Brooklyn Journal of International Law

Volume 44
Issue 2 07/01/2019

Article 7

7-1-2019

The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware

Anna W. Chan

THE NEED FOR A SHARED RESPONSIBILITY REGIME BETWEEN STATE AND NON-STATE ACTORS TO PREVENT HUMAN RIGHTS VIOLATIONS CAUSED BY CYBER-SURVEILLANCE SPYWARE

INTRODUCTION

The advancement of technology and Internet connectivity has contributed significantly in the field of human rights.[1] Smartphones have enabled users to voice their unfiltered opinions about politicians, organize mass protests against social policies, and document and distribute images of police brutality through multiple platforms at a press of a button.[2] In fact, the mass protests marking the height of the Arab Spring[3] in 2011 were organized by activists empowered by Twitter, YouTube, Facebook and other social media outlets, while their respective authoritarian governments underestimated the potential of the Internet.[4] Unfortunately, the technology that "catalyzed the Arab Spring is only as good or as bad as those who use it."[5] The same authoritarian governments also turned to these social media outlets to spread misinformation and create alternative narratives.[6] Moreover, the very same regimes, and others alike, have devoted their wealth and authority to purchase surveillance spyware systems from multinational corporations to closely monitor Internet activity in order to track and extinguish

---

1. Emma Daly, *Why Tech is a Double-Edged Sword for Human Rights*, HUM. RTS. WATCH (Jan. 6, 2014), https://www.hrw.org/news/2014/01/06/why-tech-double-edged-sword-human-rights.

2. *Id.*

3. The Arab Spring was a wave of pro-democracy protests and uprisings that took place in the Middle East and North Africa beginning in 2010 and 2011, challenging some of the region's authoritarian regimes. *Arab Spring, Pro-Democracy Protests*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/event/Arab-Spring (last visited Oct. 20, 2017).

4. Jessi Hempel, *Social Media Made the Arab Spring, But Couldn't Save It*, WIRED (Jan. 26, 2016), https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/.

5. *Id.*

6. *Id.*

dissidents.[7] Examples of surveillance spyware used by regimes with abusive human rights records include: Amesys (purchased

7. Trevor Timm, *Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA*, https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa (last visited Oct. 20, 2017). *See also* Trevor Timm, *Spy Tech Companies & Their Authoritarian Customers, Part I: FinFisher and Amesys*, https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys (last visited Oct. 20, 2017). *See also* Nicole Perlroth, *Governments Turn to Commercial Spyware to Intimidate Dissidents*, N.Y. TIMES (May 29, 2016), https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?_r=0.

by Libya),[8] Gamma International (Bahrain),[9] NSO Group (Mexico, the United Arab Emirates and possibly Saudi Arabia),[10] Qosmos (Syria),[11] and Trovicor GmbH (Syria).[12] The use of spyware

---

8. FIDH, THE AMESYS CASE (2014), *available at* https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf. The Eagle-System produced by Amesys, a French corporation, was found to be present in Libya after the fall of the Gadhafi regime. *Id.*

9. *UK's OECD Guidelines Contact Point Finds Gamma, Breached Human Rights by Selling FinFisher Spyware to Bahrain*, EUR. COMM'N, https://ec.europa.eu/digital-single-market/en/news/uks-oecd-guidelines-contact-point-finds-gamma-breached-human-rights-selling-finfisher-spyware (last visited Sept. 30, 2017). Spyware produced by Gamma International, a British corporation, found in infected devices of three Bahraini activists. The British NCP found the actions of Gamma inconsistent with Chapter II and Chapter IV of the OECD Guidelines. *See* U.K. NATIONAL CONTACT POINT FOR THE OECD GUIDELINES FOR MULTINATIONAL ENTERPRISES, PRIVACY INTERNATIONAL & GAMMA INTERNATIONAL U.K. LTD: FINAL STATEMENT AFTER EXAMINATION OF COMPLAINT (2014), *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf.

10. Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. TIMES (June 19, 2017), https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?mcubz=1. Pegasus, spyware produced by NSO Group, an Israeli corporation, was found in Mexico. *Id.* The devices of several human rights lawyers and journalists were sent a series of texts infected with Pegasus, a software capable of infiltrating mobile devices to monitor every detail of a person's cellular life, including calls, texts, e-mails, contacts, and calendars. *Id.* The software is even capable of "us[ing] the microphone and camera on a phone for surveillance, turning a target's smartphone into a personal bug." *Id.* NSO made its first deal with the United Arab Emirates (UAE) in 2013, and "within a year, the Emirati government installed NSO spyware on the phone of Ahmed Mansoor, a prominent human rights activist." Mark Mazzetti et al., *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*, N.Y. TIMES (Mar. 21, 2019), https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html. Since then Mansoor lost his job, lost his passport, lost $140,000 USD in his bank account, was beaten, and sentenced to ten years in prison for "damaging national unity." *Id.* Most recently, Omar Abdaluaziz, a Montreal-based Saudi dissident and friend of deceased journalist Jamal Khashoggi, filed a lawsuit in Israel, "charging that NSO improperly helped the . . . UAE spy on individuals with no criminal records and who posed no threat of violence" via their smartphones. David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, N.Y. TIMES (Dec. 2, 2018), https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html. *See also* Oren Liebermann, *How a Hacked Phone May Have Led Killers to*

has not only resulted in the invasion of privacy of its citizens, but it has also led to a plethora of other human rights violations ranging from arbitrary detention and torture to death.[13]

This Note proposes a better regulatory method in the sale of surveillance spyware. This method entails a multi-stakeholder approach that builds upon the newly established International Code of Conduct (ICoC) for Private Security Service Providers[14] and its oversight committee, the ICoC Association (ICoCA).[15] The proposed multi-stakeholder approach will include an oversight committee, similar to the ICoCA, consisting of representatives from multinational enterprises (MNEs) or corporations that produce and sell cyber surveillance spyware, representatives from civil society groups, such as Human Rights First or Amnesty International, and representatives from states. Similar to the ICoCA, this multi-stakeholder approach may encourage more transparency by requiring MNEs to complete reporting, monitoring and certification requirements. This proposed model, however, will require states to take a more active role and to

---

Khashoggi, CNN (Jan. 20, 2019), https://www.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html. Researchers at Citizen Lab confirmed Abdaluaziz's phone was infected by NSO's Pegasus after he clicked on a link in a fake text message concerning a package Abdaluaziz was expecting, and all of his conversations with Khashoggi were ultimately tracked. *Id.*

11. *France Investigate Tech Firm Accused of Aiding Syria*, REUTERS (July 26, 2012), http://www.reuters.com/article/syria-france-qosmos/france-investigates-tech-firm-accused-of-aiding-syria-idUSL6E8IQN9520120726. Spyware made by Qosmos, a French corporation, was found in Syria.

12. Rishi R. Gupta, *Germany's Support of Assad: Corporate Complicity in the Creation of the Syrian Surveillance State Under the European Convention on Human Rights*, 28 AM. U. INT'L L. REV. 1357, 1359–60 (2013). Spyware produced by Trovicor, a German corporation, was found in Syria. Syrian President "Bashar al-Assad used intrusive surveillance tools [produced by Trovicor] to track individuals' movements, access electronic files, and even detain and torture members of the opposition to Assad's government." *Id.*

13. *Id.* at 1360. *See also* Sarah Lange, *Article: The End of Social Media Revolutions*, 38 FLETCHER F. WORLD AFF., 47, 49–50 (2014).

14. SWISS CONFEDERATION, THE INTERNATIONAL CODE OF CONDUCT FOR PRIVATE SECURITY SERVICE PROVIDERS (Nov. 9, 2010), *available at* https://icoca.ch/sites/all/themes/icoca/assets/icoc_english3.pdf (last visited Jan. 13, 2017).

15. *The ICoCA Overview*, INT'L CODE CONDUCT ASS'N (Feb. 2017), https://www.icoca.ch/sites/default/files/resources/ICoCA-Overview_0.pdf (last visited Jan. 13, 2017).

become accountable stakeholders, forming a shared responsibility regime[16] between a state and non-state actors. This regime will not only oblige state actors to monitor corporate actions to prevent human rights violations, but it will also provide a better possibility of recourse to victims of human rights violations.

Part I of this Note will provide the following background information for contextual purposes: (1) the rise of MNEs as an effect from globalization[17] and the trend toward privatization, and (2) the emerging trend of globalized mass surveillance since the "War on Terror" and increase in cyber torts.[18] Part II of this Note will then focus on the difficulty of finding corporate liability in the current international legal system because of the general inapplicability of human rights laws to non-state actors,[19] like MNEs, and the non-binding obligations of soft law, such as the United Nations Guiding Principles of Business and Human Rights, which have resulted in ineffective remedial measures for human rights violations.[20]

Next, Part III of this Note will examine under what circumstances will wrongful acts of multi-national enterprises be recognized as internationally wrongful acts that fall under the responsibility of the state under international law. Part IV of this Note will then evaluate the newly formed ICoCA, a multi-stakeholder initiative, guided by the principles of the ICoC for Private Security Service Providers. It will evaluate the structure and function of this oversight committee and how it strives to prevent private military service providers from committing human rights violations.

---

16. Jean d'Aspremont et al., *Sharing Responsibility Between Non-State Actors and States in International Law: Introduction*, 62 NETH. INT. L. REV., 49, 49–67 (2015).

17. Yu Makogon & Yu Kinchevskyaya, *Development of Transnational Corporations in the Aspect of Globalization*, 18 VÌSNIK. KIÍVS'KOGO NACÌONAL'NOGO UNÌVERSITETU ÌMENÌ TARASA ŠEVČENKA. EKONOMÌKA 21, 21–24 (2014).

18. Markos Karavias, *Shared Responsibility and Multinational Enterprises*, 62 NETH. INT. L. REV 91, 93 (2015). *See also* Valsamis Mitsilegas, *Surveillance and Digital Privacy in the Transatlantic "War on Terror:" The Case for a Global Privacy Regime*, 47 COLUM. HUM. RTS. L. REV. 1, 2 (2016).

19. MARKOS KARAVIAS, CORPORATE OBLIGATIONS UNDER INTERNATIONAL LAW 19 (2013).

20. Stephen R. Layne, *Corporate Responsibility for Human Rights Violations: Redressability Avenues in the United States and Abroad*, 18 GONZ. J. INT'L L. 1, 13–14, (2015).

Finally, Part V of this Note will evaluate the proposition of making the state an accountable stakeholder by forming a shared responsibility regime[21] between the state and MNEs. This shared responsibility regime will build upon the newly established multi-stakeholder regime of the ICoCA. Similar to the ICoCA, the proposed oversight committee will also consist of representatives from MNEs, civil society groups and states. Through collaboration, the shared responsibility regime will provide better monitoring, reporting and certification practices for corporate entities to follow. Most importantly, the proposed regime will require a more active involvement of states, which will not only oblige state actors to monitor corporate actions to prevent human rights violations, but will also provide a better possibility of recourse to victims of human rights violations.

I. BACKGROUND INFORMATION

This Part will provide contextual information about the emergence of corporations or multinational enterprises in a globalized economy. Many factors, including the advancement of technology, have allowed states and their citizens to transcend territorial boundaries and become more interconnected.[22] This Part will also explore approximately when and how this phenomenon occurred, as well as its consequences, including the incidental increase in the practice of mass surveillance, where states across the world use technological means to not only defend its national security, but to also surveil their own citizens.[23] Mass surveillance walks a fine line between protecting citizens and intruding upon their privacy.[24] The data collected in mass surveillance respects no international boundaries, and "cross-border data collection touches on a bucket of related rights that privacy protections safeguard."[25] This includes the rights to free expression,

21. d'Aspremont et al., *supra* note 16, at 49–67.

22. ILO, A FAIR GLOBALIZATION: CREATING OPPORTUNITIES FOR ALL x (2004). *See also* Jing de Jong-Chen, *Data Sovereignty, Cybersecurity and Challenges for Globalization*, 16 GEO. J. INT'L AFF. 112, 113–14 (2015).

23. Mitsilegas, *supra* note 18, at 3–4.

24. *Id.*

25. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 475–82 (2016).

freedom of conscience and religion, free assembly, free association and other such rights.[26] While it may come as a surprise that corporations from states like France, Germany and Italy have sold intrusive technology to regimes like the Syrian government, such transactions are not uncommon.[27] E-mails were published by WikiLeaks in 2015 of Hacking Team, revealing that the Italian corporation sold its intrusive software to countries including: Ethiopia, Nigeria, South Sudan, Bahrain, Uzbekistan, Azerbaijan, Kazakhstan, Russia, Saudi Arabia and many other governments with authoritarian or one party systems.[28]

A. The Rise of MNEs

MNEs have become a superpower in today's world.[29] Since the beginning of the twenty-first century, the international economy has been altered drastically "by the advance of globalization, sweeping technological changes and the emergence of new and powerful competitors, such as China and India."[30] Globalization is often "understood to mean major increases in worldwide trade and exchanges in an increasingly open, integrated and borderless international economy."[31] It is "a process of interaction and integration among the people, companies and governments of different nations."[32] The process has not only "contributed to a 'denationalization' of economic and social activities," but also an "increase in cross-border capital and international trade," thereby "creating a permissive and protective legal and regulatory environment for MNEs."[33] Additionally, MNEs have been further empowered due to the trend towards privatization, where corporate entities are entrusted by states with the run-

26. *Id.*

27. Gupta, *supra* note 12, at 1360.

28. Cora Currier & Morgan Marquis-Boire, *A Detailed Look at Hacking Team's Emails About its Repressive Clients*, INTERCEPT (July 7, 2015), https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

29. Jed Greer & Kavaljit Singh, *A Brief History of Transnational Corporations*, https://www.globalpolicy.org/empire/47068-a-brief-history-of-transnational-corporations.html (last visited Oct. 20, 2017).

30. Makogon & Kinchevskyaya, *supra* note 17, at 21–24.

31. *Id.*

32. *Id.*

33. Karavias, *supra* note 18, at 93.

ning of hospitals and prisons, the supply of energy and the provision of security services.[34] This trend has "given rise to a retreat of the state from various fields where it traditionally" exclusively regulated, allowing MNEs to enter "reserved state businesses in the public service fields."[35] Furthermore, the retreat of the state raises concerns over whether "such public delegations to private entities occur at the expense of democratic processes . . . and individual justice."[36]

B. Emerging Trend of Mass-Surveillance and Uptick of Human Rights Violations

The right of privacy is explicitly or implicitly present in domestic legal systems around the world,[37] but it can also be found in numerous international human rights instruments, including the United Nations Declaration of Human Rights,[38] International Convention on Civil and Political Rights,[39] European Charter on Human Rights[40] and European Union Charter of

34. *Id.*

35. KARAVIAS, *supra* note 19, at 2.

36. *Id.*

37. *What Do Constitutional Privacy Protections Look Like Around the World?*, PRIVACY INT'L, https://privacyinternational.org/blog/1198/what-do-constitutional-privacy-protections-look-around-world (last visited Jan. 30, 2019).

38. G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UDHR]. Article 12 of the UDHR states: "No one shall be subjected to arbitrary interference with his privacy, family home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.* art. 12.

39. International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]. Article 17(1) of the ICCPR states: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks." *Id.* art. 17(1).

40. European Convention on Human Rights, Nov. 4, 1950, E.T.S. 5 [hereinafter ECHR]. Article 8 of the ECHR Right to respect for private and family life:

> (1) Everyone has the right of respect for his private and family life, his home and his correspondence, (2) there shall be no interference by a public authority with the exercise of this right except when in accordance with the law and when it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection

Fundamental Rights.[41] Technological advancements may have significantly improved economies around the globe, but they have also made it significantly more difficult for the right of privacy to be respected and upheld.[42] Additionally, the War on Terror and the growing trend toward the privatization of policing and security has led to the intensification of surveillance, where "surveillance is [globalized and] both quantitatively (in terms of volume of personal data accessed by the state) and qualitatively (in terms of how and why such data is processed and analyzed) different from traditional policing models that focus on the detection of criminality."[43] The United States National Security Agency's surveillance program, Prism, which was uncovered to the world by ex-Central Intelligence Agency analyst Edward Snowden in 2013, consisted of warrantless and limitless surveillance of U.S. citizens and Internet users all around the world.[44] Beyond using such technological capabilities for policing, it "can also provide authoritarian states with advanced surveillance capabilities and help governments crush democratic movements before they can get off the ground."[45]

In a world where "data no longer respects international boundaries," mass surveillance not only "touches on the right of privacy, but it also touches on related rights that privacy protections safeguard, such as the rights to free expression, free assembly, free association," and many other liberties.[46] It is especially disconcerting that collected data may be used to "stifle such rights" by using it "to identify targets for arbitrary arrests . . . or, even worse, to torture or kill."[47] Thus, unsurprisingly,

---

> of health, or morals, or for the protection of the rights and freedoms of others.

Id. art. 8.

41. Charter of Fundamental Rights of the European Union, Oct. 26, 2012, 2012 O.J. (C 326). Article 8(1), which addresses the protection of personal data, states, "Everyone has the right to the protection of personal data concerning him or her." *Id.* art. 8(1).

42. de Jong-Chen, *supra* note 22, at 114.

43. Mitsilegas, *supra* note 18, at 2.

44. *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964. *See also* Anja Mihr, *Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach*, 15 GEO. J. INT'L AFF. 24, 28 (2014).

45. Gupta, *supra* note 12, at 135–60.

46. Daskal, *supra* note 25, at 475–82.

47. *Id.*

stories of detention and torture, aided by cutting-edge Western surveillance technology, are not uncommon for transitioning states that have endured bloody conflicts.[48] For example, after the fall of Muammar Gaddafi's regime in Libya in August 2011, the *Wall Street Journal* gained access to an abandoned security unit in Tripoli, where journalists found posters and English-language training manuals stamped with the name of the French corporation, Amesys, along with "dossiers of Libyans' online activities lined up in floor to ceiling filing shelves."[49] The dossiers consisted of intercepted messages printed straight from Amesys' "Eagle System," all featuring the designation "https://eagle/interceptions" at the upper right corner of each page.[50] Since then, five individuals have filed a claim against Amesys in France's newly created Crimes against Humanity and War Crimes Unit of the Paris High Court.[51] Each of these individuals has testified that he or she was arbitrarily arrested, detained in prison, tortured, and interrogated about e-mail exchanges, chat messages or social media postings obtained by the Libyan police force between January and February 2011.[52] According to engineers at the Libyan Internet Provider, Amesys' Eagle System became fully operational after "two high-bandwidth 'mirrors' were installed—one on the country's main fiber-optic trunk and one inside the DSL switchboard—to copy all Internet traffic and feed

48. *Id.*

49. Paul Sonne & Margaret Coker, *Firms Aided Libyan Spies First Look Inside Security Unit Shows How Citizens Were Tracked*, WALL STREET J. (Aug. 30, 2011), https://www.wsj.com/articles/SB10001424053111904199404576538721260166388. *See also* Margaret Coker & Paul Sonne, *Life Under the Gaze of Gadhafi's Spies*, WALL STREET J. (Dec. 14, 2011), https://www.wsj.com/articles/SB10001424052970203764804577056230832805896 [hereinafter Coker & Sonne, *Life Under the Gaze of Gadhafi's Spies*].

50. Coker & Sonne, *Life Under the Gaze of Gadhafi's Spies*, *supra* note 49.

51. FIDH, *supra* note 8.

52. *Id.* Paris' High Court has yet to adjudicate this case. *Id.* So far, the Court has opened an investigation into Amesys, and "placed Amesys under the status of témoin assisté (assisted witness) for complicity in acts of torture committed in Libya," an identifier unique to French law that "lies somewhere between being a simple witness and being indicted for a crime." Erin Gifford, *Nexa Investigated for Sale of Surveillance Equipment Linked to Egypt Abuses*, CORPWATCH, https://corpwatch.org/article/nexa-investigated-sale-surveillance-equipment-linked-egypt-abuses (last visited Dec. 2, 2018).

it into the Eagle System."[53] The system had the capability of intercepting online and offline exchanges, allowing users to observe network traffic and peek into people's e-mails, while storing all the communications from the monitored link.[54] Thus, the system was able to detect and store the correspondence so that users can easily search in real time keywords, email addresses or names to identify suspects.[55]

II. CORPORATE LIABILITY UNDER CURRENT INTERNATIONAL LAW

This Part will examine the difficulty of finding MNEs liable under current international law. First, international law and, more specifically, international human rights law only imposes legal obligations to states and state actors.[56] Second, soft law, such as the United Nations Guiding Principles of Business and Human Rights, is simply a recommendation or guidance of due diligence and best practices and, therefore, lacks any obligation or binding force.[57] Third, the combination of the inapplicability of hard law and reliance on soft law has resulted in the insufficiency of remedial measures for human rights violations.[58]

A. International Human Rights Law Primarily Governs States or State Actors—Not Private Individuals or Private Corporations

Under the "dominant view in international law theory" international law addresses states and their governments, identifying them as primary actors.[59] Thus, international law only imposes duties on states (or state officials), and only they can incur

53. Matthieu Aikins, *Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network*, WIRED (May 28, 2012), https://www.wired.com/2012/05/ff_libya/.

54. *Id.*

55. *Id.*

56. KARAVIAS, *supra* note 19, at 19. *See also* Carlos M. Vazquez, *Direct v. Indirect Obligations of Corporations Under International Law*, 43 COLUM. J. TRASNAT'L L. 927, 932–33, (2005).

57. Adam McBeth & Justine Nolan, *The International Protection and Human Rights and Fundamental Freedoms*, *in* INTERNATIONAL CORPORATE LEGAL RESPONSIBILITY 247 (Stephen Tully ed., 2012).

58. SIMON BAUGHEN, HUMAN RIGHTS AND CORPORATE WRONGS CLOSING THE GOVERNANCE GAP 251–56 (Janet Dine ed., 2015).

59. KARAVIAS, *supra* note 19, at 10. The dominant approach in international relations theory is realism, which identifies states as the primary actors in the

liability for the breach of such obligations.[60] Following the end of World War II, "international law shifted beyond regulation . . . of states to incorporate a body of rules concerned with the substantive interests of individuals" with a primary concern for the relationship "between a state [government] and its nationals."[61] Therefore, international human rights law traditionally intended "to safeguard the rights and freedoms of individuals against arbitrary state actions"—not against the actions of other private individuals or entities, including corporations.[62]

Instead, "international law today addresses the conduct of private corporations indirectly, by requiring states to enact and enforce regulations applicable to corporations," and "only a small number of international legal norms, [usually jus cogens], apply directly to non-state actors."[63] Thus, very few human rights norms are directly applied to non-state actors, including MNEs, under the "classic model" of international law.[64] For example, the International Law Commission's (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts ("Draft Articles") is only applicable to a private corporate entity if its "conduct . . . is attributed to the state [through] a requisite link between the corporation and the state."[65] Moreover, "public international law has not fully adapted to the new reality" of post-globalization, so "international obligations remain incumbent on states rather than on non-state actors, such as corporations," despite the fact that "[non-state actors'] adverse effects on human rights have dramatically increased."[66] Thus, there is "no international mechanism [that] exists under which corporations can

---

international system, whereas the minority theory, liberalism, identifies individual and groups as primary actors with states representing them as agents within the international system. *See* Anna-Marie Slaughter, *Liberal International Relations Theory and International Economic Law*, 10 AM. U. J. INT'L L & POL'Y, 717, 721–28 (1995).

60. Vazquez, *supra* note 56, at 932–33. "The primary rules of international law are addressed to states . . . , and under the secondary rules of international law only states incur responsibility for breaching the primary rules of international law." *Id.*

61. KARAVIAS, *supra* note 19, at 19.

62. *Id.* at 19–21.

63. Vazquez, *supra* note 56, at 927.

64. *Id.*

65. Karavias, *supra* note 18, at 96.

66. Cedric Ryngaert, *Transnational Private Regulation and Human Rights: The Limitations of Stateless Law and the Re-Entry of the State*, *in* HUMAN

be held directly liable for breaches of customary or conventional international law, including human rights law, [and] the only available recourse is through domestic jurisdictions."[67]

B. The Introduction of Soft Law—United Nations Guiding Principles of Business and Human Rights, Encouraging Businesses to Respect Human Rights through Due Diligence

The United Nations and other non-governmental organizations (NGOs) have largely avoided creating international legal obligations on corporations, opting instead for a voluntary approach where businesses are encouraged to respect and protect human rights.[68] In 1999, the United Nations Global Compact initiative was officially launched, calling upon diverse groups of businesses to voluntarily join as members to support and respect the protection of international human rights and ensure their company practices are not complicit in human rights abuses.[69] While as many as 4,858 companies were members of the Compact by 2011, critics have noted that many corporations joined the Compact purely for publicity purposes and to "pacify stakeholders."[70] In 2003, the United Nations Sub-Commission on the Promotion and Protection of Human Rights promulgated the Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights (Norms), which "explicitly asserted the obligation of MNEs to promote, secure and ensure the respect and protection of human rights."[71] The Norms, however, were also non-binding on MNEs; instead, the "primary responsibility" of ensuring MNEs and other business enterprises to "respect human rights" was designated to the states.[72] Moreover, the United Nations Commission

---

RIGHTS AND BUSINESS: DIRECT CORPORATE ACCOUNTABILITY FOR HUMAN RIGHTS 99, 99 (Jernej Letnar Cernic & Tara Van Ho eds., 2015).

67. Humberto Fernando Cantu Rivera, *Business & Human Rights: From a "Responsibility to Respect" to Legal Obligations and Enforcement*, *in* HUMAN RIGHTS AND BUSINESS: DIRECT CORPORATE ACCOUNTABILITY FOR HUMAN RIGHTS 303, 322 (Jernej Letnar Cernic & Tara Van Ho eds., 2015).

68. Layne, *supra* note 20, at 7–8.

69. *Id. See also* BAUGHEN, *supra* note 58, at 212–13.

70. Layne, *supra* note 20, at 8.

71. *Id.* at 7–8.

72. *Id. See also* Sub-Commission on the Promotion and Protection of Human Rights, Economic, Social and Cultural Rights: Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to

on Human Rights did not approve the Norms and found that they had no legal standing in April 2004.[73] Finally, in 2011, the Guiding Principles of Business and Human Rights "was unanimously endorsed by United Nation's Human Rights Council . . . as the first global standard for preventing and addressing the risk of adverse impacts on human rights linked to business activity."[74] The Guiding Principles framework is centered around three pillars:

> (1) state duties to protect against third party human rights violations through appropriate policies and regulation; (2) corporate responsibility to respect human rights through the exercise of due diligence, including human rights impact assessments, tracking and monitoring and other measures; and (3) access by victims of human rights abuses to effective remedies, both judicial and non-judicial.[75]

The Guiding Principles, however, do not set forth any new legal obligations that have not already been formerly established. Principle 1 indicates that "states must protect against human rights abuses within their territory by third parties, including business enterprises, through effective legislation, regulation and adjudication."[76] States have a duty to protect a standard of conduct, they must promote the rule of law in ensuring human rights protection, and are responsible for human rights abuse by private actors if the breach can be attributed to them or where they fail to take appropriate steps to prevent, investigate, punish and redress private actors' abuse.[77] According to Principle 4, "states should take additional steps to protect against human rights abuses by business enterprises owned or controlled by the

---

Human Rights, U.N. Doc. E/CN.4/Sub.2/2003/12/Rev.2 (Aug. 26, 2003), *available at* http://www.refworld.org/docid/403f46ec4.html.

73. Comm. on Human Rights, Rep. on the Sixtieth Session, U.N. Doc. E/2004/23 E/CN.4/2004/127, at 333 (2004), *available at* http://www.refworld.org/pdfid/4267b3644.pdf.

74. Cantu Rivera, *supra* note 67, at 307–09.

75. Layne, *supra* note 20, at 8 (citing John Ruggie (Special Representative of the Secretary General), *Business and Human Rights: Mapping International Standards of Responsibility and Accountability for Corporate Acts*, U.N. Doc. A/HRC/4/35 (Feb. 19, 2007)).

76. U.N. Office of the High Comm'r of Human Rights [OHCHR], Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, U.N. Doc. HR/PUB/11/04, at princ. 1 (2011) [hereinafter Guiding Principles].

77. *Id.*

state, or that receive substantial support and services from state agencies."[78] Principle 5 specifies that "states do not relinquish its obligations when they privatize the delivery of services to businesses that may impact upon human rights."[79] All of these legal obligations have been formerly established by the Draft Articles, which will be closely analyzed in Part III of this note.

On the other hand, Principle 11 stipulates that "business enterprises should respect human rights, avoid infringing on human rights of others and address adverse human rights impacts,"[80] including "taking adequate measures for their prevention, mitigation and where appropriate, remediation."[81] Some due diligence operational mechanisms proposed by the Guiding Principles include adopting a publicly available statement of commitment towards human rights,[82] adapting a risk management system to mitigate actual impacts,[83] and tracking of the

78. *Id.* princ. 4.
79. *Id.* princ. 5.
80. *Id.* princ. 11.
81. *Id.*
82. *Id.* princ. 16. Principle 16 Policy Commitment states

> As the basis for embedding their responsibility to respect human rights, business enterprises should express their commitment to meet this responsibility through a statement of policy that: (a) is approved at the most senior level of the business enterprise, (b) is informed by relevant internal and/or external expertise, (c) stipulates the enterprise's human rights expectations of personnel, business partners and other parties directly linked to its operations, products or services, (d) is publicly available and communicated internally and externally to all personnel, business partners and other relevant parties, (e) is reflected in operational policies and procedures necessary to embed it throughout the business enterprise.

Id.

83. *Id.* princ. 17. Principle 17, Human Rights and Due Diligence, states "In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprise should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. . . ." *Id.*

implementation of the Guiding Principles' human rights policies.[84] Thus, while the Guiding Principles have admirably brought attention to the commitment businesses should have towards protecting human rights, the framework remains a solely voluntaristic system, without power to compel businesses to be legally obligated to do so.[85]

Some scholars have reasoned the Guiding Principles have triggered a new "transnational private regulation" (TPR), where MNEs essentially monitor themselves, but the effectiveness of a TPR can vary.[86] For example, due to the divergence of interests between MNEs and civil society, when "social goals are extraneous to profit-driven business venture[s]," MNEs may not have an incentive to follow a TPR "unless there is a clear business case for it."[87] While a business case might be created by consumer pressure, "such substantial consumer pressure will more likely materialize with firms with a larger market share, firms focusing on higher consumer market segments and firms focusing more on manufacturing and design than on sale of products."[88] Finally, support for TPR is more likely to occur in countries with institutions that promote corporate social responsibility—"typically, liberal-democratic western countries"—and "if such conditions are not present, a TPR will not thrive."[89] In other words, "support for a TPR is a function of consumer and institutional pressure," but without such a foundation, "MNEs will [unlikely] make strong human rights commitments through a TPR and limit themselves to blanket statements [with no] genuine desire to change business policies."[90]

84. *Id.* princ. 20. Principle 20 defines what tracking consist of: "In order to verify adverse human rights impacts are being addressed, business enterprises should track the effectiveness of their response. Tracking should: (a) be based on appropriate qualitative and quantitative indicators, and (b) draw on feedback from internal and external sources, including affected stakeholders." *Id.*

85. Layne, *supra* note 20, at 8.

86. Ryngaert, *supra* note 66, at 99–101.

87. *Id.* at 107.

88. *Id.*

89. *Id.* at 108.

90. *Id.*

C. Insufficiency of Current Judicial and Non-Judicial Remedies for Human Rights Violations in Finding Corporate Liability

The "state-centric focus of international human rights law has created a number of problems for lawyers trying to hold businesses accountable for human rights abuses," as businesses are neither subjects of treaty obligations,[91] nor are they primary actors under international law.[92] Victims of businesses seeking redress in their home country's judicial system face extensive obstacles.[93] For example, the Alien Tort Statute (ATS) was previously described as "the main engine for transnational human rights litigations in the U.S.," but the United States Supreme Court's decision in *Kiobel v. Royal Dutch Petroleum Co.*[94] reduced its utility by ruling that the presumption against extraterritoriality, which normally applies to U.S. domestic legislation, must be applied to the ATS.[95] Thus, the ATS could no longer be brought in holding MNEs accountable for human rights abuses.[96] Even when a cause of action is available within the national legal system, a host of other issues can make seeking remedies in the national legal system less attractive; for example, the principle that corporations maintain a separate legal personality may make it difficult to hold parent companies responsible for actions of their subsidiaries because each is a separate legal entity.[97] Additionally, legal systems like the United States, where the doctrine forum non conveniens is applicable, may prevent a case from moving forward when another jurisdiction is more suitable or appropriate, such as the location where the alleged tort took place.[98] Given the possible locations of cyber torts

---

91. Stuart Wallace, *Private Security Companies and Human Rights: Are Non-Judicial Remedies Effective*, 35 B.U. INT'L L.J. 69, 71 (2017).

92. David Bilchitz, *Corporations and the Limits of State-Based Models for Protecting Fundamental Rights in International Law*, 21 IND. J. GLOBAL LEGAL STUD. 143, 146 (2016).

93. Wallace, *supra* note 91, at 72.

94. *Id.* In *Kiobel v. Royal Dutch Petroleum Co.*, Kiobel (plaintiff) brought suit against Royal Dutch Petroleum—a Dutch corporation—among other British and Nigerian corporations under the ATS, alleging the corporations aided and abetted Nigerian military in violating the human rights of Nigerian nationals. Karavias, *supra* note 18, at 106. *See also* Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108, 115–19 (2013).

95. Wallace, *supra* note 91, at 72.

96. *Id.*

97. *Id.* at 73.

98. *Id.* The doctrine of forum non conveniens is:

like the ones alleged by the Libyan plaintiffs in the case against Amesys, there may be an accountability gap if forum non conveniens is applied and a more appropriate country for the case is determined to be a country with a weak judicial system but not weak enough that would cause injustice to the plaintiff.

While London solicitors like Leigh Day have taken on a number of cases involving human rights abuses by MNEs occurring in developing countries, there are similar hurdles to surmount in bringing such claims before the courts of the UK.[99] Specifically, there is the need to: (1) establish jurisdiction, which means the defendant corporation must be domiciled in the United Kingdom; (2) find a way around the separate corporate personality of the English parent company and its foreign subsidiary; (3) establish the applicable law governing the tort claim; and (4) fund the litigation.[100] Thus, while the British courts may be a possible forum if the defendant corporation is incorporated or domiciled in the United Kingdom, this still leaves a significant amount of MNEs that will not be subjected to the same accountability and potential plaintiffs without access to judicial remedy.

The Guiding Principles demand that non-judicial grievance mechanisms be (1) legitimate by "enabling trust from the stakeholder groups for whom they are intended"; (2) accessible and "known to all stockholder groups for whom they are intended"; (3) predictable with "a clear and known procedure" and "means of monitoring implementation"; (4) equitable; and (5) transparent.[101] Non-judicial grievance mechanisms that mirror the Guiding Principles, such as the Organization for Economic Coopera-

---

> A discretionary power that allows courts to dismiss a case where another court, or forum, is much better suited to hear the case. A court will not grant a forum non conveniens dismissal if there is no other forum that could hear the case, or if the other forum would not award the plaintiff any money even if he or she won. Similarly, courts will not grant a forum non conveniens dismissal where the alternative forum's judicial system is grossly inadequate.

Forum non Conveniens, LEGAL INFO. INST., www.law.cornell.edu/wex/forum_non_conveniens (last visited Jan. 30, 2019).

99. BAUGHEN, *supra* note 58, at 172.

100. *Id.*

101. Guiding Principles, *supra* note 76, princ. 31.

tion and Development (OECD) Guidelines for Multinational Enterprises, require countries who voluntarily join the OECD to establish National Contact Points (NCPs) where victims may file complaints about the operation of MNEs.[102] Similar to the Guiding Principles, the OECD Guidelines are voluntary and not legally enforceable, and the practice of NCPs varies within each country; thus, a country may either take a passive stance on the complaint or adopt a more proactive role.[103]

For example, Privacy International, the European Center for Constitutional and Human Rights, and two other Bahraini NGOs filed an OECD complaint at the British NCP and German NCP alleging Gamma International and Trovicor GmbH produced and sold surveillance technology and provided technological support to Bahrain, and therefore, shared responsibility for the arrests, imprisonment and torture of opposition members, journalists and dissidents in Bahrain.[104] The German NCP rejected the complaint, finding it not substantial enough to warrant further scrutiny, whereas, the British NCP proceeded with an investigatory review.[105] The British NCP, however, was only able to find Gamma International lacked a due diligence process and a publicly available statement of commitment to human rights because the NCP lacked the investigatory powers, such as the ability to compel documents or disclosure, to confirm the specific accusation alleged on the complaint.[106] Thus, even non-judicial remedies, such as the grievance mechanism available through the OECD Guidelines, may not be sufficient avenues for remedies under Principle 31 of the Guiding Principles.[107]

III. ANALYSIS OF CIRCUMSTANCES WHERE MNES' ACTIONS WILL BE ATTRIBUTABLE TO THE STATE AS INTERNATIONALLY WRONGFUL ACTS FOR LEGAL OBLIGATIONS TO ARISE: WHEN IS

102. *About the OECD Guidelines for Multinational Enterprises*, OECD, http://mneguidelines.oecd.org/about.htm (last visited Oct. 21, 2017). *See also* BAUGHEN, *supra* note 58, at 217–18.

103. *Id.*

104. *UK Rebukes German-British Software Company Gamma*, EUR. CENTER CONST. & HUM. RTS., https://www.ecchr.eu/en/our_work/business-and-human-rights/surveillance-technology.html (last visited Oct. 21, 2017).

105. *Id.*

106. *Id.*

107. *See* BAUGHEN, *supra* note 58, at 251–56.

THERE AN ATTRIBUTABLE NEXUS BETWEEN THE STATE AND PRIVATE CORPORATION?

This Part will address when and how MNEs' actions will be attributable to a state for legal obligations to arise under international law. Section A will take a close examination of relevant articles under the ILC's Draft Articles to better understand when state liability will arise for human rights violations. Section B will examine the circumstances where corporate action may be attributable to a state under the Draft Articles, including when the actions of state-owned enterprises (SOE) may be attributable to a state to incur liability under international law.

A. A Close Evaluation of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts

The ILC spent over half a century to develop the Draft Articles with the intention of developing the "law of state responsibility" via observations of state practice and case law as opposed to drafting a full convention or treaty.[108] The Draft Articles sought to codify "the basic rules of international law concerning the responsibility of states for internationally wrongful acts" by laying out the "conditions under international law for when [a state is] to be considered responsible for wrongful actions or omissions and the legal consequences which flow [from] there."[109]

The general rule is that the only conduct attributed to a state at the international level is that of its organs of government, or others who have acted under the "direction, instigation or control of those organs."[110] According to Article 4 of the Draft Articles:

> (1) the conduct of any state organ is considered an act of that state under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the state, and whatever its character as an organ of the central Government or of a territorial unit of the state, and (2) an organ includes any person or

108. Natasha Arnpriester, *Combating Impunity: The Private Military Industry, Human Rights and the Legal Gap*, 38 U. PA. J. INT'L L. 1189, 1229 (2017).

109. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, U.N. Doc. A/56/10, at 31 (Oct. 24, 2001) [hereinafter Wrongful Acts].

110. *Id.* art. 4.

> entity which has the status in accordance with the internal law of the state.[111]

Despite these rules, "there exists a range of situations where non-state actors can possibly share responsibility for their contributions to harmful outcomes."[112]

According to Article 5, which is titled "Conduct of persons or entities exercising elements of governmental authority,"

> The conduct of a person or entity which is not an organ of the state under Article 4, but which is empowered by the law of that state to exercise elements of the governmental authority, is considered an act of the state under international law, provided the person or entity is acting in that capacity in the particular instance.[113]

This article addresses the "increasingly common phenomenon of parastatal entities, which exercise elements of governmental authority in place of state organs, as well as situations where former state corporations have been privatized but retain certain public or regulatory functions."[114]

Under Article 8, "the conduct of a person or group of persons shall be considered an act of the state under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."[115] In such instances the test is "whether their conduct involve governmental activity."[116] This commonly occurs when "state organs supplement their action" by employment of private entities who act "as auxiliaries while remaining outside the official structure of the state."[117] Furthermore, according to Article 7 of the Draft Articles, under the circumstances where the individual or entity authorized to conduct governmental activity "exceeds its authority or contravenes its given instruction," the action is considered to be an act of the state under international law.[118]

---

111. *Id.*
112. d'Aspremont et al., *supra* note 16, at 49–67.
113. Wrongful Acts, *supra* note 109, art. 5.
114. *Id.* cmt. 1.
115. *Id.* art. 8.
116. *Id.* cmt. 1–2.
117. *Id.*
118. *Id.* art. 7. The Draft Articles does, however, distinguish "cases where officials acted in their capacity, as such albeit unlawfully or contrary to instruc-

B. When Are the Actions of an MNE Attributable to the State? What about the Actions of SOEs?

Examples of when the actions of non-state entities, including MNEs, may be attributed to a state can be found under Article 5 and 8 of the Draft Articles. For example, according to Commentary 2 of Article 5, non-state entities include "public corporations, semi-public entities, and even in special cases, private companies, provided that the entity is empowered by the law of the [s]tate to exercise functions of a public character normally exercised by state organs."[119] This includes "private security firms [contracted] to act as prison guards and in that capacity may exercise public powers, such as powers of detention and discipline pursuant to a judicial sentence or to prison regulations."[120] According to Article 8, Commentary 2, examples of entities operating "under the control or instructions of the state" include those who are "employed as [auxiliary military or volunteers] to neighboring countries to carry out particular missions abroad]" despite not being "part of the state's armed forces."[121]

The conduct of state-owned and controlled enterprises raises its own set of questions and issues.[122] International law recognizes that corporate entities, even state-owned entities, are legally separate from their shareholders under national law, and it will recognize this separateness except in circumstances where "the corporate veil is a mere device for fraud or evasion" of liability.[123] Therefore, just because a corporation is state-owned does not mean the actions of the entity is automatically attributable to the state.[124] Instead, the "conduct [of the state

---

tions, from cases where the conduct is so removed from the scope of their official functions that it should be assimilated to that of private individuals, not attributable to the State." In such circumstances, such conduct should be considered activity "carried out by persons cloaked with governmental authority." *Id.* cmt. 7.

119. *Id.* art. 5, cmt. 8.

120. *Id.*

121. *Id.* art. 8, cmt. 2. Identifying whether the conduct "was carried out under the direction or control of the state" is more complex. There will be attribution to the state "only if [the state] directed or controlled the specific operation and the conduct complained of was an integral part of that operation." Additionally, "the degree of control exercised by the State" over the entity in question is a key issue in the determination of attribution. *Id.* cmt. 3–4.

122. *Id.* cmt. 6.

123. *Id.*

124. *Id.*

owned enterprise] is considered to be separate unless it was exercising elements of governmental authority within the meaning of Article 5."[125] If, however, "there is evidence that the state was using its ownership interest or control of a corporation to achieve a particular result, . . . the conduct in question has been attributed to the state."[126]

IV. A CLOSE EVALUATION OF THE ICOC AND THE ICOCA—AN INNOVATIVE APPROACH IN PREVENTING HUMAN RIGHTS VIOLATIONS BY PRIVATE MILITARY SECURITY CORPORATIONS (PMSCS)

This Part will evaluate the ICoC and ICoCA in detail to better understand how the innovative multi-stakeholder oversight committee, consisting of representatives from corporate entities, civil society groups and state actors, strives to prevent private military security providers from committing human rights violations by better regulation of corporate practices.

Section A briefly discusses the formation of the ICoC for contextual purposes, while Section B discusses the formation of the ICoCA and closely examines the structure, governance and function of the oversight committee—an innovative mechanism with significant potential in the regulation of PMSCs.

A. Formation of the ICoC

Similar to the emerging trend in cyber surveillance, state use of PMSCs has greatly expanded, sparked in large by the United States' reliance on contractors in the wars in Afghanistan and Iraq.[127] Moreover, globalization and the trend toward outsourcing government functions to the private sector has increasingly expanded opportunities for the growth of transactional business

125. *Id.* cmt. 6.

126. *Id.* "In one case before the Iran-United States Claim Tribunal" the tribunal found a state established foundation, which "held property for charitable purposes under close governmental control," was a public and not a private entity, and the foundation's "administration of allegedly appropriated property fell under Article 5." *Id.* art. 5, cmt. 2.

127. Reema Shah, *Beating Blackwater: Using Domestic Legislation to Enforce the International Code of Conduct for Private Military Companies*, 123 YALE L.J. 2259, 2259 (2014).

sectors like private security.[128] The increased rise in PMSCs has also been met with growing controversy over reports of unpunished criminal misconduct and human rights abuses.[129] For example, in the 1990s, DynCorp employees hired to represent the United States contingent in the United Nations Police Task Force in Bosnia were involved in sex trafficking scandals.[130] In September 2007, the United States State Department contracted with the private military firm, Blackwater USA, which provided the contractors that opened fire upon the busy Nisour Square in Baghdad, killing numerous unarmed Iraqi citizens, including young children.[131] In 2004, security contractors employed to be interrogators by CACI International and Titan were involved in the Abu Gharib prison abuses.[132] There are a number of challenging problems, however, with seeking to remedy PMSCs' human rights abuses.[133] The combination of "the limited

---

128. Amol Mehra, *Bridging Accountability Gaps – The Proliferation of Private Military and Security Companies and Ensuring Accountability for Human Rights Violations*, 22 GLOBAL BUS. & DEV. L.J., 323, 323 (2010).

> The use of PMSC in Iraq is illustrative of the complexity stemming from the proliferation of this group of actors. At least 310 private security companies from around the world have received contracts from U.S. agencies to protect American and Iraqi officials, installations, convoys, and other entities in Iraq since 2003. And with more than six years into the conflict in Iraq, there has been no centralized database to account for all the securities companies in Iraq financed by American money. Other democratic countries, such as United Kingdom, for example, has contracted out to PMSCs for training in operation, and maintenance of its nuclear submarines while Australia and Canada have entirely privatized many of their military services, including military recruiting in Australia and electronic warfare in Canada.

Id. at 324.

129. *Id.* at 325.

130. *Id.*

131. Arnpriester, *supra* note 108, at 1192. *See also* Mehra, *supra* note 128, at 325.

132. *Id.* at 325. Reports of the Abu Gharbib incident confirm the prison personnel, half of which was comprised of PMSCS, committed a series of human rights violations, including torture, rape and murder, but none of the PMSCs have been prosecuted despite the conviction of several U.S. military officers. Arnpriester, *supra* note 108, at 1194–95.

133. Wallace, *supra* note 91, at 74.

capacity of the state where PMSCs operat[e] . . . and the absence of the extraterritorial reach of legislation from the states in which the PMSCs are domiciled, generates a bubble of impunity."[134]

Although the United Nations Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of Rights of Peoples to Self-Determination developed a draft International Convention on the Regulation, Oversight and Monitoring of Private Military and Security Companies, states with large private security industries, including the United States and the United Kingdom, opposed the Convention, and there will be significant opposition before it can become law.[135] Instead, a joint initiative between Switzerland and the International Committee of the Red Cross created the Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies ("Montreux Document"), which reiterated states' international legal obligations as they relate to human rights laws and provided "good practices" on the use of PMSCs that were endorsed by several states.[136] Building upon the Montreux Document, the ICoC was finalized in November 2010.[137] Unlike the Montreux Document, however, the ICoC is directed toward PMSCs' obligations and lays out guidelines and international standards on human rights for PMSCs.[138] The ICoC "is the fruit of a multi-stakeholder initiative with the overarching objectives to articulate human rights responsibilities of PMSCs," by establishing a set of principles and standards consistent with international law that PMSCs, especially those

134. *Id.* at 76.

135. *Id.* at 85. The Draft Convention included provisions that restricted the type of activities that can be carried out by PMSCs, and a number of positive obligations (legislative and administrative) upon the states "to ensure PMSCs and their personnel are held accountable for violations of applicable national or international law," including ensuring PMSCs to fulfill proper due diligence requirements. Nigel White, *Due Diligence Obligations Developing a Responsibility Regime for PMSCs*, 31 CRIM. JUST. ETHICS, 233, 252 (2012).

136. Arnpriester, *supra* note 108, at 1223.

137. *Id.* at 1224.

138. *Id.* at 1225. ICoC is the first international regulatory code aimed directly at improving human rights performance of private security providers. Nicola Jagers, *Regulating the Private Security Industry: Connecting the Public and the Private through Transnational Private Regulation*, 6 HUM. RTS & INT'L LEGAL DISCOURSE 56, 67 (2012).

situated in conflict-ridden zones, should comply with.[139] Over the course of an eighteen-month process, private security companies, states, including Australia, United Kingdom and the United States, civil society organizations and academics collaborated to produce "a code of conduct for the private security industry based on international human rights and humanitarian law standards."[140] In 2010, fifty-eight PMSCs signed on; however, by 2013, 708 companies formally committed to operate according to the ICoC's directives.[141]

The ICoC "explicitly applies key principles of human rights to PMSCs, [by filling] in important gaps in international law without the need for a long and laborious treaty-revision process."[142] The ICoC provides detailed obligations requiring "signatory PMSCs to reform particular organizational and procedural practices."[143] For example, PMSCs "agree to prohibit personnel from engaging in sexual exploitation" and "detention unless a government contract specifically allows it, [and even if it is allowed], detainees must be treated in accordance to international law."[144] Moreover, PMSCs "must commit to vet[ting] and train[ing] employees extensively," including checking and ensuring "that all personnel do not lack the character and fitness to perform security services pursuant to the ICoC."[145] The ICoC even "extends these requirements to subcontractors" of the PMSC; thus, signatory PMSCs "must take reasonable and appropriate steps to ensure" the subcontractor's personnel also comply with the principles of the ICoC.[146] The ICoC "is particularly stringent in requiring PMSCs to prepare incident report[s] documenting any incident[s] involving its personnel that involves the use of any weapon" or any "case of torture or . . . cruel treatment," which "must be submitted to the client who contracted the PMSC, and

139. *History*, INT'L CODE CONDUCT ASS'N, https://icoca.ch/en/history (last visited Jan. 13, 2017) [hereinafter ICoCA Website]. "The main purpose of the ICoC is to set forth a commonly agreed set of principles for PMSCs and to establish a foundation to translate those principles into related standards as well as governance and oversight mechanisms." Jagers, *supra* note 138, at 67.

140. ICoCA Website, *supra* note 139.

141. *Id.*

142. Laura Dickinson, *Regulating the Privatized Security Industry: The Promise of Public/Private Governance*, 63 EMORY L.J. 417, 420–21 (2013).

143. *Id.* at 421.

144. *Id.* at 422.

145. *Id.* at 423.

146. *Id.*

other competent authorities."[147] Finally, the ICoC obligates each PMSC "to establish internal grievance procedures for both its employees and third parties to invoke in cases of alleged . . . violations," and such "[p]rocedures must be fair, accessible and offer effective remedies."[148]

B. The Formation of the ICoCA, an Innovative Approach in Regulation with Significant Potential, and a Close Examination of Its Structure and Governance Mechanism

The ICoCA is the oversight committee charged with monitoring the implementation and compliance of the ICoC, consisting of a Board of Directors, a General Assembly (GA), and a Secretariat.[149] The GA appoints the Board of Directors, which consists of "an even distribution of representatives from civil society groups, states and the [PMSC] industry."[150] The Board of Directors "serves as the executive body overseeing the Secretariat." It "report[s] on the implementation of the ICoC, make[s] recommendations to the GA, and develops the ICoCA's operating procedures."[151] The Secretariat "gathers information for compliance reports on the [PMSCs], receive[s] complaints from third parties," and "address[es] specific compliance concerns" with PMSCs.[152]

The ICoCA takes an integrated approach in its governance mechanism. First, its "monitoring function is designed to identify concerns about or barriers to compliance with the ICoC" by collecting information on the participating PMSCs through: "remote monitoring (public source screening) . . . , company self-assessment . . . and field based reviews (monitoring of specific areas of companies performance)."[153] Second, its certification function involves the review of a PMSC's systems and policies to determine if it meets "the principles and standards derived from the ICoC," as well as "the requirements for personnel management and human rights performance."[154] Finally, the ICoCA's "complaints function facilitates access to fair and accessible

147. *Id.* at 424.
148. *Id.*
149. Wallace, *supra* note 91, at 87.
150. *Id.*
151. *Id.*
152. *Id.*
153. *The ICoCA Overview*, *supra* note 15.
154. *Id. See also* Wallace, *supra* note 91, at 87–88.

grievance procedures" for individuals adversely affected by PMSCs.[155] While the ICoC creates a series of procedures by which PMSCs must follow, the ICoCA is "empowered to take steps to support [signatory members] in their obligations under the ICoC."[156] In cases of noncompliance with the ICoC, the ICoCA may impose sanctions, which include suspension or termination of membership or certification.[157] Although noncompliance may not result in civil or criminal liability, the ICoC regime, "has a far more robust compliance and accountability mechanism than many other [existing] voluntary industry-driven codes of conduct." The "ultimate sanction of banishment from the regime, [which] may render firms ineligible to receive lucrative contracts," may serve as an incentive for compliance, "particularly if governments agree to only hire [ICoC] certified contractors."[158] After all, one of the "main reason[s] put forward by PMSCs for joining the ICoC is their competitiveness and reputational concerns . . . in preserving their government contracts, since governments are among their main customers."[159] For example, states like the "United Kingdom and the United States have announced they will require PMSCs to be signatories of the ICoC."[160]

Although the ICoCA was formally launched in September 2013, it is still very much a newly established mechanism, such that "it[s] complaint procedure only went into effect in September 2016, and it [only began] accepting complaints in early 2017."[161] Thus, it is "not yet possible to assess the efficacy of this procedure."[162] While some scholars have already found weaknesses in the ICoCA's proposed mechanism so far,[163] others have

155. *The ICoCA Overview*, *supra* note 15.
156. Dickinson, *supra* note 142, at 452.
157. *Id.* at 453.
158. *Id.*
159. Jagers, *supra* note 138, at 69.
160. *Id.*
161. Arnpriester, *supra* note 108, at 1228.
162. *Id.*
163. According to some scholars, the ICoC has introduced some extremely positive developments but it suffers from some debilitating shortcomings that reduce the effectiveness of the ICoCA's remedial mechanism. Wallace, *supra* note 91, at 97–98. For example, "the requirement that complainants exhaust other avenues of redress [before approaching] ICoCA means [an unlikelihood of] swift remedies . . . and the fact that the ICoC relies so heavily on external

argued for building upon the established ICoCA mechanism to form a "self-regulation-plus" approach, where PMSCs not only adhere to the ICoC and oversight body of the ICoCA, but also abide by the certification and auditing standards adopted by states, which may potentially ensure PMSCs respect and comply with human rights standards.[164] Therefore, "while adherence to the ICoC and membership of the ICoCA appear voluntary in nature, . . . their approach does resemble a form of mixed co-regulation where states, civil society actors, and private actors—in this case, PMSCs—are regulating jointly."[165] There are arguably "elements of meta-regulation where PMSCs must seek 'official validation' . . . [for] governmental contractual arrangements via [approval by the state and by] membership of the ICoCA."[166] Thus, this "self-regulation-plus system may even have the potential to be a positive and sophisticated example of [a hybridized system consisting of both market and social regulation]."[167]

A key factor for the effective enforcement of the ICoC by the ICoCA, a form of TPR, is the extent to which the state actively participates with private regulators.[168] Active state participation should include "incorporating the [ICoC] standards into their public procurement policies or by requiring [its contracting PMSCs] to do so."[169] States must " actively support the development of the emerging certification process to ensure that the system matures effectively and becomes more widely recognized

---

factors, from groups offering certification services to external remedial mechanisms, leaves its effectiveness at the [mercy of third parties.]" *Id.* Furthermore, there is skepticism surrounding the ICoCA's enforcement ability because of its reliance on market forces and its limited capacity in addressing complaints through sanctions. *Id.* Overall, some scholars have found the ICoCA to have "a disproportionate focus on procedural compliance of PMSCs . . . rather than substantive compliance with international human rights law." *Id.* Despite its "great deal of promise," the ICoC may be "far from providing an effective remedy for human rights violations at the hands of PMSCs." *Id. See also* Arnpriester, *supra* note 108, at 1227. *See also* Jagers, *supra* note 138, at 83–84.

164. Sorcha MacLeod, *Private Security Companies and Shared Responsibility: The Turn to Multi-Stakeholder Standard-Setting and Monitoring Through Self-Regulation – 'Plus'*, 62 NETH. INT. L. REV., 119, 122–24 (2015).

165. *Id.* at 123.

166. *Id.* at 124.

167. *Id.*

168. Jagers, *supra* note 138, at 86.

169. *Id.* at 86–87.

and adopted."[170] In doing so, states would demonstrate to the international community that their "due diligence obligations under international human rights law are being met," because "doing anything [less] will be perceived as unsatisfactorily shifting all responsibility for human rights violations onto PMSCs."[171] Thus, the ICoC and ICoCA regulatory mechanism carries potential and "with support of important gatekeepers, such as the United Kingdom and the United States . . . there is potential for 'hardening' of the Norms in the ICoC."[172]

V. PROPOSITION OF A SHARED RESPONSIBILITY REGIME THAT BUILDS UPON THE MULTI-STAKEHOLDER REGULATORY APPROACH USED BY THE ICOC AND ICOCA

Finally, this Part will evaluate the proposition of making states accountable stakeholders by forming a shared responsibility regime[173] between states and MNEs. Section A will summarize why such a shared responsibility regime with strong state participations is needed. Next, Section B will describe how a shared responsibility regime can be formed by building upon the newly established multi-stakeholder approach taken by the ICoC and ICoCA. This Note will also explore how a shared responsibility regime can be transferred to the regulation of the sales of cyber-surveillance spyware by MNEs by building upon the Wassenaar Agreement—the current international arrangement dealing with arm transfers, including the transfers of spyware. The proposed shared responsibility regime will not only oblige state actors to monitor corporate actions to prevent human rights violations, but it will also provide a better possibility of recourse to victims of human rights violations.

A. Why Such a Shared Responsibility Regime with a Strong State Participation is Imperative and Necessary

As the world has become more interconnected, there has been an "increase [in] the likelihood of concerted action," but the current international legal framework does not "address this new

170. MacLeod, *supra* note 164, at 138–39.
171. *Id.*
172. Jagers, *supra* note 138, at 87.
173. d'Aspremont et al., *supra* note 16, at 49–67.

reality."[174] The inapplicability of international laws in light of these "modern international relations" calls for a serious discussion about shared responsibility.[175] It has been proposed that "the international legal system allows for various conceptualizations of the 'shared responsibility' between states and MNEs, which operate in parallel towards closing of the perceived 'accountability gap' associated with the conduct of the MNEs."[176] As previously discussed, the Draft Articles do not turn a blind eye to the operation of MNEs. Instead, some of the rules are actually amenable to corporate conduct that can be attributed to the state should there exist a requisite link between the corporation and the state, potentially generating state responsibility.[177] If a corporation "[acts] on the instruction of, or under the direction or control of the state," its conduct may be attributable to the state.[178] Moreover, "situations of shared responsibility involving non-state actors may exceptionally arise, [under] institutional regimes, where states contract with a non-state actor, such as a corporation, to carry out certain activities."[179] Similar to "the undeniability that state regulation is imperative in the

174. Andrew Nollkaempur, *Shared Responsibility in International Law: A Conceptual Framework*, 42 MICH. J. INT'L L. 359, 436 (2013).

175. *Id.*

176. Karavias, *supra* note 18, at 91.

177. *Id.* at 96–97.

178. *Id.*

179. d'Aspremont et al., *supra* note 16, at 56. For example:

> Under the United Nations Convention on the Law of the Sea (LOSC), corporations can enter into a contract to explore polymetallic nodules and accordingly incur obligations and responsibility under international law, and in its 2011 Advisory Opinion, the Seabed Chamber of the International Tribunal of the Law of the Sea held that joint and several liability arises where different entities have contributed to the same damages so that full reparation can be claimed from all or any of them. While the Chamber may only have referred to responsibility shared between states and international organizations, it is arguable that also corporations, on the basis of the contract, may share responsibility for wrongful acts in breach of the contract, but such a scenario follows the existence of responsibility due to contractual obligations as opposed to international law.

Id.

regulation of PMSCs, given the nature of its activities in conflict-ridden zones and intimate connection to states,"[180] regulation of spyware also requires strong state participation.

B. Transferring the Multi-Stakeholder Approach of the ICoC and ICoCA to Build Upon the Current Export Regulation Regime Found in the Wassenaar Arrangement

"To date, the most notable international agreement dealing with arm transfers, including the transfers of surveillance spyware, is the Wassenaar Arrangement," where forty-one participating states voluntarily agreed "to meet on a regular basis to ensure that transfers of arms and technologies are carried out responsibly and in furtherance of international and regional peace and security."[181] Formed in 1996, the Wassenaar Arrangement "attempts to control the proliferation of dual-use technologies through a variety of mechanisms, including controls on distribution, information-sharing among member states and the notification of transfers or denials of dual-use goods to non-member states."[182] After the discovery of information technologies,

---

180. Jagers, *supra* note 138, at 88.

181. Annyssa Bellal, *Arms Transfers and International Human Rights Law*, *in* WEAPONS UNDER INTERNATIONAL HUMAN RIGHTS LAW 448, 467–68 (Stuart Casey-Maslen ed., 2014).

182. Jamil Jaffer, *Strengthening the Wassenaar Export Control Regime*, 3 CHI. J. INT'L L. 519, 520 (2002). The Wassenaar Arrangement formed in 1996 had four primary goals:

> (1) members sought to promote transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies; (2) members aspired to use domestic policies to ensure that transfers of conventional arms and dual-use goods and technologies would not contribute to the development of military capabilities; (3) members wanted to complement and reinforce the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognized measures designed to promote transparency and great responsibility; and (4) members were interested in enhancing cooperation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses if the situation in a region or the behavior of a state is, or becomes, a cause of serious concern.

Innokenty Pyetranker, *An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement*, 13 NW. J. TECH. &

from French-based Amesys in the surveillance systems of former Prime Minister Muammar Gadhafi's regime in Libya, the participating states all unanimously agreed to adopt amendments to the Wassenaar List of Dual Use Goods and Technologies in December 2013.[183] Additionally, the participating states reaffirmed their commitment to "maintain effective export controls [of arms and technologies] on the agreed list" and ensure their national policies "do not undermine international and regional security."[184] Furthermore, the participating states agreed to continue periodically reviewing the agreed list to "take into account technological developments" and continue their exchange of information, including a report of any export denials.[185]

Each participating state remains the sole arbiter of the approval or denial of export licenses, "thereby mitigating [the] potential efficacy" of the Wassenaar Arrangement.[186] While some states have legislated, at both regional and national levels, laws in compliance to the Wassenaar Arrangement, many states still

---

INTELL. PROP. 153, 161 (2015). Thus, the members "committed to sharing information, controlling the distribution of items on the munitions and dual-use lists, and notifying one another of transfers and denials of listed items to non-members." *Id.*

183. Roszel Thomsen & Philip Thomsen, *Export Controls on Intrusion and Surveillance Items: Noble Sentiments Meet the Law of Unintended Consequences*, 19 J. INTERNET L. 22, 22–23 (Sept. 2015).

> The 2013 amendments manifested in a number of changes to the Wassenaar Arrangement's control list of dual-use goods and technologies; two changes was the addition of a category which mandates export controls on certain forms of software and associated goods, specifically IP network communications surveillance systems and an addition of a category which mandates export controls of "intrusion software"—software specially designed or modified to avoid detection by monitoring tools, performing any of the following: (a) extraction of data or information, from a computer or network-capable device or (b) modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Pyetranker, *supra* note 182, at 163.

184. *What is the Wassaneer Arrangement?*, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/the-wassenaar-arrangement/ (last visited Nov. 12, 2017).

185. *Id.*

186. Bellal, *supra* note 181, at 468.

continue to "have no legislation at all to prohibit or even limit transfers where weapons are likely to be used to violate human rights."[187] Because "the issuance of export licenses is at the national discretion of each participating state and based on states' unique perspectives and interests, . . . implementation of the multilateral effort to effectively control the acquisition of [dual-use goods] by governments with questionable human rights records" has been inconsistent.[188] While the efficacy of the Wassenaar Arrangement is currently subpar, it does illustrate a possible entry point for other stakeholders, such as state actors and civil society groups, to partake in an otherwise private transaction. Similar to the need to build upon the ICoCA's approach, more active state participation will be very important. Otherwise, the MNE selling the spyware would only be attributable to a state actor if the MNE happens to be a SOE or is under the control or direction of the state.

This Note proposes the development of a code analogous to the ICoC by building upon the export regulating mechanisms proposed in the Wassenaar Arrangement, including controls on distribution, information-sharing, notification of transfers or denials of dual-use goods and other relevant procedures, to better prevent human rights violations. Additionally, an oversight committee similar to the multi-stakeholder structure of ICoCA, consisting of equal representatives from civil society groups (i.e. Amnesty International), MNEs that produce and sell spyware and state actors that approve the exportation of goods (i.e. the United States Commerce Department's Bureau of Industry and Security), should be created to form a shared responsibility regime between state actors and non-state actors. Like the ICoCA, the oversight committee would review the MNEs corporate systems, policies and personnel management to determine if they meet the principles and standards derived by the newly developed code for membership and exportation of dual-use goods. Moreover, the oversight committee would monitor for non-compliance and address complaints of human rights violations to support MNE members in performing their obligations under the code. If MNEs are found in non-compliance, the oversight committee would have the power to issue sanctions or revoke membership.

---

187. *Id.* at 471.

188. Thomsen & Thomsen, *supra* note 183, at 23.

While the addition of civil society groups in this multi-stakeholder approach may encourage more transparency compared to the previous arrangement, where each state had its discretion in approving or denying the exportation of an MNE's dual-use product, the most important part of the shared responsibility regime remains the need for active participation of states and national legislation to correspond to the proposed code. First, the state's national legislation should reflect the export controls agreed upon by the ICoC. Similar to the PMSCs' membership in ICoCA, MNEs' membership in the proposed regime and their compliance to the code would affect their reputation in the cyber surveillance industry, as well as their lucrative opportunities of exporting their products in contractual sales. Moreover, a state's approval and issuance of export licenses for an MNE's sales of dual-use goods would depend on the MNE's membership and compliance to the proposed Code and regime. Under this proposed regime, if the oversight committee fails to take action against an MNE that does not comply to the proposed code, the victim would be able to file a grievance with the proposed oversight committee and bring a civil claim against the state for a human rights violation attributable to the state.

CONCLUSION

The use of cyber surveillance spyware has not only resulted in the invasion of privacy of numerous citizens, but also a plethora of other human rights violations ranging from arbitrary detention, torture and even death.[189] The five cases filed against the French corporation, Amesys, in Paris High Court's Crimes against Humanity and War Crimes Unit, are just a few of the many examples of such human rights violations.[190] Unfortunately, international law and, more specifically, international human rights law only imposes legal obligations to states and state actors.[191] Soft law, such as the United Nations Guiding Principles of Business and Human Rights, may have admirably brought attention to the commitment businesses should have towards protecting human rights, but the Guidelines remain solely voluntary without power to legally obligate businesses to

189. Gupta, *supra* note 12, at 1359–60.
190. FIDH, *supra* note 8.
191. KARAVIAS, *supra* note 19, at 19.

comply.[192] Thus, the state-centric focus of international human rights law has created a number of problems for lawyers trying to hold corporations judicially accountable for human rights abuses,[193] and the non-judicial grievance mechanisms relying on soft law have resulted in the insufficiency of remedial measures for human rights violations.[194] While the current international legal framework does not turn a blind eye to the operation of private corporations, legal obligations will arise only if private corporate conduct can be attributed to the state.[195] Thus, a shared responsibility regime, where the state becomes an accountable stakeholder, must be developed.[196] It will not only obligate state actors to better monitor corporate actions to prevent human rights violations, but will also provide a better possibility of recourse to victims of human rights violations.

Anna W. Chan[*]

192. Layne, *supra* note 20, at 13–14.
193. Wallace, *supra* note 91, at 71.
194. BAUGHEN, *supra* note 58, at 251.
195. Karavias, *supra* note 18, at 96–97.
196. d'Aspremont et al., *supra* note 16, at 49–67.

* B.A., New York University (2008); J.D., Brooklyn Law School (2019); Associate Managing Editor, *Brooklyn Journal of International Law*. Many thanks to the staff of the *Brooklyn Journal of International Law* for their help and support in the publication of this Note. A special thank you to George Somi and Wynee Ngo for their patience in the editing process. Thanks to my family and friends for understanding my continual rainchecks for the last three years. And lastly, thank you to my partner, Philip Sanchez, for his continual support, encouragement and always being an amazing dog dad, we survived law school together. All errors or omissions are my own.