# Let's keep this between you, me, and my cell phone: Huawei, Espionage, & International Law

*By Anya Hovanic†*



## I. Introduction

Depending on where you live, the name "Huawei" may not be as recognizable as "Samsung."[1] However, as the second-largest manufacturer of smartphones in the world,[2] the Chinese telecommunications giant Huawei is steadily becoming a household name across the globe. These days the international behemoth

---

† J.D. Candidate, 2023, University of North Carolina School of Law; Circulation Editor, North Carolina Journal of International Law, 2022/23; Captain, United States, Air Force Reserve; USCG-licensed Third Mate, Unlimited Tonnage.

1 *See generally*, Sherisse Pham, *Samsung Slump Makes Huawei the World's Biggest Smartphone Brand for the First Time, Report Says*, CNN BUS. (Jul. 30, 2020, 3:11 AM ET), https://www.cnn.com/2020/07/30/tech/huawei-samsung-q2-hnk-intl/index.html [https://perma.cc/ZHS5-A4WN] (noting that Huawei sells "over 70% of its smartphones" in China, while Samsung "has a very small presence" there).

2 In 2020, Huawei briefly surpassed Samsung as "the world's top smartphone seller" in quarterly sales. *Id*.

constantly lurks in news media, Huawei's name surfaces during coverage on the company's lengthy history of legal disputes,[3] during marketing announcements such as the debut of virtual assistant "Lysa,"[4] or amidst accusations of developing AI software to identify a specific ethnic group in China in aid of the Chinese government.[5]

Since 2013, Huawei has been the rumored bogeyman behind numerous data breaches, leading to the accusation of using their smartphone and cellular technology as a means of surveillance by the Chinese government.[6] As of yet, punishments levied against Huawei for its offenses have been strictly limited to national action.[7] Despite the sanctions and legal action, the company shows no indication of reformation and as the list of allegations continue, these actions and suspected illegal conduct amount to a culture of spying known as economic espionage. Economic espionage has been defined as the "state-sponsored theft of confidential information belonging to foreign companies," which is then passed to domestic companies "in order to enhance their competitive position within the market and . . . strengthen the national economy." [8] As the number of countries with bans against Huawei

---

3 *See, e.g.,* Sean Keane, *Huawei Ban Timeline: Detained CFO Makes Deal with US Justice Department*, CNET (Sep. 30, 2021, 8:10 AM PST), https://www.cnet.com/tech/services-and-software/huawei-ban-timeline-detained-cfo-makes-deal-with-us-justice-department/ [https://perma.cc/CVU4-VGHJ].

4 *See* Deng Li, *Huawei LYSA: Meet Huawei's First Virtual Person, She Is Realistic and Beautiful*, HUAWEI CENTRAL: NEWS (Jun. 20, 2021), https://www.huaweicentral.com/lysa-meet-huaweis-first-virtual-person-she-is-realistic-and-beautiful-video-demo/ [https://perma.cc/565Z-BVM2].

5 The purpose of identifying such groups is for re-education camps within the People's Republic of China. *See* Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html [https://perma.cc/URY9-KTQH].

6 *See Former CIA Boss Says Aware of Evidence Huawei Spying for China*, REUTERS (Jul. 19, 2013), https://www.reuters.com/article/us-huawei-security/former-cia-boss-says-aware-of-evidence-huawei-spying-for-china-idUSBRE96I06I20130719 [https://perma.cc/WU89-LH23].

7 *See* Keane, *supra* note 3 (noting, among other things, that Trump effectively banned Huawei with a national security order on May 15, 2019).

8 Russell Buchan, *Economic Espionage Under International Law*, EJIL: TALK!, (Jan. 16, 2019), https://www.ejiltalk.org/economic-espionage-under-international-law/ [https://perma.cc/9U7D-B5YG].

grows,[9] so does the need to address grievances relating to economic espionage within the realm of international law.

This Note will explore the background, scope, and recent actions of Huawei in Part I. Part II will examine the existing framework of international law in regards to economic espionage, and Part III will provide analysis of Huawei's actions and the possible recourse they could face under current international law. Finally, this Note will conclude with a recommendation for the future of international law by explaining the need for means of redress for economic espionage and the benefit that it will provide in other realms.

## I. Huawei

### *A. Origins and Growth*

Huawei is far from a simple and straightforward telecommunications company. Even its foundation is cloaked in ambiguity; "Huawei's independence and origins are in dispute."[10] Huawei's "obsession with secrecy" has driven it to shroud its business formation and operations, and seems to have left even the United States government suspicious.[11] In fact, the United States discredits the private company's claim of independence to this day.[12] The Huawei-approved and publicized story is that the company was founded in 1987 by Ren Zhengfei who, through the aid of five private individual investors, "raise[d] Huawei's $5,000 start-up capital."[13] Ren is characterized as a self-starting innovator who came up with creative ways of garnering prestige to the fledging company.[14] Originally beginning as a "sales agent for [a] Hong Kong company producing Private Branch Exchange . . . switches," the company grew throughout the 1990s as it expanded

9 *See* Keane, *supra* note 3 (noting that several countries, including Romania, Sweden, and the United Kingdom, have instituted bans that bar Huawei from providing 5G network and equipment).

10 Norman Pearlstine et al., *The Man Behind Huawei*, LOS ANGELES TIMES (Apr. 10, 2019), https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/ [https://perma.cc/MT5D-84QK].

11 Huawei's publicized origin story is "entirely unbelievable, according to the U.S. government." *Id.*

12 *Id.*; *see also infra* Part I.B.

13 *Id.*

14 *See id.*

into technology and entered the international market.[15] Other major milestones included the Research and Development ("R&D") center in Stockholm, Sweden in 2000, and later claiming earnings of one hundred million United States Dollars ("USD") generated solely through international markets.[16] By the start of 2010, Huawei was a network provider worth many millions.[17] Today, Huawei claims to serve over one-third of the world's population in some capacity.[18]

The scope of Huawei's technology is broad, but can best be classified into three categories: (1) consumer products, (2) carrier services, and (3) enterprise business. The consumer products division concerns the sales of various products, ranging from smartphones, tablets, televisions and other related technology.[19] Consumer products generate over half of the company's total revenue at 482.9 billion Chinese Yuan ("CY"), approximately $75B USD.[20] Huawei's carrier services primarily consist of cellular and internet networks, including fixed and wireless systems,[21] which generate a third of Huawei's revenue, 302B CY ($46B USD).[22] Carrier service also includes Huawei's 5G network, the center of the United States growing concerns.[23] Finally, Huawei's enterprise venture is comprised of incorporating artificial intelligence and processing into everyday systems, such as transportation and education.[24] The enterprise business produces an annual revenue of

---

15 *Our Company*, HUAWEI, https://www.huawei.com/en/corporate-information [https://perma.cc/8BQ5-V4KC] (last visited Jan. 22, 2023).

16 *See id.*

17 *See id.*

18 *See Id.*

19 *See generally* Main Consumer Page, HUAWEI, https://consumer.huawei.com/en/ [https://perma.cc/Z5PF-J6M6] (last visited Oct. 15, 2021).

20 HUAWEI INVEST. & HOLDING CO., LTD., 2020 ANNUAL REPORT 17 (2021) https://wwwfile.huawei.com/minisite/media/annual_report/annual_report_2020_en.pdf [https://perma.cc/3KVR-8HVA] [hereinafter ANNUAL REPORT].

21 *See* Main Carrier Page, HUAWEI, https://carrier.huawei.com/en/ [https://perma.cc/L4KY-8T2C] (last visited Oct. 15, 2021).

22 ANNUAL REPORT, *supra* note 20, at 17.

23 *See Our Company*, HUAWEI, *supra* note 15*; see also infra* Part I.B.

24 *See* HUAWEI, https://e.huawei.com/en/products-and-solutions?l2=adn [https://perma.cc/NPL5-PD9F] (last visited Oct. 15, 2021). For example, Huawei seeks to incorporate the transportation industry with their communication networks to offer "stability and reliability across various industry-specific signaling systems." Huawei, https://e.huawei.com/en/solutions/industries/transportation/digital-railway/operational-

about 100B CY ($15.5B USD).[25] With such a staggering number of resources across a wide range of products, platforms, and services, Huawei is positioned to exert a lot of influence over its customers.

Huawei's international reach extends to nearly all continents, but in varying levels of influence.[26] Some nations have significantly complex relationships with Huawei. Countries with the most influence by Huawei are ones with Huawei-constructed infrastructure and include Bahrain,[27] Hungary,[28] and the majority of "Africa, [where] Huawei has built seventy percent of the continent's 4G networks."[29] With Huawei technology ingrained into a nation's infrastructure, the client nation is more susceptible to network throttling and breaches of client information, including information critical to national security.[30] In contrast, some other nations have taken various measures to scale back the prevalence of Huawei's influence within their borders. India, France, Italy, Vietnam, and Canada "have taken measures that amount to a de facto ban without actually barring Huawei."[31] Only four countries have explicitly

---

communication [https://perma.cc/U4HX-L6ER] (last visited Oct. 15, 2021).

25 ANNUAL REPORT, *supra* note 20 at 17.

26 *See id*. at 133.

27 *See* Alexander Cornwell, *Bahrain to Use Huawei in 5G Rollout Despite U.S. Warnings*, REUTERS (Mar. 26, 2019, 7:55AM), https://www.reuters.com/article/us-huawei-security-bahrain/bahrain-to-use-huawei-in-5g-rollout-despite-us-warnings-idUSKCN1R71B3 [https://perma.cc/7WQB-UXQU] (discussing the approval and rollout of a commercial 5G network using Huawei technology in Bahrain).

28 *See* Reuters Staff, *Hungarian Minister Opens Door to Huawei for 5G Network Rollout*, REUTERS (Nov. 5, 2019, 3:59 AM), https://www.reuters.com/article/us-hungary-telecoms-huawei/hungarian-minister-opens-door-to-huawei-for-5g-network-rollout-idUSKBN1XF12U [https://perma.cc/NRC4-924L] (discussing the Hungarian foreign minister approving Huawei in the rollout of the nation's 5G network).

29 David Sacks, *China's Huawei is Winning the 5G Race. Here's What the United States Should do to Respond*, COUNCIL ON FOREIGN RELS. (Mar. 29, 2021, 3:00AM), https://www.cfr.org/blog/china-huawei-5g [https://perma.cc/N9VB-J9DR].

30 *See generally* Greg Heffer, *Huawei Blocked: Tech Must Be Stripped from UK's 5G Network By 2027*, SKY NEWS (July. 15, 2020, 05:04AM), https://news.sky.com/story/huawei-blocked-tech-must-be-stripped-from-uks-5g-network-by-2027-12028177 [https://perma.cc/XM7V-9FXH] (noting that, when advising British Parliament against allowing Huawei to build their 5G network, U.S. Secretary Pompeo recommended the Parliament use software which "will not threaten national security, economic security, privacy, intellectual property, or human rights," suggesting that Huawei does, in fact, threaten those things).

31 Sacks, *supra* note 29 (noting that while each nation has taken a different approach, the ultimate effect is preventing Huawei from building and operating service provider

banned Huawei: Australia, Japan, New Zealand, and the United States.[32] The driving reason for outward bans stems primarily from concerns that the Chinese government is gathering information via backdoor outlets within Huawei technology.[33] However, these allegations are not the only ones plaguing Huawei's business practices. Considering Huawei's secrecy around its origins, the exponential growth into the international market, and the company's widespread influence across the globe, it is no surprise that Huawei is highly scrutinized, particularly when the company is found at the center of controversy.

### *B. Controversy over independence*

In order to understand the implication of Huawei's actions, it is important to understand some of China's economic policies, particularly the Belt and Road Initiative ("BRI").[34] In 2013, China's President Xi Jinping announced the BRI as a strategy seeking "to connect Asia with Africa and Europe via land and maritime networks with the aim of improving regional integration, increasing trade and stimulating economic growth."[35] The BRI defines "five major priorities: (1) policy coordination; (2) infrastructure connectivity; (3) unimpeded trade; (4) financial integration; and (5) connecting people" and is associated with "investments in infrastructure development," including telecommunication networks.[36] The motivations behind the BRI are speculated to include both geopolitical and economic motivations with the intent to "promote[] a vision of a more assertive China."[37]

---

equipment to each country).

32 Emily Feng, *China's Tech Giant Huawei Spans Much of the Globe Despite U.S Efforts to Ban It*, NPR (Oct. 24 2019 2:30PM), https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it [https://perma.cc/2VWW-QFYZ].

33 *See id.*

34 BELT AND ROAD PORTAL, https://eng.yidaiyilu.gov.cn/ (last visited Dec. 20, 2021) [https://perma.cc/N2S3-HTMA].

35 *Belt and Road Initiative*, EUR. BANK FOR RECONSTRUCTION AND DEV., https://www.ebrd.com/what-we-do/belt-and-road/overview.html [https://perma.cc/MTU9-YTUY] (last visited Jan. 15, 2023).

36 *Id.*

37 Andrew Chatzky & James McBride, *China's Massive Belt and Road Initiative*, COUNCIL ON FOREIGN RELS. (Jan. 28, 2020, 7:00 AM), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative [https://perma.cc/9D24-Q3HG].

Huawei is uniquely situated to advance the BRI mission, particularly the consumer products and carrier service divisions. Not only are consumer products, particularly cellphones, primarily used for "connecting people," but the service provider division has also branched into the transportation industry.[38] As Huawei ventures into digital railways and smart airports,[39] the connection between Huawei and the BRI grows, suggestive of a relationship between the company and the Chinese government. The current controversies surrounding Huawei coupled with the background context of the BRI have caused concern for several nations, particularly those opposed to an increased Chinese presence in the global economy.[40]

Of those nations with concerns over the ties between Huawei and the Chinese government, several bolster their suspicion through numerous sources. The United States government insists that Huawei's founder Ren Zhengfei "was a high-ranking intelligence officer with the People's Liberation Army and that his connections played a role in Huawei being plied with government support,"[41] contrary to the company's assertions.[42] Additionally, despite assurances from Huawei's commissioned legal report that "Chinese law doesn't require [Huawei] to cooperate in intelligence gathering,"[43] the international community still has doubts. Specifically, eyebrows have been raised over the 2017 National Intelligence Law requiring "any Chinese organization or citizen to "support, assist in, and cooperate in national intelligence work" in accordance with other Chinese laws."[44] Conversely, Dr. Gu Bin of the Beijing Foreign Studies University defends the National Intelligence Law as intended to be interpreted through the mindset that "national intelligence work must be defensive in nature," and will not be used actively.[45] However, these defenses have "been met

38 *See* ANNUAL REPORT, *supra* note 20.

39 *See id*.

40 *See* Sacks, *supra* note 29.

41 Pearlstine et al., *supra* note 10.

42 *See id*. (quoting Guo Ping, one of Huawei's chairmen, as saying that "[n]o Chinese government agency or legal entity from China or abroad holds any share of Huawei.")

43 *Id*.

44 *Id.*

45 Bonnie Girard, *The Real Danger of China's National Intelligence Law*, DIPLOMAT (Feb. 23, 2019), https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/ [https://perma.cc/SY6X-9UQH].

by skepticism overseas, given the Communist Party's penchant for superseding the country's laws."[46] Despite assurances to the contrary, there remains doubt as to the influence the Chinese government exerts over the supposedly privately-owned company and its actions.

### *C. Controversy surrounding Huawei and its actions*

At the start of 2019, twenty-three charges were brought against Huawei and its chief financial officer, Meng Wanzhou.[47] The first of charges are for "deliberately dodg[ing] sanctions against Iran by dealing through a company called Skycom."[48] Skycom is believed to be a subsidiary company of Huawei.[49] Ten other allegations were levied for criminal charges of obstruction of justice and attempted theft of trade secrets.[50] These allegations stemmed from a deliberate attempt to steal T-Mobile's robot arm "Tappy," which was designed to "mimic[] human fingers to test phone durability."[51] Huawei originally had an agreement with T-Mobile allowing engineers to access Tappy, until a Huawei employee was accused of taking Tappy outside of the lab.[52] The arm was later recovered by T-Mobile, but only after the engineer had "first emailed pictures and technical information to colleagues in China."[53] Prosecutors alleged Huawei had launched an internal incentive program rewarding employees "who stole confidential info from competitors."[54] The incentive is believed to have been a factor that encouraged one Huawei engineer to steal Tappy.[55]

Huawei's perceived clandestine activities do not stop at the physical theft of property. Huawei has been subject to several accusations of illegally monitoring and gathering data via its

---

46 Pearlstine et. al., *supra* note 10.

47 *Huawei: Tappy the Robot and the Rest of the US Charges*, BBC (Jan. 29, 2019) https://www.bbc.com/news/world-us-canada-47040685 [https://perma.cc/VW7W-CRDD] [hereinafter *Huawei: Tappy the Robot*]. Of note, Meng Wanzhou is the daughter of the founder Ren Zhengfei. *Id.*

48 *Id.*

49 *See id.*

50 *See id.*

51 *Id.*

52 *See id.*

53 *Id.*

54 *Id.*

55 *See id.*

products, and is suspected of acting on behalf of the Chinese government in this matter.[56] Huawei has been accused of building equipment which allows the company to "tap into telecoms using interfaces designed only for law enforcement without alerting the carriers."[57] Further criticism was levied when Huawei filed for a patent on artificial intelligence techniques which could be used to target people based on race, including those of Uighur descent.[58] This is especially controversial due to allegations of the Chinese government detaining Uighur people in forced-labor camps.[59] In response, Huawei claims the patent application reference to race was incorrect, and that the company "opposes discrimination of all types, including the use of technology to carry out ethnic discrimination."[60] Finally, other reported incidents include the backdoor hacking of the Huawei-built servers installed within the African Union.[61] Although Huawei and China have both denied any role in the breach, "for five years confidential data [was] transferred to Shanghai between midnight and 2 a.m."[62] Huawei's involvement with these controversies has continued to dampen the company's image, particularly because of the suggested connection between the company and Chinese government.

As of September 25, 2021, Huawei's global presence has slightly retreated, despite success in the release and deferred charges of Meng Wanzhou.[63] And yet, despite plummeting in the ranks of global smartphone providers,[64] Huawei is adapting and expanding

---

56 *See* Isobel Asher Hamilton, *The US Says Huawei Has Been Spying Through "Back Doors" Designed for Law Enforcement*, INSIDER (Feb. 12, 2020, 12:48PM) https://www.businessinsider.com/us-accuses-huawei-of-spying-through-law-enforcement-backdoors-2020-2 [https://perma.cc/5Z83-N5CC].

57 *Id*.

58 *See* Leo Kelion, *Huawei Patent Mentions Use of Uighur-Spotting Tech*, BBC (Jan. 13, 2021), https://www.bbc.com/news/technology-55634388 [https://perma.cc/32LF-H3RX].

59 *See id.*

60 *Id*.

61 *See* Pearlstine et. all., *supra* note 10.

62 *Id*.

63 *See* Dan Strumpf, *U.S Set Out to Hobble China's Huawei, and So It Has*, WALL ST. J. (Oct. 7, 2021, 10:37 AM), https://www.wsj.com/articles/u-s-set-out-to-hobble-chinas-huawei-and-so-it-has-11633617478 [https://perma.cc/7NSA-MWE4] ("[Huawei's] revenue has dropped for three straight quarters. The company has fallen to No. 9 in smartphone sales, with buyers evaporating from Europe to China.")

64 *See Huawei Only Held 4% Smartphone Market Share in Q1 2021*, GIZMOCHINA

its business scope.[65] Included in this expansion is Hungary's announcement of its corporate agreement with Huawei to "build Europe's first smart railway hub managed by a 5G private network."[66] The entirety of the network will be built, maintained, and potentially covertly monitored by Huawei.[67]

Based upon both its alleged and confirmed actions, this Note argues that Huawei has committed crimes potentially amounting to economic espionage,[68] and is likely to continue in the future. The additional concern of Huawei's massive scope of global influence leads one to the question: if global-scale economic espionage is being committed, can it be addressed under international law?

## II. Background law

One of the first hurdles in addressing economic espionage and intellectual property rights violations is the conclusion that "international trade law is inapplicable to economic espionage."[69] Interestingly enough, there is not an explicit rule that decrees "nations are not to spy on each other," and the practice has remained long-standing throughout the ages.[70] In fact, espionage is such a long-standing practice that it even became a plot device in Shakespeare's *Hamlet*.[71] While the act itself has deep historical

---

(Jun. 11, 2021), https://www.gizmochina.com/2021/06/11/huawei-held-4-smartphone-market-share-q1-2021/ [https://perma.cc/2DHT-QDYZ] ("the Chinese tech giant's smartphone operations has been struggling as US sanctions cut off its primary chip supplier TSMC [Taiwan Semiconductor Manufacturing Company]").

65 *See id.*

66 *Hungary to Build Europe's First 5G Smart Railway Port Together with Huawei*, GLOB. TIMES (Oct. 7, 2021, 08:08PM), https://www.globaltimes.cn/page/202110/1235745.shtml [https://perma.cc/VMZ8-43TY].

67 *See id.; see also* Hamilton, *supra* note 56 (discussing Huawei potentially using its networks for covert monitoring).

68 *See generally* Buchan, *supra* note 8 (discussing economic espionage and the role of international law in addressing it).

69 *Id.*

70 *See* Juan Pablo Hernandez, *The Legality of Espionage in International Law*, The Treaty Examiner, Issue 1 pp. 31-38 (Apr. 2020).

71 *See generally,* WILLIAM SHAKESPEARE, HAMLET act 2, sc. 2, ll. 306-318 (detailing Hamlet discovering that his two friends were sent to spy on him). For further evidence of antiquity in the practice of espionage, see Rose Mary Sheldon's work in uncovering documentation of international espionage in four-thousand-year-old cuneiform archives. *See* Rose Mary Sheldon Spying in Mesopotamia, 33 STUD. IN INTEL. 7 (1989).

roots, the means of carrying out such activities has continued to evolve, keeping pace with the changes in technology.[72] This evolution has made it troublesome to define and classify what actions could be considered espionage. Because the focus of this Note is in the realm of economic espionage, we will turn to existing laws concerning the legal protection of a company's intangible assets as a means of identifying laws that may be used to address crimes of economic espionage. Intellectual property law provides the natural avenue for addressing the effects of economic espionage due to its need "to balance the rights and interests of different groups: of creators and consumers; or businesses and their competitors; of high and low-income countries."[73] The two major organizations who maintain and enforce intellectual property rights internationally are the United Nations and the World Trade Organization.[74]

### *A. The United Nations ("UN")*

The United Nations was founded in 1945.[75] Its membership currently stands at 193 Member States,[76] of which the Republic of China was a founding party.[77] Along with its primary purpose in achieving "international peace and security," the UN also seeks "[t]o achieve international co-operation in solving international problems of an economic . . . character."[78] The UN is structured primarily through a series of councils dedicated to specific realms of responsibility, as well as a "judicial organ" in the form of the International Court of Justice ("ICJ"). [79] Any Member nation that is party to a case before the ICJ must comply with its decisions or else

---

72 *See The Evolution of Spy Technology*, CIOREVIEW (Aug. 12, 2019), https://www.cioreview.com/news/the-evolution-of-spy-technology-nid-30210-cid-158.html [https://perma.cc/U6TT-RL6Q].

73 WORLD INTELL. PROP. ORG., WHAT IS IP? 3 (2020), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf [https://perma.cc/VFA7-SBP8].

74 *See infra* Part II.A & B.

75 *See* UNITED NATIONS, https://www.un.org/en/about-us (last visited Oct. 13, 2021) [https://perma.cc/KC7L-HQKR].

76 *See id*.

77 *See* U.N. Charter art. 110(3).

78 *Id*. at art. 1.

79 UNITED NATIONS, https://www.un.org/en/about-us/main-bodies (last visited Oct. 13, 2021) [https://perma.cc/6V5D-A4JZ]; U.N. Charter art. 92.

may face recourse via the UN's Security Council.[80] The ICJ also has jurisdiction over matters "specially provided for in the Charter of the United Nations or in treaties and conventions in force," and is empowered to interpret the law and determine if a nation is in violation.[81]

Although there are many treaties that may be broadly interpreted to include protections for intellectual property rights, there is one treaty that speaks directly on the subject. Administered by the World Intellectual Property Organization ("WIPO"), the Paris Convention for the Protection of Industrial Property ("Paris Convention") is a treaty adopted in 1883 for the protection of intellectual property and repression of unfair competition.[82] Under Article 10*bis*, Unfair Competition, countries are "bound to assure to nationals of such countries effective protection against unfair competition," defined as "any act of competition contrary to honest practice in industrial and commercial matters."[83] Dr. Russell Buchan[84] of the University of Sheffield believes Article 10*bis* of the Paris Convention "can be invoked to confront the growing threat posed by economic espionage."[85] His premise is based upon three assumptions: (1) economic espionage can be considered "an act of competition," (2) economic espionage would be considered "an act of 'unfair' competition," and (3) Article 10*bis* imposes obligations extraterritorially.[86] Unfortunately, however, the Paris Convention has never been enforced in such a manner.

---

80 *See* U.N. Charter art. 94.

81 Statute of the International Court of Justice, art. 36(1).

82 *See* Paris Convention for the Protection of Industrial Property of March 20, 1883, as Revised at Brussels on December 14, 1900, at Washington on June 2, 1911, at The Hague on November 6, 1925, at London on June 2, 1934, at Lisbon on October 31, 1958, and at Stockholm on July 14, 1967, 828 U.N.T.S. 305 [hereinafter Paris Convention]. China is a signatory of the Paris Convention as of March 19, 1985 but declined to be bound to article 28, Disputes. *See* Paris Notification No. 114, World Intell. Prop. Org. (Dec. 19, 1984), https://www.wipo.int/treaties/en/notifications/paris/treaty_paris_114.html [https://perma.cc/V584-A37A].

83 Paris Convention, *supra* note 81 at art. 10*bis*.

84 *See* Bio for Russell Buchan, EJIL: TALK!, https://www.ejiltalk.org/author/rbuchan/ [https://perma.cc/PL5V-FDXL] ("Dr. Russell Buchan is a Senior Lecturer in international law the University of Sheffield, UK.")

85 Buchan, *supra* note 8.

86 *Id*.

*B. The World Trade Organization ("WTO")*

The WTO was officially founded on January 1, 1995, as the successor to the General Agreement on Tariffs and Trade ("GATT") which was first formed on October 30, 1947.[87] As with the UN, China was also a founding member of the GATT.[88] Recognizing the benefits of multilateral trade, the WTO seeks to "open trade for the benefit of all" by providing "a forum for negotiating agreements aimed at . . . ensuring a level playing field for all."[89] The WTO operates by having its member countries agree to abide by the global rules of trade put forward by the WTO, known as the multilateral trading system.[90] The WTO creates agreements through its general assembly, and in return for abiding to the agreements, "each member receives guarantees that its exports will be treated fairly and consistently in other members' markets."[91] Among these agreements is the Dispute Settlement Understanding, a remedy in the event that a government "think[s] their rights under the WTO agreements are being infringed."[92] Judgements are rendered via specially-appointed independent experts, and "are based on interpretations of the agreements and individual members' commitments."[93] If a party to a dispute does not find the expert-rendered determination acceptable, they have alternative means of appeal; through "a ruling by a panel of experts" and the guarantee of "the chance to appeal the ruling on legal grounds."[94] Interestingly, the Dispute Settlement procedures are only enforceable through the member's own commitments or else face the possibility of economic sanction, however the WTO boasts a

87 *See History of the Multilateral Trading System,* WORLD TRADE ORG., https://www.wto.org/english/thewto_e/history_e/history_e.htm [https://perma.cc/3VUU-YZ4A].

88 *See id.*

89 *Overview*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/wto_dg_stat_e.htm [https://perma.cc/4Q8K-574H].

90 *See* WORLD TRADE ORG., WTO IN BRIEF 6 (2021) https://www.wto.org/english/thewto_e/whatis_e/inbrief_e/inbr_e.pdf [https://perma.cc/9YAY-37R9] [hereinafter WTO IN BRIEF].

91 *Id*.

92 *Id.* at 7.

93 *Id.*

94 *Id*.

track record of 300 disputes resolved since its inception.[95] As the arbiter of legal definitions, the Dispute Settlement Understanding will be the primary method of resolving any matters concerning the interpretation of a treaty, and any alleged violations.

The WTO established the Intellectual Property Agreement ("TRIPS"), which set guidelines on "how copyrights, patents, trademarks, . . . industrial designs and undisclosed information such as trade secrets—'intellectual property'—should be protected when trade is involved."[96] TRIPS requires that nations provide judicial authority to issue injunctions and damages against an infringer of intellectual property rights.[97] However, the only mandatory criminal procedures and penalties are for cases of "willful trademark counterfeiting or copyright piracy on a commercial scale."[98] This means a nation need not create criminal procedures for all violations of intellectual property rights but has the liberty to choose which particular infringements amount to criminal activity "where [the infringements] are committed willfully and on a commercial scale."[99]

## III. Significance of the Case

As previously discussed, the threat of corporate espionage is especially dangerous if it is conducted in conjunction with State support—whether explicit or implicit.[100] While the extent of the relationship between Huawei and China is still undetermined, it is highly suggestive that the Chinese Central government is interested in the affairs and development of Huawei, that the Chinese Central government may be providing support, and that the Chinese Central government may have the power to instruct Huawei to share its significant access to consumer networks, products, and associated data.[101] Unfortunately, the current global forums are not designed to address the symbiotic relationship of a private company sponsored

---

95 *See id.*

96 *See id.*

97 Agreement on Trade-Related Aspects of Intellectual Property Rights arts. 41-45, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS].

98 *Id.*, art. 61.

99 *Id.*

100 *See supra* Part I.B.

101 *See supra* Part I.B & II.B.

by the state.[102] Furthermore, leaving the matter to be resolved by individual state action is an inadequate response and can disadvantage countries that have relied on Huawei networks to their detriment.[103] Finally, individual state action "is undermined by the fact that states find it difficult to exercise their jurisdiction over government agents once they return to their home state."[104] This Note proposes two solutions meant to empower the UN or WTO with mechanisms to address the threat of nation-state supported corporate espionage.

### A. The UN should create standards for defining the roles of state actors v. private actors.

The ICJ has the authority to interpret Article 10*bis* of the Paris Convention to address actions of economic espionage as a violation against unfair competition, but the ICJ faces several challenges before a suit can be brought against Huawei. The first and most difficult challenge is Article 34, Section 1 of the Statute of ICJ: "Only states may be parties in cases before the Court."[105] Huawei is incorporated as a private international company "wholly owned by its employees," where "[n]o government agency or outside organization holds shares in Huawei."[106] Additionally, there is no regular standard indicating how much evidence is sufficient to prove state involvement with a private party to constitute state action.[107] Therefore, without a standard of state-involvement and without evidence directly showing explicit state involvement with Huawei, the company cannot be brought before the ICJ.

The issue of states not being liable for the actions of private actors is a frequent problem with espionage and other emerging

---

102 *See infra* Part III.A.

103 In response to the announcement of removal of existing Huawei software in British networks, other network providers have warned the sudden total removal "would cost billions of pounds and lead to customers losing phone signal for several days." Alexander Martin, *Huawei: The Company and the Security Risks Explained*, SKY NEWS (Sep. 23 2020, 15:06 PM) https://news.sky.com/story/huawei-the-company-and-the-security-risks-explained-11620232 [https://perma.cc/UC7M-X5F9]; *see also infra* Part III.B.

104 Buchan, *supra* note 8.

105 Statute of the International Court of Justice art. 34(1).

106 Pearlstine et al., *supra* note 10.

107 *See* Buchan, *supra* note 8 ("[t]he takeaway point is that there is no general and uniform rule on the spatial scope of treaties.")

practices in modern "warfare," particularly in cyberspace.[108] In regards to this same impediment in cyberspace, security technologist Bruce Schneier[109] recommends "establishing rules of engagement . . . including ways to identify where attacks are coming from and clear definitions of what does or does not constitute an offensive action" as well as understanding the role of "cybermercenaries" in contrast to "a non-state actor."[110] In this instance instead of a "cybermercenary,"—a cyberspace-hacking party hired on behalf of a nation[111]—during economic espionage, a private company leaks or shares client information to the host nation. If a similar standard of liability were to be developed and adopted by the UN for economic espionage by state-sponsored versus non-state actors, a nation could be held liable for such actions of a private company. Particularly in the domain of cyberspace and other rapidly evolving sectors, such as those heavily reliant upon technology, the UN should choose to read treaty language involving those areas to apply extraterritorially. This would allow "cybermercenaries," companies engaged in economic espionage, and other similar criminals to be held accountable in the courts of international law.

Assuming that such a standard existed, and the allegations tying Huawei and the Chinese government are verified, the ICJ would need to interpret Article 10*bis* of the Paris Convention to include economic espionage. Article 10*bis* can address economic espionage if three inferences are made from the text: (1) economic espionage constitutes an "act of competition;" (2) economic espionage amounts to an act of unfair competition; and (3) Article 10*bis* imposes obligations extraterritorially.[112] These inferences can be

---

108 *See* Bruce Schneier, *Cyberconflicts and National Security*, U.N. CHRON. (Aug. 12, 2013), https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security [https://perma.cc/4JG2-GM6B] ("[w]hen you are being attacked in cyberspace, the two things you often do not know are who is attacking you and why . . . There is espionage, sometimes by lone actors and sometimes by national espionage organizations.")

109 *See About Bruce Schneier*, https://www.schneier.com/blog/about/ (last visited Oct. 14, 2021) [https://perma.cc/T8UQ-G2TT] ("Schneier is a fellow at the Berkman Klein Center for Internet & Society at Harvard University; a lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation and Accessnow; and an Advisory Board Member of the Electronic Privacy Information Center and Verified Voting.org.")

110 Schneier, *supra* note 108.

111 *See id.*

112 Buchan, *supra* note 8.

supported based upon the intent of the Paris Convention for broader interpretation of its text, the delineated scope of protection, and indication within the text "that it is nationality that restricts the application of Article 10*bis* rather than geographic location of the targeted nations."[113]

Continuing under the lens of the UN, China could be brought before the ICJ to answer for Huawei's actions; unfortunately, this is not likely to be a timely or reliable response in the current setting for a number of reasons. First, overcoming Huawei as a private actor is nearly impossible at the given moment because there is a lack of momentum in the UN moving towards holding private entities responsible as state actors. However, this momentum is not completely stalled; General Assembly report A/70/174 reported a finding regarding information and communication technologies ("ICTs") that "states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by the non-State actors to commit such acts."[114] If such recommendations were enacted into resolution, this would have created a direct indemnification for state-sponsored corporate espionage. However, the following two General Assemblies were unable to establish a consensus for any further action.[115] Delays also occur at the adjudication stage; the ICJ is currently experiencing "a particularly high level of activity," as reported in the 1 August 2020-31 July 2021 summary report, where the Court delivered four judgements and currently faces fourteen pending cases on the Court's General List.[116] Finally, the range of remedies available to the UN[117] and lack of precedent render it impossible to predict the official response to a judgement against China.

---

113 *Id.*

114 Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Letter dated 26 June 2015 from the Chair of the Group to the Secretary-General at ¶ 28(e), U.N. Doc. A/70/174 (Jul. 22, 2015).

115 *See* Fact Sheet, U.N. Off. for Disarmament Affs., Developments in the Field of Information and Telecommunications in the Context of International Security (Jul. 2019), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [https://perma.cc/ND8D-B5SN].

116 U.N. GAOR, 76th Sess., 4th supp. at 5-6, U.N. Doc A/76/4 (Aug. 1, 2021).

117 *See* U.N. Charter art. 41 (empowering Security Council to require UN members to take measures including "interruption of economic relations and of rail, sea, air, postal, telegraphic, radio and other means of communication in severance of diplomatic relations" to enforce its decisions).

With the discouraging amount of uncertainty and lack of precedent in the UN, it will be unreliable to depend upon the UN to address Huawei's actions. Therefore, alternative means of addressing the matter under international law must be considered, particularly under the WTO.

### *B. Petition WTO to include economic espionage criminal procedures*

As the TRIPS agreement presently stands, Huawei may only be held liable for economic espionage via state prosecution. TRIPS only requires that home nations maintain criminal procedures for "willful trademark counterfeiting or copyright piracy on a commercial scale."[118] Allegations and charges of economic espionage arising out of Huawei will only be tried under Chinese law, unless actors are caught within the borders of another country.[119] Chinese law currently reflects criminal penalties for "obtaining an obligee's business secrets by stealing, luring, coercion or any other illegitimate means," resulting in imprisonment for a period of not more than seven years.[120] As of yet, Huawei has never been charged with a violation of this law, and logic suggests a nation is unlikely to prosecute a state-sponsored company. Thus, trying the matter in the International Court would allow for the victim nation to seek adequate damages and for a stronger stance against state-sponsored activity.

Assuming a country successfully alleges that China is not abiding by the TRIPS agreement in failing to prosecute Huawei, the standard of review is in likely in favor of China. TRIPS agreement disputes are bound to be heard under the Dispute Resolution Agreement.[121] Assuming the dispute would be brought under Article 61,[122] there may require a more difficult undertaking in proving China's current law is in violation under existing TRIPS standards. A previous precedent found China's existing law sufficient passed a preliminary review for inconsistency with TRIPS, while also

---

118 TRIPS, *supra* note 97 at art. 61; *see also supra* Part II.B.

119 *See e.g., Huawei: Tappy the Robot*, *supra* note 47.

120 Criminal Law of the People's Republic of China, Art. 219(1) (Jul. 1, 1979), https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/5375/108071/F-78796243/CHN5375%20Eng3.pdf [https://perma.cc/VMH4-LWK5].

121 *See* TRIPS, *supra* note 97 at art. 64.

122 *See id.* art. 61.

finding the United States failed to prove "criminal thresholds were inconsistent with China's obligations under . . . the TRIPS agreement."[123] Although this victory for China does not guarantee victory against future charges, having precedent to point to offers support of its position of compliance. However, if Article 61 were to be amended to require criminal procedures for economic espionage, it is possible the standard of review by panel members may find China's current procedures and penalties insufficient and could issue an advisory opinion for remedy. After an advisory opinion is published by the panel, the panel generally publishes recommendations for each country, which a nation may choose to adopt.[124] There are procedures for compensation and suspension of concession, should a nation fail to adequately adopt or choose to not follow the recommendation of the panel.[125] However, these penalties "shall be temporary,"[126] leaving the WTO relatively toothless in its enforcement.

## IV. Conclusion

Presently, there is no way to combat economic espionage, and therefore Huawei's actions will continue to go unpunished by international law. The UN is unable and likely unwilling, due to lack of unanimous support, to prosecute private actors—regardless of state sponsorship. While the WTO seems to be aligned with the ideology of protecting fair practices and intellectual property rights, the organization does not have a lasting mechanism for enforcement, leaving state action as the only available remedy. Despite adopting stricter criminal laws, it does not seem likely that China will fully police these violations, as Huawei is not the sole

123 In 2007, the United States alleged a complaint against China for a lack of criminal procedures and penalties for commercial scale counterfeiting and piracy, amounting to an inconsistency with TRIPS art. 61. *See* Request for Consultations by the United States, *China – Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, at 2, WTO Doc. WT/DS362/1 (Apr. 16, 2007). *See also* Summary of Key Panel Findings, (2021 ed.) ("[t]he Panel found China's criminal measures . . . was not enough to find a violation because Art. 61 does not require Members to criminalize all copyright and trademark infringement") [https://perma.cc/V4S2-6LAA].

124 *See* Understanding on Rules and Procedures Governing the Settlement of Disputes art. 19, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401.

125 *See id*. art. 22.

126 *Id*. art. 22(8).

suspected perpetrator. Other Chinese-owned companies, such as Tik Tok, have been shrouded in similar allegations of backdoor espionage.[127]

The issue of not creating international procedures to address economic espionage, is that it is an infinite feedback loop. As actors continue to commit economic espionage, they get better at it. Likewise, as technology continues to evolve and society continues to rely on it, the need for a standard of liability will increase. Creating international remedies now is paramount, because there needs to be some mechanism of deterrence against espionage. Without any sort of available remedy rooted in international law, there are no means of redress for victim nations. Without redress, the perpetrators remain undeterred from committing future criminal conduct. And with the burgeoning technology and communication industry, the threat of injury will only continue to grow.

127 *See* Zak Doffman, *Is TikTok Spying on You for China?*, FORBES (Jul. 25, 2020 11:22 AM) https://www.forbes.com/sites/zakdoffman/2020/07/25/beware-tiktok-really-is-spying-on-you-new-security-report-update-trump-pompeo-china-warning/?sh=1200be264014 [https://perma.cc/C8P7-Y7ST].