl/topics/constitution/constitution-and-charter# accessed 28 April 2024.

Ontario Court of Appeal, R. v. McArthur, (Doherty and Goudge, JJ.A. and Cavarzan, J. (ad hoc) 27 February 2004), docket C13278. https://ca.vlex.com/vid/r-v-mcarthur-m-680551653 accessed 16 April 2024 and 6 May 2024.

Tang, Thomas Yun-tong and Michelle W. T. Cheng. "The Politicization of Everyday Life: Understanding the Impact of the 2019 Anti-Extradition Law Amendment Bill Protests on Pro-Democracy Protesters' Political Participation in Hong Kong." *Critical Asian Studies* 54, no. 1 (2022): 128-148.

Trottier, Daniel. "Denunciation and Doxing: Towards a Conceptual Model of Digital Vigilantism." *Global Crime* 21, no. 3-4 (2020): 196-212.

Trottier, Daniel. "Digital Vigilantism as Weaponisation of Visibility." *Philosophy & Technology* 30, no. 1 (2017): 55-72.