Canadian Journal of Law and Technology

Volume 19 | Number 1 Article 3

1-27-2023

The Adverse Human Rights Impacts of Canadian Technology Companies: Reforming Export Control with the Introduction of Mandatory Human Rights Due Diligence

Siena Anstis

RJ Reid

The Adverse Human Rights Impacts of Canadian Technology Companies: Reforming Export Control with the Introduction of Mandatory Human Rights Due Diligence

Siena Anstis[*] and *RJ Reid*[**]

Abstract

Netsweeper, a Canadian company, has produced and sold Internet-filtering technology to authoritarian regimes abroad. According to public research from the Citizen Lab, this technology has been used to censor religious content in Bahrain, information on Rohingya refugees in Myanmar and India, political campaign content in United Arab Emirates, and information on HIV/AIDS in Kuwait. This article considers how Canadian export control law deals with technologies that negatively impact human rights abroad and identifies a gap in the existing export control scheme. We suggest this gap could be closed by adopting a proactive human rights due diligence requirement on companies seeking to export products under Canadian law. There is existing precedent in other jurisdictions for imposing a human rights due diligence requirement on companies more broadly as a matter of law. A legislative amendment to Canada's export regime would move Canada towards meaningful compliance with the United Nations Guiding Principles, reflect a growing normative acceptance that companies have a duty to respect human rights under international law, and potentially open avenues for legal remedy.

INTRODUCTION

Netsweeper is one of many Canada-based technology companies situated along the Toronto-Waterloo Innovation Corridor.[1] The company sells a suite of technology products related to Internet categorization and filtering that enable administrators to restrict Internet users' access to certain websites.[2] They market their products as allowing librarians to block pornography, schools to enable safe search options on platforms like Google, and workplaces to block social media sites in an effort to combat lost productivity.[3] While these technological

[*] Senior Legal Advisor with the Citizen Lab at the University of Toronto, Munk School of Global Affairs and Public Policy. Professor Ron Deibert provided supervision and guidance in the researching and drafting of this article.

[**] Articling student with McCarthy Tetrault LLP.

1 See "Contact Netsweeper Today", online: *Netsweeper* < www.netsweeper.com/company/contact-us/ > .

2 See "Netsweeper", online: *Netsweeper* < www.netsweeper.com/ > .

functions are seemingly innocuous, evidence suggests that their products are also used for other purposes that are not advertised. The Citizen Lab, a research group at the University of Toronto, found evidence that Netsweeper products were being used to block religious content in Bahrain, information on Rohingya refugees in Myanmar and India, political campaign content in United Arab Emirates (UAE), and information on HIV/AIDS in Kuwait, among other categories.[4] Netsweeper products are also used in other countries with poor human rights records, such as Afghanistan, Pakistan, Qatar, Somalia, Sudan, and Yemen.[5] The Citizen Lab's research suggests that the Canadian company has produced and exported technology used to facilitate the suppression of free expression—including most notably, political, religious, and LGBTQ+ content—and discrimination against minority populations. Such uses of Netsweeper's products have infringed on multiple internationally-protected human rights and form part of a broader ecosystem of technology used for surveillance and censorship online.[6] Nonetheless, the company's business activities are legal under Canadian law and the company has even at times received investment support from Export Development Canada.[7]

This article uses the Netsweeper case study to illustrate defects in Canada's export control regime from the perspective of international human rights law and in the context of technology exports.[8] After a review of the existing Canadian export control scheme, we note that Netsweeper's Internet-filtering technology is not presently subject to export regulation, despite its potentially harmful impacts on human rights. We then observe several possible routes to addressing this deficiency, such as amending the *Wassenaar Arrangement*'s[9] (the *Arrangement*) export control list to capture such technology or amending Canada's *Export and Import Permits Act*[10] (*EIPA*) to provide human rights violations as an explicit and stand-alone basis for export control. However, in this article, we build on a growing normative movement towards mandatory human rights due diligence and focus on the possibility of enacting such a requirement on technology companies seeking to export their products from Canada. We argue that this approach is particularly justified in so far as it could open up legal remedies against technology companies that fail to comply with due diligence

---

3 See *ibid.*

4 See Jakub Dalek et al, Planet Netsweeper" (25 April 2018), online (pdf): *Citizen Lab* <citizenlab.ca/2018/04/planet-netsweeper/>.

5 See *ibid.*

6 See Jon Penney et al, "Advancing Human-Rights-By-Design in The Dual-Use Technology Industry" (2018) 71:2 J Intl Affairs, online: .

7 See Dalek et al, *supra* note 4 at 99.

8 The authors note that other types of exports that are not captured by export control laws may similarly raise human rights concerns and this is not a problem specific or exclusive to the technology sector.

9 See "The Wassenaar Arrangement", online: *Wassenaar* <www.wassenaar.org/>.

10 *Export and Import Permits Act*, R.S.C, 1985, c. E-19 [*EIPA*].

requirements, separate and apart from whether the Government of Canada decides to issue an export license for their products. Further, we argue that the requirement of proactive disclosure is particularly important with regard to the accountability of technology companies. There is little public insight into product development in this sector and, consequently, the potential impact of new technologies on human rights. Thus, proactive disclosure requirements could be particularly meaningful.

In **Parts 1 and 2**, we review the Netsweeper case study, introduce Canada's obligations under international human rights law, and describe how international human rights and dual-use technologies are considered and addressed in Canada's current export control regime. We identify a gap in the current export regime in relation to technology like that being produced by Netsweeper and suggest different ways of closing it. In **Part 3** of this Article, we focus on one particular solution, namely imposing a human rights due diligence requirement on technology companies seeking to export their products abroad. In doing so, we discuss the United Nations Guiding Principles (UNGPs) and examine the global normative trend towards the inclusion of human rights due diligence in the corporate sector into domestic law. In **Part 4**, we argue for the express inclusion of such a mandatory obligation on technology companies seeking to export under Canadian law and consider how this might capture technology like that produced by Netsweeper. We then discuss how such an amendment to the Canadian export control regime could open the possibility of legal remedies directly against companies, which would serve to meet, at least in part, the 'remedy' requirement of the UNGPs. While not a panacea, robust export controls that are considerate of human rights abuses could present a step forward in mitigating the negative human rights effects flowing from emerging technologies.[11]

1. CANADIAN TECHNOLOGY COMPANIES AND INTERNATIONAL HUMAN RIGHTS LAW

In 2018, the Citizen Lab released a report documenting Netsweeper installations on public Internet Protocol (IP) networks in ten countries that each presented systemic human rights concerns.[12] Its research findings showed that Netsweeper technology was used to block: (1) political content sites, including websites linked to political groups, opposition groups, local and foreign news, and regional human rights issues in Bahrain, Kuwait, Yemen, and UAE; (2) Google searches for keywords relating to LGBTQ+ content (e.g., the words "gay" or "lesbian") in the UAE, Bahrain, and Yemen; (3) non-

---

[11] See Sarah McKune & Ron Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking" (2 March 2017), online (pdf): *Citizen Lab* citizenlab.ca/2017/03/whos-watching-little-brother-checklist-accountability-industry-behind-government-hacking/ > .

[12] See Dalek et al, *supra* note 4.

pornographic websites under the mis-categorization of sites like the World Health Organization and the Center for Health and Gender Equity as "pornography"; (4) access to news reporting on the Rohingya refugee crisis and violence against Muslims from multiple news outlets for users in India; (5) Blogspot-hosted websites in Kuwait by categorizing them as "viruses" as well as a range of political content from local and foreign news and a website that monitors human rights issues in the region; and (6) websites like Date.com, Gay.com (the Los Angeles LGBT Center), Feminist.org, and others by categorizing them as "web proxies."[13]

As the Citizen Lab noted in its report, this impacted a number of internationally-protected human rights, such as the right to freedom of opinion and expression; the right to freedom to seek, receive, and impart information and ideas; protections against discrimination and minority protection; and the rights to liberty and security of the person.[14] International human rights institutions have taken a similarly critical view of Internet-filtering. For example, in *General Comment No. 34*, the UN Human Rights Committee noted that Article 19 of the *International Covenant on Civil and Political Rights* protects all forms of expression, including "electronic and internet-based modes of expression."[15] In his 2011 report, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, described how "blocking and filtering" represented one "restriction on the right of individuals to express themselves through the Internet" and that "States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression" because they do not meet the requirements of international human rights law.[16]

A number of other regional and international human rights instruments declare that freedom of expression applies to the Internet; that mandatory blocking of entire websites, IP addresses, ports, network protocols, or types of uses are an "extreme measure" that can "only be justified in accordance with international standards"; and that content filtering systems "which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression."[17] In short, the use of Netsweeper

---

[13] See *ibid.*

[14] See *ibid.* See also analysis by international human rights organizations, such as Article 19: *Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech* (London, UK: Article 19, 2016) at 11, online (pdf): *Article 19* <www.article19.org/resources/freedom-of-expression-unfiltered-how-blocking-and-filtering-affect-free-speech/>.

[15] United Nations Human Rights Committee, *General Comment No. 34, Article 19: Freedoms of opinion and expression*, 102nd Sess, UN Doc CCPRC/GC/34 (2011) at 3.

[16] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion, Frank La Rue,* HRC, 17th Sess, UN Doc A/HRC/17/27 (2011) at 9—10.

[17] Frank La Rue et al, *Joint Declaration on Freedom of Expression and the Internet* (1 June

technology by importing countries in filtering and blocking websites and content clearly leads to a negative and unjustified interference with internationally-protected human rights.

While this article focuses on Netsweeper's technology as a case study, there are likely other companies developing and exporting technology from Canada that may fall within a similar gap in export control rules.[18] However, due to a lack of transparency and insight into this sector and challenges in tracking the abuse of technologies, like Internet-filtering tools or emerging and novel technologies, it is difficult to identify and highlight additional business entities. Moreover, as the technology sector is an inherently fast-developing field, there is potential for new Canadian companies or products to raise human rights concerns at any time. Canada's export control regime must be able to respond to known cases like Netsweeper and anticipate other cases that could jeopardize Canada's human rights commitments, as discussed in the next section.

2. INTERNATIONAL HUMAN RIGHTS AND CANADA'S EXPORT CONTROL REGIME

Before discussing the role of international human rights in Canada's export control laws, it is important to briefly discuss some of the relevant international legal instruments that Canada has ratified to understand where export control law falls short of supporting Canada's international obligations. As of 2020, Canada has ratified seven core United Nations (UN) treaties and is party to a number of other international human rights treaties.[19] At an abstract level, this suggests that successive Canadian governments have generally been concerned with the protection of international human rights law as a broad concept both domestically and abroad.[20] Additionally, Canada's current foreign policy

---

2011) at 3, online (pdf): *Organization for Security and Co-operation in Europe* < www.osce.org/fom/78309 > .

[18] For example, several companies with a Canadian business presence develop digital forensic technologies. This technology can be used in a manner that infringes human rights, as illustrated in Myanmar in 2021. See Hannah Beech, "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown", *New York Times* (1 March 2021), online: < www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html > . While digital forensic technology was included in the *Wassenaar Arrangement* Control List in 2019, at the time of publication of this article, these amendments to the Control List have not been incorporated into Canadian export law meaning that such technology is not subject to export control in Canada. See Government of Canada, "Regulation — Order Amending the Export Control List" (13 March 2020), online: *Government of Canada* < www.international.gc.ca/controls-controles/about-a_propos/expor/regulation-reglement-2020.aspx?lang = eng > .

[19] See "UN Treaty Body Database", online: *United Nations Human Rights Treaty Bodies* < tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID = 31&Lang = EN > .

[20] Canada has historically played a leadership role in the promotion of international human rights. During the 1990s, for example, when Lloyd Axworthy served as Minister

position acknowledges that countries have a duty to promote and protect human rights and views such duties as an integral part of Canadian efforts abroad.[21] Yet despite these commitments, the will to follow through on preventing or remedying international human rights violations domestically and abroad[22] has been deficient. Specific to this article, the impact of technology on human rights abroad is an issue that has received relatively little attention in Canada. Canadian policy regarding human rights has focused primarily on the extractive sectors, which is consistent with the presence of Canadian companies in that industry and the fact that the discussion regarding technology-related human rights harms is still in its relative infancy. Canada has also not been a leader with regard to the push towards mandatory human rights due diligence for the business sector.[23] Despite gaps in Canada's commitment to the protection of international human rights, the fact that Canada has ratified a number of treaties protecting human rights provides a broader framework for situating how Canada should treat the potential for human rights in export violations, an issue that will be discussed later in this article.

Having set out the contours of the technology at issue in this case study and its unlawful interference with international human rights, as well as having addressed Canada's international obligations more generally, this next section provides an overview of the Canadian export control regime, its controls on dual-use technologies,[24] and the role of human rights considerations in this

---

of Foreign Affairs under the Chrétien government, Canada played key roles in both the campaign against landmines, which resulted in the Ottawa Mine Ban Convention (the treaty-making process for which the United States could not be involved), and the resolution of the Kosovo crisis through Canada's support for the NATO intervention and Russian participation in the G8 forum (in response to the stalemate at the UN Security Council). See *e.g.* Michael Manulak, "Canada and the Kosovo Crisis: Looking back, 20 years on", *Open Canada* (6 June 2019), online: opencanada.org/canada-and-kosovo-crisis-looking-back-20-years/ > .

[21] See Government of Canada, "Canada's approach to advancing human rights" (9 January 2020), online: *Government of Canada* < www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_-rights-promouvoir_droits.aspx?lang = eng > .

[22] This article sets aside the issue of extraterritoriality, although any practical analysis of whether there has been a violation of human rights outside Canada's national borders would have to grapple with debates regarding the scope of application of treaties like the *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976, accession by Canada 19 May 1976).

[23] See Brian Burkett et al, (Fasken), "First-step analysis: business and human rights in Canada" (28 February 2020), online: *Lexology* < www.lexology.com/library/detail.aspx?g = 851da4d5-6f41-4d9c-a1d2-7aba3a33d610 > .

[24] Different definitions of the term "dual-use technologies" has been proposed in the literature, but this article mainly focuses on the broader definition used by Professor Ronald Deibert: a technology that "may serve a legitimate and socially beneficial purpose, or, equally well, a purpose that undermines human rights." See Ron Deibert, "What to do about 'dual use' digital technologies?" (29 November 2016), online: *Ronald*

legislative scheme. We conclude that the current export control system in Canada is deficient in that it does not capture the Internet-filtering technology being exported by Netsweeper, despite its negative impact on internationally-protected human rights, as described above. We then consider different mechanisms by which to close that gap, with a particular focus on human rights due diligence obligations on the business sector.

(a) The Canadian Export and Import Permits Act and Human Rights Considerations

Canada's export control regime is predominantly governed by the *EIPA*, although controls on exports to specific countries can also be mandated through the *Special Economic Measures Act* or the *United Nations Act*.[25] The *EIPA* has traditionally been oriented around values of economic and national security rather than human rights. This fits with a broader trend in international trade law, where historically human rights have not been a major concern.[26] (However, as will be discussed, recent amendments to Canadian legislation made to comply with requirements of the international *Arms Trade Treaty*[27] (*ATT*) mean that human rights considerations are slowly penetrating the Canadian export control regime.)

Deibert < deibert.citizenlab.ca/2016/11/dual-use/ >. In the context of the *Wassenaar Arrangement*, "dual-use" is understood more narrowly to indicate "an item which serves both civilian and military purposes." See Machiko Kanetake, "The EU's dual-use export control and human rights risks: the case of cyber surveillance technology" (2019) 3:1 Europe & World: L Rev 1 at 2, DOI: < 10.14324/111.444.ewlj.2019.14. > [Kanetake (2019)].

[25] *Special Economic Measures Act*, S.C. 1992, c. 17 [*SEMA*]; *United Nations Act*, R.S.C., 1985, C. U-2. A thorough discussion of these pieces of legislation is outside the scope of this article. However, it is worth noting that the scope of Canadian security concerns has on occasion been broadened to encompass human rights. Prior to 2017, the Canadian government could only impose sanctions under *SEMA* for a "grave breach of international peace and security" yet Canada sanctioned countries like Zimbabwe and Myanmar. The actions of these countries did not appear to threaten international peace or pose a threat to Canada but the governments of both did have atrocious human rights records, and this was likely a major influence in imposing sanctions. See Michael Nesbitt, "Canada's 'Unilateral' Sanctions Regime Under Review: Extraterritoriality, Human Rights, Due Process, and Enforcement in Canada's Special Economic Measures Act" (2017) 48:2 Ottawa L Rev 513 at 525. Further, in 2017, Canada passed the *Justice for Victims of Corrupt Foreign Officials Act* which among other things amended *SEMA* to allow Canada to impose sanctions in response to "gross and systematic human rights violations." *See Justice for Victims of Corrupt Foreign Officials Act*, S.C, 2017, c. 21; *SEMA*, *supra* note 25, s. 4 (1.1) (c).

[26] See Ben Wagner & Stéphanie Horth, "Digital technologies, human rights and global trade? Expanding export controls of surveillance technologies in Europe, China and India" in Ben Wagner, Matthias C Kettemann & Kilian Vieth, eds, *Research Handbook on Human Rights and Digital Technology* (Cheltenham: Edward Elgar, 2019) at 299.

[27] UNTS 3013 (entered into force 24 December 2014) [*ATT*].

Under subsection 3(1) of the *EIPA*, the Governor-in-Council can establish an "Export Control List" and place articles on it which they deem necessary to control for any of the listed purposes.[28] These purposes are based on national security and economic concerns and do not include an express concern for human rights impacts. Under section 4 of the *EIPA*, the Minister can also establish a list of countries and control any export or transfer of goods or technology to that country.[29] The Minister can place a country on such an "Area Control List" when they deem it necessary, giving them a much wider latitude than with the Export Control List. This power is used sparingly, however, because it covers *all* exports to that country. North Korea is the only country currently on the Area Control List.[30]

Section 7 and following of the *EIPA* set out powers regarding the issuance of export permits and certificates. Subsection 7(1) empowers the designated Minister to issue a permit to "export or transfer goods or technology included in an Export Control List or to export or transfer goods or technology to a country included in an Area Control List" (and the Minister can also issue a general permit for the same under subsection 7(1.1)).[31] Under subsections 7.1(1) and (2), the Minister "may issue" a specific or general "permit to broker in relation to any goods or technology specified in the permit" as well.[32]

Under section 7.2, the Minister "may take . . . into consideration whether the goods or technology" in the permit application "may be used for a purpose prejudicial to the safety or interests of the State by being used to do anything referred to in paragraphs 3(1)(a) to (n) of the *Security of Information Act*".[33] More specifically, under subsection 7.3(1), the Minister is also subject to some mandatory considerations, in respect of arms, ammunition, implements, or munitions of war, as to whether the goods or technology in the permit would contribute or undermine peace and security or be used to commit violations of international human rights law (among other grounds).[34] Subsection 7.4 of the *EIPA* provides that the Minister:

> *[S]hall not issue* a permit under subsection 7(1) or 7.1(1) in respect of arms, ammunition, implements or munitions of war if, after considering available mitigating measures, he or she determines that there is a *substantial risk* that the export or the brokering of the goods or technology specified in the application for the permit would result in any of the negative consequences referred to in subsection 7.3(1).[35]

---

[28] *EIPA*, *supra* note 10, s. 3(1).

[29] *Ibid.,* s. 4.

[30] *EIPA*, *supra* note 10, *Area Control List*, SOR/81-543.

[31] *EIPA*, *supra* note 10, ss. 7(1)—(1.1).

[32] *Ibid.,* ss. 7.1(1)—(2).

[33] *Ibid.,* s. 7.2.

[34] *Ibid.,* s. 7.3(1).

[35] *Ibid.,* s. 7.4 (emphasis added).

As noted, the negative consequences referenced in subsection 7.3(1) include those that would result in a "*serious* violation of international human rights law".[36]

Thus, in the case of arms, ammunition, implements, or munitions of war, it is clear that the government is now required to consider how issuing an export permit to the company seeking to export that item abroad would impact human rights. For other goods subject to export control, it remains somewhat ambiguous as to whether they are mandatorily subject to the same "substantial risk" test. However, government guidance contained in the "Export and brokering controls handbook" suggests that all exports will be subject to such an analysis.[37] Further, it is necessary to underline that the possibility of negative human rights impacts arising from an export is not a basis in and of itself for export control. There must be some pre-existing basis, listed in subsection 3(1) if there is no destination-based control, for an item to be subject to export control and then, consequently, reviewed on the basis of human rights.[38]

In order to understand the realistic impact of these amendments to the *EIPA* on preventing exports that negatively impact human rights, it is necessary to briefly consider how "substantial risk" has been interpreted. Guidance on export control defines it as "compelling evidence" of a "connection between the proposed export and the negative consequences."[39] As noted, these negative consequences can include international human rights law violations. In a backgrounder document on the amendments for accession to the *ATT*, the Canadian government noted the types of questions that would arise in ascertaining negative consequences with respect to international human rights. These questions included whether the parties identified in the permit application have a "persistent record of serious violations of human rights" or whether there is "substantiated information to indicate that the items have been, or may be, used to commit serious violations of international human rights."[40] (These are factors that would have been present in the export of Netsweeper technology to, for example, Sudan).

---

[36] *Ibid.,* ss. 7.3(1)(b)(i)—(ii) (emphasis added).

[37] See Global Affairs Canada, Export Control Division, "Export and brokering controls handbook" (August 2019) at F.3, online: *Government of Canada* <www.international.gc.ca/trade-commerce/controls-controles/reports-rapports/ebc_handbook-cce_-manuel.aspx?lang=eng>. See also Government of Canada, "Questions and answers: Strengthening Canada's export control program" (28 January 2020), online: *Government of Canada* <www.international.gc.ca/trade-commerce/consultations/export_controls-controle_exportations/QandA-QetR.aspx?lang=eng> ["Strengthening Canada's export control program"].

[38] "Strengthening Canada's export control program", *ibid.*

[39] *Ibid.*

[40] Global Affairs Canada, "Global Affairs Canada's Proposed Strengthening of Canada's Export controls Regime" (30 January 2019) at 3, online (pdf): *Government of Canada* <www.international.gc.ca/trade-commerce/consultations/export_controls-controle_exportations/background-information.aspx?lang=eng>.

While the inclusion of a substantial risk test was a step in the right direction in terms of furthering State protection of human rights in so far as they impact persons abroad, a 2019 briefing note regarding Canadian exports to Saudi Arabia suggests that the Canadian government will not take a robust approach in its application where significant economic and political factors may be in play. This note concluded that "[w]hile the overall Saudi human rights record is [REDACTED] problematic, Canadian officials have no information or evidence linking Canadian exports of military equipment or other controlled items to any human rights violations committed by the Saudi government."[41] Thus, Global Affairs Canada was of the view that "there is no substantial risk that current Canadian exports of military equipment or other controlled items to [Saudi Arabia] would result in any of the negative consequences referred to in section 7.3(1) of the [*EIPA*] within [Saudi Arabia]."[42] While the Canadian government froze exports to Saudi Arabia in 2018 after the murder of Jamal Khashoggi, it resumed exports in the spring of 2020.[43] Considering the widespread and readily available evidence of human rights abuses by Saudi Arabia, both domestic and abroad, most notably in the context of the war in Yemen,[44] this begs the question of whether there could ever be a "substantial risk" with regard to human rights and a controlled Canadian technology export.[45] While this article does not address this particular issue of interpretation and enforcement in more depth, it is illustrative of a broader problem that we seek to partially address in our reform proposal: potential government inaction.

(b) The Wassenaar Arrangement and the Regulation of Exports of Dual-use Technology under Canadian Export Law

In order to understand the gap in Canada's export control regime with regard to Netsweeper technology, it is also necessary to briefly review how dual-use technology—understood in the context of the *Arrangement* as technology having both military and civilian purposes[46]—is subject to export controls in

---

41 Global Affairs Canada, "MEMORANDUM FOR INFORMATION: Update on export permits to Saudi Arabia" (17 September 2019) at 3, online (pdf): *Government of Canada* < www.international.gc.ca/trade-commerce/controls-controles/arms-export-saudi-arabia_exportations-armes-arabie-saoudite.aspx?lang = eng >

42 *Ibid.*

43 David Moscrop, "Weapons sales to Saudi Arabia reveal that Canada is willing to trade jobs for its principles", *Washington Post* (10 April 2020), online: < www.washingtonpost.com/opinions/2020/04/10/weapons-sales-saudi-arabia-reveal-that-canada-is-willing-trade-jobs-its-principles/ > .

44 Nick Cumming-Bruce, "War Crimes Committed by Both Sides in Yemen, U.N. Panel Says", *The New York Times* (3 September 2019), online: < www.nytimes.com/2019/09/03/world/middleeast/war-crimes-yemen.html > .

45 See Jennifer Pedersen, "'We Will Honour Our Good Name': The Trudeau Government, Arms Exports, and Human Rights" in Norman Hillmer & Philippe Lagassé, eds, *Justin Trudeau and Canadian Foreign Policy* Canada and International Affairs (Cham: Springer International Publishing, 2018) 207.

Canada. And, further, this review broadly illustrates that novel human rights-infringing technologies that do not already fall within the *Arrangement* may not be caught by current export control rules.

The *Arrangement* has been adopted as the primary tool for regulating dual-use surveillance technology, although imperfectly,[47] and thus as the main international tool for regulating emerging cyber technologies that have both civilian and surveillance-type capabilities.[48] It was established in the 1990s in order "to contribute to regional and international security and stability" and facilitate international consensus on the export of arms and dual-use technologies.[49] The *Arrangement* is a non-binding international instrument, with Member States voluntarily incorporating its "Control List" into their own domestic export control regimes.[50] There is also an information exchange function, with countries sharing "information about specific denials and licenses."[51] Canada, which is a member of the *Arrangement*, has included the export restrictions spelled out in the *Arrangement* through the inclusion of the *Arrangement*'s Control List in Groups 1 and 2 under the *EIPA* Export Control List.[52]

The *Arrangement* itself did not originate in a specific concern for human rights.[53] As Ruohenen and Kimppa note, the *Arrangement* was originally driven by the goals of preventing the proliferation of weapons of mass destruction and improving the transfer regulation of conventional arms.[54] However, concern for human rights increased with negotiations leading to the *ATT*[55] and developments

---

46 See Kanetake (2019), *supra* note 24 at 2.

47 See *e.g.* Fabian Bohnenberger, "The Proliferation of Cyber Surveillance Technologies Challenges and Prospects for Strengthened Export Controls" (2017) 3:4 Strategic Trade Rev 81; David Kaye, *Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, HRC, 41st Sess, UN Doc A/HRC/41/35 (2019).

48 Wagner & Horth, *supra* note 26.

49 *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Public Documents: Volume I: Founding Documents*, WA-DOC (17) PUB 001, compiled by Wassenaar Arrangement Secretariat (February 2017) at 4 [*Wassenaar Arrangement Founding Documents*].

50 Wagner & Horth, *supra* note 26 at 300—301.

51 *Ibid.*

52 "Export and brokering controls handbook", *supra* note 37. It is worth noting that there is a delay in Canada's implementation in domestic law of updates to the *Arrangement*'s Control List. See Jessica B Horwitz, Sabrina A Bandali & Sreedhar Cheekoori (Bennett Jones LLP), "Amendments to Canada's Export Control List Take Effect May 1, 2020" (1 May 2020), online: *Lexology* < www.lexology.com/library/detail.aspx?g = ae409b69-73a4-4467-83d8-590f04df2176 > .

53 Wagner & Horth, *supra* note 26 at 302.

54 Jukka Ruohonen & Kai K Kimppa, "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity" (2019) 16:2 J Information Technology & Politics 169.

regarding the deployment of surveillance technology and its impact on human rights eventually led to the expansion of the *Arrangement* (and, more broadly, greater concern for human rights in export controls).[56] Thus, in 2013, "IP network communications surveillance systems or equipment" and "intrusion software" were added to the Control List. As Wagner and Horth summarize, the goal of these additional entries was to prevent the use of technologies in the context of state repression, surveillance, and human rights abuses.[57]

While the 2013 amendments to the *Arrangement* were lauded for expanding its scope to capture surveillance technologies used by repressive regimes abroad, these amendments—according to a technical analysis by Access Now—did not capture Internet-filtering tools such as those produced by Netsweeper.[58] We argue that such technology should be captured by export control in some manner, considering its potential for interfering with internationally-protected human rights. This could be accomplished through different mechanisms, such as by revising the *Arrangement*'s Control List to include Internet-filtering technology, which would eventually be adopted in domestic law in Canada through the *EIPA* Export Control List. Alternatively, as recommended by the Senate Standing Committee on Human Rights, another option is to make explicit reference to respect for internationally-recognized human rights in subsection 3(1) of the *EIPA*.[59] Thus, the Minister could designate an item as subject to export control—and thus require a permit—because of the human rights impacts the good could have abroad. Finally, new requirements could also be made for technology companies to engage in a human rights due diligence analysis, which could then trigger the application of export controls and a review by the government before a permit is issued.[60] An expanded version of this proposal is the focus of this article.

---

55 *Ibid.*

56 Wagner & Horth, *supra* note 26 at 302—303.

57 *Ibid.* at 303—306. However, as the authors note, there was a backlash against the scope of the amendments, leading to a narrowing of these controls in 2017. See *ibid.* at 305; Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research" (5 January 2018), online (blog): *Lawfare* <www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research>.

58 See Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies" (Access Now, 2015) at 27. See also Canada, Senate, Standing Senate Committee on Human Rights, *Evidence from Ronald J. Deibert, Professor of Political Science, University of Toronto, Munk School of Global Affairs*, 41-1, No 12 (30 November 2016). It may be that with additional information regarding Netsweeper's products there is a basis for concluding that it is export control, but this article proceeds on research that this is not currently the case.

59 Canada, Senate, Standing Senate Committee on Human Rights, "Promoting Human Rights: Canada's Approach to its Export Sector" (June 2018) at 22.

60 The Standing Senate Committee on Human Rights similarly recommended, although in less precise language, that "[c]onsideration should be given to embedding due-diligence

Under the current export regime, the Canadian government provides technical descriptions of what products are on the *EIPA* Export Control List. In the case of technology, as the Netsweeper case and, more broadly, as definitional wrangling around the language of the *Arrangement* shows, this can be a difficult venture as technical specifications are complex and constantly evolving. Furthermore, the dual-use nature of many technologies can make it difficult to label a product as nefarious based on a technical description alone. Rather, the context of use and the end-user itself are significant. Thus, in this next section of the article, we review the human rights due diligence framework in the UNGPs and note a broader normative trend towards mandatory human rights due diligence in the business sector in various domestic jurisdictions. We then articulate in more detail how a human rights due diligence requirement on Canadian technology businesses seeking to export might look in law and what the implications would be for such a change to the export control regime and the availability of remedies in the face of human rights harms. While mandatory due diligence has a role to play in restricting human rights abuses linked to Canadian business activities more generally, it may prove particularly critical in the area of technology exports where technical capacities are developed in secrecy, are rapidly evolving and changing, and where item-specific regulation may not be sufficiently swift to keep up.

3. THE UNITED NATIONS GUIDING PRINCIPLES AND THE TREND TOWARDS MANDATORY HUMAN RIGHTS DUE DILIGENCE

In this section, we review and discuss issues surrounding the UNGPs and describe a broader normative trend towards nailing down the substantive content and operation of human rights due diligence requirements through incorporation in domestic legislation.

(a) Mixed Meanings: Due Diligence in the UNGPs

While there is a global normative trend towards the inclusion of mandatory human rights due diligence in domestic legislation, there are differing and sometimes conflicting understandings of what human rights due diligence means. In 2011, the UN Human Rights Council unanimously endorsed the UNGPs.[61] While the UNGPs are not a legally-binding instrument, the endorsement established—for the first time—a consensus on the responsibilities of both States and businesses in regard to transnational business operations.[62] Under this

obligations related to end-uses and end-users in contracts for the export and sale of Canadian military and strategic goods." See *supra* note 59 at 25.

[61] See "Business and Human Rights", online: *United Nations Human Rights Office of the High Commissioner* < www.ohchr.org/EN/Issues/Business/Pages/BusinessIndex.aspx > .

[62] *Frequently asked questions about the guiding principles on business and human rights,* United Nations Human Rights Office of the High Commissioner (OHCHR), UN Doc

framework, States have a duty to *protect* human rights and must set clear expectations for how businesses domiciled in their jurisdiction operate abroad.[63] Business entities, meanwhile, must *respect* human rights, which is a lower threshold than protect but one with some semblance of a positive duty.[64] Both States and companies are subject to an obligation to provide access to a remedy in the case of human rights violations.[65]

Principle 15 of the UNGPs elaborates on how business enterprises can operationalize their respect for human rights, most notably by having "a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights."[66] Principle 17 elaborates on the content of human rights due diligence. Namely, "[t]he process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed."[67] Further, such due diligence should cover three types of adverse human rights impacts: (1) where the business causes or may cause human rights harms, (2) where the business contributes or may contribute to human rights harms, and (3) where the business has not contributed to the human rights harms, but the negative impact is linked to its operations.[68]

Human rights due diligence is considered by many scholars and commentators to be a central and key concept to emerge from the UNGPs, defining the corporate responsibility to respect human rights.[69] Yet despite its

---

HR/PUB/14/3 (2014) at 8, online (pdf): < www.ohchr.org/documents/publications/faq_principlesbussinesshr.pdf > .

63 See *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework,* OHCHR, UN Doc HR/PUB/11/04 (2011) at 3—4, online (pdf): < www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf > [UNGPs].

64 See *ibid.* at 13—16.

65 See *ibid.* at 27—28.

66 *Ibid.* at 15—16.

67 *Ibid.* at 17—18.

68 John Gerard Ruggie & John F Sherman, III, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquodale" (2017) 28:3 Eur J Intl L 921 at 927, DOI: < 10.1093/ejil/chx047 > .

69 See *e.g.* Björn Fasterling & Geert Demuijnck, "Human Rights in the Void? Due Diligence in the UN Guiding Principles on Business and Human Rights" (2013) 116:4 J Bus Ethics 799 at 801, DOI: < 10.1007/s10551-013-1822-z > (arguing that there is a tension in the UNGPs between the central concept of due diligence, which the authors describe as the "heart of Principles' conception of corporate responsibility to respect human rights", and the alternative argument that respecting human rights is a perfect [moral] duty which represents the 'cost of doing business'); James Harrison, "Establishing a meaningful human rights due diligence process for corporations: learning from experience of human rights impact assessment" (2013) 32:2 Impact Assessment and Project Appraisal 107 at 108, DOI: < 10.1080/14615517.2013.774718 > (similarly

prominent role in the UNGPs, human rights due diligence is still a relatively amorphous concept and has been the subject of extensive debate.

An interpretive guide on respecting human rights issued by the UN Office of the Commissioner of Human Rights defines human rights due diligence as an "ongoing management process that a reasonable and prudent enterprise needs to undertake, in the light of its circumstances (including sector, operating context, size and similar factors) to meet its responsibility to respect human rights."[70] While this may seem straightforward, human rights due diligence may take on different meanings and operations, and there have been conflicting understandings emerging in the literature.[71] To some, for example, the term imposes the business concept of "due diligence" and represents a way of managing risk and choosing whether to proceed with a certain course of action.[72] In contrast, to others the term imposes a legal norm of "due diligence" and represents a "standard of conduct" required to discharge a legal obligation and avoid liability. In this second camp, there may also be differing interpretations on whether a due diligence standard of conduct is appropriate in the face of human rights harms or whether there should be strict liability for business actors who cause human rights violations and due diligence should be reserved for harms caused by third parties.[73] To others, including Ruggie, the lead author of the UNGPs, human rights due diligence was never intended to denote a legal standard of conduct. It was intended to serve as a company's *social* license to operate, not its *legal* license.[74] From this viewpoint, a business enterprise's respect for human rights is not a specific legal obligation but an expected standard of conduct enforced through norms and social pressure that applies over and above any specific requirements of law.[75]

---

noting that human rights due diligence is "the central component" of the corporate to duty respect human rights under the UNGPs and that the core procedural element will likely involving a human rights impact assessment, although noting that there are shortcomings in that procedural process that have to be overcome); Jonathan Bonnitcha & Robert McCorquodale, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights" (2017) 28:3 Eur J Intl L 899 at 900, DOI: <10.1093/ejil/chx042> (finding that due diligence "is at the heart" of the UNGPs but arguing that the UNGPs invoke due diligence as two concepts—as a process to manage risk and as a standard of conduct to avoid liability—which causes confusion in what exactly is meant by due diligence). *Contra* Ruggie & Sherman, *supra* note 68 at 923 (who argue that the UNGPs are more complex than just a due diligence requirement and that "human rights due diligence is but one component of a more complex system").

[70] *The corporate responsibility to respect human rights: An interpretive guide*, OHCHR, UN Doc HR/PUB/12/02 (2012) at 6, online (pdf): <www.ohchr.org/documents/publications/hr.pub.12.2_en.pdf>.

[71] See *e.g.* the debate between Bonnitcha & McCorquodale, *supra* note 68 and Ruggie & Sherman, *supra* note 69 on the meaning ascribed to due diligence in the UNGPs.

[72] See *ibid.*

[73] See Bonnitcha & McCorquodale, *supra* note 69.

[74] See Ruggie & Sherman, *supra* note 69 at 923.

(b) Greater Clarity? Defining Human Rights Due Diligence in Domestic Law

In addition to conceptual concerns regarding the meaning and role of due diligence, there is also overlap between State obligations under international human rights law, due diligence, and the obligations of business actors. As noted in Principle 4, there may be situations where States should be "requiring human rights due diligence."[76] Indeed, State authorities may be able to fulfil their duty to protect human rights by creating a legal obligation (such as a due diligence obligation) for corporations to fulfil their duty to respect human rights. This intersection between the State's duty to protect and a business enterprise's duty to respect means that the line between legal and social duty, as noted by Ruggie, is perhaps not clearly demarcated, and can be expected to shift over time. Many scholars and commentators see the UNGPs' introduction of the responsibility to respect human rights as leading to the eventual crystallization of consequential and concrete legal duties.[77] For Muchlinski, since the UNGPs advocate for due diligence mechanisms, and due diligence mechanisms normally create direct duties of care, this evolution is expected, if not inevitable. Muchlinski supports this argument, in part, with the example of Canada, where the general concept of due diligence found its roots as a simple risk assessment process before gaining judicial legitimacy as a defence to strict liability offences, to its current role as a central component of environmental, health, safety, and securities regulatory regimes and a proxy for "reasonableness" in civil tort cases.[78]

Indeed, academic commentators have accurately forecasted efforts at human rights due diligence codification in domestic law with attached enforceable legal obligations. In 2017, France adopted its *Duty of Vigilance Law,* which requires all transnational businesses over a certain size to establish and implement an effective due diligence process for monitoring severe human rights violations that arise directly or indirectly from their operations.[79] At the time of writing this

---

[75] See *ibid.* at 924.

[76] UNGPs, *supra* note 63 at 6.

[77] Olga Martin-Ortega, "Human Rights Due Diligence for Corporations: From Voluntary Standards to Hard Law at Last?" (2013) 31:4 Nethl Intl L Rev 44; Doug Cassel, "Outlining the Case for a Common Law Duty of Care of Business to Exercise Human Rights Due Diligence" (2016) 1:2 Bus & Human Rights J 179, DOI: <10.1017/bhj.2016.15>; Peter Muchlinski, "Implementing the New UN Corporate Human Rights Framework: Implications for Corporate Law, Governance, and Regulation" (2012) 22:1 Bus Ethics Q 145; Radu Mares, "Global Corporate Social Responsibility, Human Rights and Law: An Interactive Regulatory Perspective on the Voluntary-Mandatory Dichotomy" (2010) 1:2 Transnational Leg Theory 221, DOI: <10.1080/20414005.2010.11424508>.

[78] Muchlinski, *supra* note 77 at 157. Further, in other fields, such as international environmental law, due diligence is a central component of the prevention principle and demonstrates the legal operation of this term. See *e.g.* Timo Koivurova, "Due Diligence" in Anne Peters & Rüdiger Wolfrum, eds, *Max Planck Encyclopedias of International Law*, (Oxford University Press, 2010).

article, Germany is considering a *Federal Bill on the Strengthening of Corporate Due Diligence to Avoid Human Rights Impacts in Global Value Chains*,[80] meanwhile the Finnish government has committed to exploring mandatory human rights due diligence laws.[81] Further, in October 2020, the European Commission launched a public consultation on a possible sustainable corporate governance initiative, just several weeks after the European Parliament Committee on Legal Affairs developed its own recommendation for a new *Directive on Corporate Due Diligence and Corporate Accountability*.[82] The European Commission previously promised mandatory due diligence legislation in 2021 and in January 2021, the European Parliament adopted a report calling on the European Union to legally require companies to protect human rights in supply chains.[83] Other laws, such as the United States' due diligence requirements for conflict minerals in the *Dodd-Frank Act* and the proposed Dutch *Child Labour Due Diligence Law*, adopt human rights due diligence for specific issues.[84] In short, there is a growing normative trend towards

---

[79] *LOI n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*, JO, 28 March 2017, 0074 [*Duty of Vigilance Law*].

[80] See Suzanne Spears & Udo Herbert Olgemöller, "Mandatory human rights due diligence laws: Germany takes another step towards global value chain regulation" (20 October 2020), online: *Allen & Overy* <www.allenovery.com/en-gb/global/news-and-insights/publications/mandatory-human-rights-due-diligence-laws-germany-takes-another-step-towards-global-value-chain-regulation>.

[81] See Maysa Zorob, "The Lengthy Journey towards a Treaty on Business & Human Rights", (30 September 2019), online: *Business & Human Rights Resource Centre* <www.business-humanrights.org/en/the-lengthy-journey-towards-a-treaty-on-business-human-rights>. See also Nicolas Bueno, "The Swiss Popular Initiative on Responsible Business: From Responsibility to Liability" in Liesbeth Enneking et al, eds, *Accountability, International Business Operations and the Law: Providing Justice for Corporate Human Rights Violations in Global Value Chains* (Routledge, 2019) 239 (on a proposal to introduce a human rights and environmental due diligence requirement to the Constitution of Switzerland.)

[82] Suzanne Spears & Camille Leroy, "A first step towards EU-wide legislation on mandatory human rights due diligence" (29 October 2020), online: *Allen & Overy* <www.allenovery.com/en-gb/global/news-and-insights/publications/a-first-step-towards-eu-wide-legislation-on-mandatory-human-rights-due-diligence>.

[83] European Parliament Working Group on Responsible Business Conduct, "European Commission promises mandatory due diligence legislation in 2021" (30 April 2020), online: *Responsible Business Conduct* ; European Parliament, "MEPs: Hold companies accountable for harm caused to people and planet" (27 January 2021), online: *European Parliament* <www.europarl.europa.eu/news/en/press-room/20210122IPR96215/meps-hold-companies-accountable-for-harm-caused-to-people-and-planet>.

[84] *Dodd-Frank Wall Street Reform and Consumer Protection Act*, Pub. L. No. 111-203, 124 Stat. 13776 (2010) [*Dodd Frank Act*]; Zorob, *supra* note 81. See also James Reardon & Tomas Navarro, "The dawn of human rights due diligence in Switzerland?" (December 7, 2020), online (blog): *The FCPA Blog* <fcpablog.com/2020/12/07/the-dawn-of-human-rights-due-diligence-in-switzerland/> (on the Swiss government's proposed reform of the Code of Obligations and Criminal Code that introduces due diligence requirements with respect to minerals and metals from conflict zones and child labour).

conceptualizing international human rights law obligations on States as requiring the imposition of due diligence in its legal form on the domestic business sector. While not all concepts and operations of due diligence are the same in these legal instruments,[85] we argue that the inclusion of due diligence as part of a legislative structure provides a mechanism for iterating specific obligations and potentially prescribing real avenues for enforcement and remedy.

(c) Meta-regulation and the Furtherance of Regulatory Objectives

Laws mandating human rights due diligence tend to avoid imposing exact standards, and instead encourage a form of self-regulation. For example, France's *Duty of Vigilance Law* includes only five requirements for a "Vigilance Plan": (i) risk-mapping; (ii) assessment plans of related entities; (iii) actions to prevent/mitigate; (iv) alert mechanisms; and (v) an ongoing monitoring scheme.[86] The "Conflict Mineral Report" required by the *Dodd-Frank Act* must contain: (i) a description of the measures taken to exercise due diligence; (ii) a description of the products manufactured or contracted to be manufactured with conflict minerals; and (iii) a certification that the due diligence measures were audited by an independent private sector auditor.[87] Such a regulatory system has been called "meta-regulation," and is designed to stimulate modes of self-organization that encourage a proactive response from the business enterprise.[88] The role of the regulator becomes one of managing the risk management of the business enterprise.

There is qualified evidence that carefully designed meta-regulation systems coupled with management commitment and resources can indeed deliver substantial and sustained improvements in regulatory objectives.[89] In addition, it is a practical best option when the complexity, subjectivity, and variance between industry operations defies manageable regulatory standards. This is perhaps particularly the case in the technology industry, which is rapidly evolving and where regulation dependent on technical specifications has proved complicated. The expected downside to meta-regulation is "cosmetic compliance," i.e. the superficial adoption of procedures without meaningful substantive change.[90] Business enterprises are not incentivized to establish a strict regime with which to police themselves and governments are not incentivized to

---

[85] Bonnitcha & McCorquodale, *supra* note 69 at 906—908.

[86] *Duty of Vigilance Law*, *supra* note 79 art. 1.

[87] *Dodd Frank Act*, *supra* note 84, s. 1502(b).

[88] See Neil Gunningham, "Strategizing compliance and enforcement: Responsive regulation and beyond" in Christine Parker & Vibeke Lehmann Nielsen, eds, *Explaining Compliance: Business Responses to Regulation* (Northampton, MA: Edward Elgar Publishing, 2011) 199.

[89] See *ibid.*

[90] See *ibid.* Indeed, in the area of dual-use technologies, there have been several instances of such cosmetic compliance. For example, some companies that develop spyware technology for use by state actors have proclaimed to be concerned with human rights,

label such regimes as insufficient if they surpass the potentially non-existent due diligence requirements of the business's foreign competitors. The imposition of additional legal requirements regarding transparency, external verification, and independent monitoring and review can help to mitigate the dangers of self-regulation.[91]

The limitations of meta-regulation mean that the codification of human rights due diligence into law does not definitively set the standards for business enterprises and is no guarantee that negative human rights impacts will be perfectly and fulsomely addressed. As with other broad regulatory regimes, the process of constructing meaning is political, and stakeholders—mainly business enterprises, civil society, and government—will compete for legal constructions of due diligence in favour of their interests. This battle will likely play out primarily in courts in jurisdictions that have adopted domestic mandatory due diligence models.[92] Regardless of these challenges, formalizing human rights due diligence and its requirements into law sets the basic parameters for interpretation and guides the discretion of a business's corporate social responsibility.[93] Formalization also moves human rights due diligence forward, transforming it from what may be seen as merely a soft norm and attaching real consequences and liabilities where it is not met. In this next section, we consider how mandatory human rights due diligence might be incorporated as a part of Canadian export controls to mitigate the potential export of human rights infringing technologies by Canada's technology business sector.

4. DEVELOPING MANDATORY HUMAN RIGHTS DUE DILIGENCE FOR EXPORTING CANADIAN TECHNOLOGY COMPANIES

(a) Incorporating a Due Diligence Requirement into Canada's Export Regime

Canada has avoided specific legislative enactments or amendments in response to the UNGPs, preferring to pursue policy options to strengthen its domestic business and human rights framework. The most substantive addition, the creation of the Ombudsperson for Responsible Enterprise, was done with an existing budget and did not require a parliamentary vote.[94] No effort to codify human rights due diligence requirements has as of yet been made in Canada.

---

but researchers have found that their technologies are still being used against human rights defenders and civil society.

91 Harrison, *supra* note 69 at 111—116.

92 Christine Parker & Vibeke Lehmann Nielsen, "To Comply or Not to Comply - that isn't the question: how organizations construct the meaning of compliance" in Christine Parker & Vibeke Lehmann Nielsen, eds, *Explaining Compliance: Business Responses to Regulation* (Northampton, MA: Edward Elgar Publishing, 2011) 103.

93 Mares, *supra* note 77.

94 See generally Government of Canada, "Office of the Canadian Ombudsperson for

Canada's export control regime remains disassociated from the UNGPs, and while the *Justice for Victims of Corruption Foreign Officials Act* and the amendments necessary for compliance with the *ATT* have been passed, the Senate Standing Committee on Human Rights' recommendations regarding export control and emerging technologies discussed above have not been implemented or actively pursued by the current Trudeau government.[95] This inaction is in direct contrast to the same government's professed agenda of protecting and promoting human rights abroad.[96] Stretching the definition of international security and developing increasingly elaborate technical descriptions of controlled exports will not sufficiently cover dual-use technologies that negatively affect human rights. However, human rights due diligence requirements on Canadian technology businesses as a condition to export could potentially help to fill this gap.[97] The greater incorporation of human rights concerns in the context of export control in Canada would follow a normative growing trend, where human rights concerns are beginning to seep into international trade and international investment regimes, as well as domestic law regimes, and give Canadian international human rights policy real teeth.[98]

What could such a legislative regime look like? The *EIPA* could be amended to specifically require all technology companies that manufacture or design technology products for export from Canada to undertake a mandatory[99] human

---

Responsible Enterprise" (1 March 2020), online: < core-ombuds.canada.ca/core_ombuds-ocre_ombuds/index.aspx?lang = eng > .

95 See Standing Senate Committee on Human Rights, "Promoting Human Rights", *supra* note 59.

96 See Government of Canada, "Canada's approach to advancing human rights" (9 January 2020), online: *Government of Canada* < www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_-rights-promouvoir_droits.aspx?lang = eng > .

97 As Kanetake notes in a review of amendments to dual-use regulation in the EU, "the export control of digital and emerging technologies cannot be separated from the wider normative development at the regional and international levels. In particular, the decisions to export such technologies cannot be exempt from the expectation to integrate the UNGPs' human rights due diligence in all aspects of business practices." See Machiko Kanetake, "Controlling the Export of Digital and Emerging Technologies" (2021) Security & Human Rights 1 at 10, DOI: < 10.1163/18750230-31010005 > [Kanetake (2021)]. Such an amendment, of course, is not a panacea that will remedy the situation in and of itself. In particular, progress in ensuring respect for human rights abroad by Canadian technology companies will rest to a large extent on the existence of a robust enforcement regime for any due diligence obligations and ensuring that the Canadian government is held to account over export control decisions.

98 See Wagner & Horth, *supra* note 26 (on this trend in Europe, China, and India).

99 The Canadian Export and brokering controls handbook does note that: "[i]n addition to compliance with the EIPA, exporters and brokers of controlled goods and technology have a responsibility to conduct due diligence verification of actual and potential foreign customers and to provide all relevant information in their permit applications" and that this "assessment should be seen as another step in the exporter's due diligence process."

rights due diligence program to examine the potential or existing human rights impacts of their proposed export products in the three scenarios envisaged by the UNGPs: where a company causes or may cause negative human rights impacts, contributes to or may contribute, or their operations are or may be linked to such impacts. The minimum requirements of such due diligence could look similar to the French *Duty of Vigilance Law* and include, for example, a requirement of risk-mapping in relation to human rights impacts of exported technology, identification of actions to prevent and mitigate any negative impacts, alert mechanisms, and the development a monitoring and public reporting scheme. They could also include direct guidance from the UNGPs, the associated commentary of which elaborates on the specific timing, scope, and modality of such assessments.[100] While an exhaustive discussion of what human rights should concern companies is beyond the scope of this article, a starting point could be a requirement that companies consider Canada's international human rights obligations.[101]

In cases where human rights due diligence by a company reveals a reasonable risk of infringement of human rights through the use of their exported product, the company would be required to bring this information to the attention of the relevant Canadian government authorities and to submit an application for an export permit. The application would include specific details and findings regarding the due diligence program as well as mitigation strategies that could be used to reduce the risk of rights infringement. Global Affairs Canada would consider the information as part of a broader analysis in determining whether there was a "substantial risk" of negative human rights impacts requiring the denial of an export license. Permits for technology exports could be granted contingent on the recipient (where the end-user is a State) having a sufficient legal framework to manage the potential risks generated by the technology and the company's implementation of mitigation strategies, including the provision of customer support conditional on compliance, incorporating protective measures into technological products (human-rights-by-design), contractual safeguards, or ongoing monitoring obligations. A specific mechanism for ongoing public consultation and cooperation between the company and civil

---

However, this appears to be phrased more as a recommendation than as binding language and there is no clear legal ramification for failing to conduct sufficient due diligence. The handbook also identifies the OECD Due Diligence Guidance for Responsible Business Conduct as something that "Canadian exporters should familiarize themselves with". See "Export and brokering controls handbook", *supra* note 37.

[100] See UNGPs, *supra* note 63 at 18—24. See *e.g.* Kaye, *supra* note 47 (regarding the implementation of the UNGPs in the context of the technology sector).

[101] Further, companies should be guided by the interpretative work of treaties bodies like the *International Covenant on Civil and Political Rights*' Human Rights Committee, which discusses the scope of application of treaty provisions in its General comments, as well as the reporting done by the UN Special rapporteurs analyzing the impact of technology on human rights.

society on the implementation of due diligence requirements and a subsequent monitoring program could also be a requirement to an export license. Such a regime would necessitate amending subsection 3(1) of the *EIPA* to include human rights impacts as a stand-alone ground for export control, in conjunction with this new obligation of due diligence on the business sector.[102]

Companies that fail to apply for an export license despite there being a reasonable risk of human rights infringement or fail to follow-through on the conditions of their permit could be found in violation of the *EIPA* and face criminal sanctions. Such failures could also give rise to civil liability, as will be discussed below. At a minimum, even if the government was permissive in granting permits and civil liability was not established, the incorporation of human rights due diligence into the export control system could help to provide much needed transparency into the exporting of dual-use technologies, particularly if Canada's export control system moved more fully to an open data system as opposed to requiring access to information requests. In this context transparency would enable civil society to monitor for—and subsequently advocate against—exports that would offend the conscience of Canadians.[103] In addition, such transparency may increase corporate regulatory compliance and help establish appropriate norms.[104]

A human rights due diligence mechanism for Canadian exports would complement and be facilitated by the existing business and human rights ecosystem in the country and abroad. Over the next few years, the new Office of the Ombudsperson for Responsible Enterprise will hopefully develop the requisite capacity to investigate allegations of human rights abuses abroad and

---

[102] This article does not purport to provide a complete answer to the content of a human rights due diligence analysis but suggests some contours. As Lauterbach knows, more analysis is required to set out a comprehensive framework. See Claire Helen Lauterbach, "No-go zones: Ethical geographies of the surveillance industry" (2017) 15:3/4 Surveillance & Society 557, DOI: < 10.24908/ss.v15i3/4.6616 > . Further, EU documentation may prove a useful resource in outlining key facts that the human rights due diligence process should be designed to ascertain and assess. See *e.g.* Council of the EC, *User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment,* [2019], online (pdf): *European Council* < www.consilium.europa.eu/media/40659/st12189-en19.pdf > .

[103] See *e.g.* the comprehensive database on UK Arms Licenses, online: *Campaign Against Arms Trade* < www.caat.org.uk/resources/export-licences > . Canada's annual "Report on the export of military goods" excludes items that are not "designed for military purposes" and thus does not cover information regarding Canadian export of dual-use technology. See Government of Canada, "2019 Exports of Military Goods", online (pdf): *Government of Canada* < www.international.gc.ca/trade-commerce/controls-controles/reports-rapports/military-goods-2019-marchandises-militaries.aspx?lang = eng > .

[104] See Raymond Robertson, "Lights On: How Transparency Increases Compliance in Cambodian Global Value Chains" (2019) 73:4 Industrial & Labour Relations Rev 939, DOI: < 10.1177/0019797393919893333 > ; Bjorn Fasterling, "Development of Norms through Compliance Disclosure" (2012) J Bus Ethics 106, 73, DOI: < 10.1007/s10551-011-1055-y > .

strengthen Canada's enforcement capabilities in instances where companies were deficient in their due diligence obligations.[105] Furthermore, the Ombudsperson is already mandated with advising Canadian companies on their practices and policies with regard to responsible business conduct, making them an obvious outlet to issue guidance on when and how companies should conduct human rights due diligence for their exports. International industry groups like the information communications technology sector's Global Network Initiative could also play a role in standardizing appropriate levels of diligence for their industry through published codes of conduct, statements of principles, and other guidance. Meanwhile, Canada's Organization for Economic Co-operation and Development National Contact Point could advocate for other OECD members implementing similar export regimes, helping to level the playing field for Canadian businesses.

At the risk of such a mechanism seeming far-fetched, it is worth noting that a proposal moving export control towards a greater focus on human rights[106] (including integrating human rights due diligence)[107] has been accepted by the European Parliament and Council.[108] Although, negotiations towards this draft were challenging and civil society has raised concerns with continued shortcomings in the accepted language.[109] The proposed language of the EU's recast dual-use regulation provides that an export authorisation is required for the export of "cyber-surveillance items" that are not already listed for export control where the "exporter has been informed by the competent authority that

---

[105] The Ombudsperson's mandate would need to be expanded beyond the garment, mining, and oil and gas sectors; however, this expansion is already intended to occur. The larger issue is whether the investigative powers given to Office of the Ombudsperson by the government are sufficient for them to fulfill their fact-finding role.

[106] As summarized by Kanetake (2019), *supra* note 24 at 6 "the proposal was an attempt to situate a consideration of human rights not as a marginal consideration, but as one of the key normative grounds for controlling the export of sensitive items", which was a distinct shift from the *Arrangement* because of its focus on human rights as a normative justification for export control (rather than one focused on military uses).

[107] The final compromise text also integrates language regarding due diligence obligations on exporting companies. See Kanetake (2021), *supra* note 97.

[108] At the time of drafting, the European Parliament and Council had agreed to amend the EU's Dual-Use Regulation, although the amendments had not yet become law.

[109] For critique on the draft language produced in November 2020, see Amnesty International et al, "Urgent call to the Council of the EU: Human Rights must come first in Dual Use first draft" (November 2020), online (pdf): *Amnesty International* < www.amnesty.eu/wp-content/uploads/2020/11/Letter-to-the-Council-Dual-Use.pdf > . See also Kanetake (2019), *supra* note 24 (for a detailed history of the progression of the negotiations). Ben Wagner argues that while "[e]xport controls are not a panacea for all human rights problems. . .they do provide a valuable basis for additional development of the international dual-use regime in a manner that supports human rights more effectively." See Ben Wagner, "Whose Politics? Whose Rights? Transparency, Capture and Dual-Use Export Controls" (2021) Security & Human Rights 1 at 11, DOI: < 10.1163/18750230-31010006 > .

the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law."[110] Further, if an exporter becomes "aware according to its due diligence findings" that such cyber-surveillance items it proposes to export, which are not listed, are intended to be used as such, it is required to notify the competent authority which shall decide on export authorisation.[111]

(b) Civil Liability to Enforce Due Diligence Requirements and Ensure a Remedy

Two other issues merit discussion from our proposal to incorporate mandatory human rights due diligence into the Canadian export scheme. First, while enacting such provisions is a significant first step, there is also a concern regarding 'cosmetic compliance' by companies and a lack of incentives for countries to hold businesses to a high standard for conducting and reporting in the context of human rights due diligence.[112] Second, responsibility under the UNGPs does not stop solely with due diligence, but also includes a principle of adequate and effective remedies.[113] We argue that both issues further favour the enactment of express human rights due diligence requirements under Canadian law and that this should include a specific mechanism for imposing liability where there is failure to comply with such legal due diligence requirements. While there will likely always be issues of enforcement by the government in terms of issuing an export license or not, the possibility of civil liability directly against companies who fail to meet due diligence requirements opens up new avenues for compliance.

More particularly, even if the Canadian government were to continue to interpret "substantial risk'" under the *EIPA* narrowly (as the Saudi situation suggests could be the case) or turn a blind eye to certain companies that fail to meet the requirements of the due diligence law, the due diligence obligations would exist separate and apart from government internal policy and the application of export control law. In countries like Canada with robust judicial systems and the possibility of material damage awards, this could provide an opportunity for creating a liability scheme that might be tied to meaningful

---

[110] See EC, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL setting up a Union regime for the control of exports brokering, technical assistance, transit and transfer of dual-use items (recast) - Confirmation of the final compromise text with a view to agreement*, Interinstitutional File: 2016/0295(COD), [2020], art 4(a)(1), online: *Council of the European Union* .

[111] *Ibid.* at art 4(a)(2).

[112] See *e.g.* Rachel Chambers & Anil Yilmaz Vastardis, "Human Rights Disclosure and Due Diligence Laws: The Role of Regulatory Oversight in Ensuring Corporate Accountability" (2021) 21:2 Chicago J Intl L 323.

[113] UNGPs, *supra* note 63 at 27—35.

remedies and provide incentive to companies to take their legal obligations seriously.

Civil liability against companies could be constructed by way of one of two mechanisms related to the imposition of mandatory human rights due diligence legislation: (1) express inclusion into relevant human rights due diligence export control legislation, or (2) through developments in the common law. In some instances, domestic due diligence laws have explicitly created civil liability. France's *Duty of Vigilance Law*, for instance, creates civil liability to compensate for the harm that the due diligence measures would have avoided had the business complied with the law.[114] A since-rejected Swiss proposal likewise functioned as a method of clarifying the legal consequences of failing to comply with due diligence duties.[115] (In contrast, laws such as the United Kingdom's *Modern Slavery Act,* California's *Transparency in Supply Chains Act,* or Australia's *Modern Slavery Act* function solely as a reporting tool and do not lead to civil liability.[116]) Besides statutory enactment, it is also open for courts in common law jurisdictions to find that a domestic business owes a duty of care to exercise human rights due diligence in their operations abroad.[117] Recognition of such a duty would mean that a corporation's failure to oversee their business operations would be subsumed under the law of negligence and would not require new nominate torts. While the Supreme Court of Canada has recently signalled a willingness to consider new nominate torts to cover human rights abuses, the law of negligence would offer the field of business and human rights more stable judicial footing and is conceptually easier to rectify with modern tort law.[118]

A 2016 survey of international case law found that no common law court has recognized corporations as having a duty of care to exercise human rights due diligence in their operations abroad.[119] The closest instance found was the 2013 decision in the ongoing Ontario case of *Choc v. Hudbay Minerals Inc*.[120] The case concerns alleged complicity in human rights violations by Hudbay at its mining operations in Guatemala. The issue to be decided in the preliminary motion was whether the plaintiffs were asserting a reasonable cause of action against Hudbay, given that the company's operations in Guatemala were overseen by a subsidiary and not Hudbay itself. Justice Brown of the Superior Court of Justice

---

[114] *Duty of Vigilance Law*, *supra* note 79, art. 2.

[115] Bueno, *supra* note 81.

[116] See Zoe McKnight, "Human Rights Due Diligence: Legislative Scan" (2018) Canadian Labour Congress Research Paper No 54, online (pdf): *Canadian Labour* <canadianlabour.ca/wp-content/uploads/2019/04/054-HRDD-Legislative-Scan-2018-09-26.pdf>.

[117] A duty of care to not commit human rights violations would be insufficient owing to the fact most violations would be committed by a third party or corporate subsidiary.

[118] See *Nevsun Resources Ltd. v. Araya*, 2020 SCC 5, 2020 CarswellBC 447, 2020 CarswellBC 448 (S.C.C.) at paras. 127-130.

[119] See Cassel, *supra* note 77 at 196-198.

[120] *Choc v. Hudbay Minerals Inc.*, 2013 ONSC 1414, 2013 CarswellOnt 10514 (Ont. S.C.J.).

for Ontario did not have to decide whether there was a duty of care, but rather whether such a duty was at least *arguable* and thus worth proceeding to trial. Employing the *Anns/Cooper* test, which is used by Canadian courts to evaluate a novel duty of care, Justice Brown held that it was not plain and obvious that Hudbay did not owe the plaintiffs a duty of care. This holding was based on the finding that the alleged human rights violations may have been both foreseeable and proximate to Hudbay executives who—based on the facts pled by the plaintiffs—knew of the risks and had repeatedly made representations and formulated the corporate response about how to deal with human rights concerns at the mine.[121]

The case of *Choc v. Hudbay Minerals Inc.* suggests the slow crystallization of human rights due diligence into a legal standard through common law, as argued by Muchlinski and others. But the emphasis is best placed on the word "slow." First, the case only stands for the proposition that it is arguable that such a duty exists, and it is only a trial court holding. Second, the proximity factor in the *Anns/Cooper* test requires a sufficiently close relationship between the plaintiff and defendant, which was made arguable in *Choc v. Hudbay Minerals Inc.* by the express representations and actions of Hudbay executives. The lesson that Canadian businesses may take from this decision is to limit what human rights representations they make regarding their business operations abroad. Thus, even if a duty of care is established in the *Choc v. Hudbay Minerals Inc.* case, it is perhaps unlikely to be repeated unless corporations have an explicit legal obligation to investigate and report on the human rights impact of their operations.

With these considerations in mind, and in the contexts of technology exports that impact human rights, the preferable avenue to ensure compliance and remedy would be amending the *EIPA* to mandate proactive human rights due diligence in all cases of a proposed export and impose express liability and remedy provisions where a company fails to do so or does so inadequately. That said, even in the absence of an express liability provision such as this, the creation of a legal obligation to consider affected populations through a proactive due diligence requirement could eventually contribute to a tipping point in establishing proximity between the parties and thus a duty of care. While failure to conduct the human rights due diligence at all or to a satisfactory degree would not automatically prove negligence, the standards imposed by a legal obligation to conduct human rights due diligence in the scenarios envisaged under the UNGPs would be highly relevant to the assessment of reasonable conduct in the standard of care.[122]

---

[121] See *ibid.* at para 69.

[122] *R. v. Saskatchewan Wheat Pool*, 1983 CarswellNat 521, 1983 CarswellNat 92, (*sub nom.* Canada v. Saskatchewan Wheat Pool) [1983] 1 S.C.R. 205 (S.C.C.) at paras. 225-226; *Ryan v. Victoria (City)*, 1999 CarswellBC 79, 1999 CarswellBC 80, [1999] 1 S.C.R. 201 (S.C.C.).

In summary, the inclusion of a proactive human rights due diligence requirement for exports could provide the nudge needed to establish a common law duty of care to exercise human rights due diligence. The creation of a liability mechanism against companies that export technologies that negatively impact human rights could also respond in part to the requirements under the UNGPs that States facilitate remedies for human rights violations. The impact of a proactive due diligence requirement on the duty of care and negligence liability is an important consideration, as government inaction remains a continual obstacle to enforcement and the explicit creation of civil liability through a statutory provision is unlikely to be added to Canada's export control regime. If a business is legally mandated to assess and report on the likely human rights impact of its enterprise abroad, finding a foreseeable and proximate relationship between the business and the affected populations becomes possible.

CONCLUSION

The discussion of human rights due diligence tends to focus on the business activities of subsidiary corporations. These subsidiaries—in sectors such as mining and textiles—often operate in States with insufficient governance mechanisms, where human rights abuses are likely to be committed, particularly regarding labour and environmental issues. Abuses in these cases may be considered somewhat incidental to the final product (i.e. they form a part of the supply chain, but the product itself as a whole—such as a t-shirt or a computer—does not give rise to a human rights violation). However, the UNGPs also apply to technology companies and the products they export abroad. Human rights abuses in these cases are not incidental to the production of a good, but may very well end up being a core feature of the goods or service offered in the context to which they are exported—as demonstrated by the Netsweeper case study.

Technologies that have the potential to negatively affect human rights are wide-ranging in their purposes and design and are constantly changing with technological advancements. In this article, we propose that an amendment to the *EIPA* could go further in ensuring that the exports of technology companies are examined for their potential to impact human rights negatively. While there are several mechanisms at ensuring this, we suggest that one to be explored is a proactive human rights due diligence requirement on technology companies seeking to export their products abroad. While this would be a substantial step forward in Canadian law, as described in this article, there is growing normative support for such due diligence requirements in other jurisdictions.