CORPORATE VIOLATIONS OF HUMAN RIGHTS: ADDRESSING THE COORDINATED SURVEILLANCE AND PERSECUTION OF THE UYGHUR PEOPLE BY THE CHINESE STATE AND CHINESE CORPORATIONS

Ross Smith[*]

TABLE OF CONTENTS

[*]J.D., University of Georgia School of Law, 2021. B.A. in History and Political Science, Northwestern University, 2017. I want to say thank you to all of the *Georgia Journal of International and Comparative Law* members and University of Georgia Law Library staff who aided in the publication of this note. I want to give a special thank you to Professor Harlan Cohen, who provided me with valuable insights and guidance during the writing process.

I. INTRODUCTION

The rise of social media platforms has simplified individuals' ability to form deep connections and maintain better communication with members of their communities as well as with loved ones, friends, work colleagues, and others across the globe. While social media has many positive impacts in society, the trend of increasing digitalization across the globe also arguably gives rise to many unanticipated, destructive externalities. These negative externalities range from the improper use of user data by corporate entities to the exploitation of the powerful reach of social media by terrorist organizations.[1]

Member states of the United Nations (U.N.) have taken some steps to counter the harmful byproducts of the social media revolution, such as the Tech Against Terrorism initiative, which "promote[s] constructive working relationships between the tech and government sectors" to "tackle terrorist use of the internet whilst respecting human rights."[2] While the U.N. has taken steps to address many of the negative side effects of social media, there are ongoing concerns regarding how the international community can address the economic incentives of social media corporations and the unique nature of social media platforms that encourage exploitation of users.[3] One inherent difficulty in promoting international standards for social media corporations and platforms is that government actors arguably have a strong incentive to utilize user data collected by social media platforms as a means of monitoring and manipulating public opinion. This government incentive makes it difficult for the international community to reach a consensus on standards that states will hold themselves to when interacting with social media corporations and user data.

Some bodies have formulated concrete protections of individual rights and user data, such as the European Union's privacy law from 2016, the General Data Protection Regulation.[4] However, these developments have not been echoed worldwide, and many communities likely still face exploitation of their data by corporate and government actors. Questions remain as to how the international community can address the exploitation of social media platforms by

---

[1] Alex Voloshin, *Social Media Corporations: International Law and the Regulation of Social Media Abuse*, SEMINAR ON CORP. & INT'L L. (May 9, 2018).

[2] *About Tech Against Terrorism*, TECH AGAINST TERRORISM, https://www.techagainstterrorism.org/about/ (last visited Oct. 9, 2020).

[3] *Social Media's Moral Reckoning: Changing the Terms of Engagement with Silicon Valley*, HUM. RTS. WATCH (Dec. 21, 2018, 6:01 AM), https://www.hrw.org/news/2018/12/21/social-medias-moral-reckoning.

[4] Commission Regulation 2016/679, 2016 O.J. (L 119) 1.

government actors and how domestic actors can pressure foreign states and international corporations to comply with international law.

Some of the most egregious abuses and manipulation of user data have occurred in China, where the Chinese State enacted a repressive surveillance regime in the Xinjiang province over its Uyghur Muslim population in the name of national security.[5] Examinations of the Chinese regime in Xinjiang reveal that the State is facilitating "segregated surveillance," where security personnel force the Uyghur Muslim population to "submit to monitoring and data collection while generally ignoring the majority Han Chinese, who make up 36 percent of Xinjiang's population."[6] The Chinese government procures surveillance equipment to use in Xinjiang from large state-owned enterprises such as the China Electronics Technology Corporation and Chinese multinational tech firms such as Hikvision and Huawei.[7] The Chinese State has placed potentially "as many as 1.5 million Uyghurs and members of other Muslim minorities" into "re-education and detention centers," which are used to promote loyalty to the Communist Party.[8]

This note seeks to examine the various international legal mechanisms and regimes that could support a finding of corporate liability in situations where tech companies have played a large role in government abuses of human rights and examines potential alternatives at the regional and transnational levels. First, this note will closely examine the ongoing Chinese surveillance regime in the Xinjiang province and international responses to the Chinese corporate actors' conduct. This first section also discusses China's political strength on the international stage and the state's perception of and attitude towards its international legal obligations. Second, this note will explore the relative lack of relevant applicable international law and regulations to this issue, which is the product of both rapid technological development and political incentives for states to exploit and manipulate user data. Third, this note will examine international responses to the challenges of the social media and technological revolution on the regional level, as well as states' domestic policies aimed at ensuring corporate responsibility for human rights violations and protection of user data.

Lastly, this note will argue that existing international legal mechanisms are insufficient to protect user data and prevent human rights abuses facilitated by exploiting digital channels. Existing international criminal legal regimes cannot realistically hold many corporate actors liable for their international crimes,

---

[5] 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.

[6] *Id.*

[7] *Id.*

[8] Nick Cumming-Bruce, *U.S. Steps Up Criticism of China for Detentions in Xinjiang*, N.Y. TIMES (Mar. 13, 2019), https://www.nytimes.com/2019/03/13/world/asia/china-muslim-xinjiang.html?module=inline.

much less those who state actors shield. Given China's role on the U.N. Security Council and its overall influence in East Asia and worldwide, this paper argues that existing international law and international legal mechanisms fail to effectively hold Chinese corporate actors accountable for their human rights abuses in the Xinjiang province.

Instead, individual states must work with corporate actors, such as executives in tech firms and the social media industry, to promote responsible handling of user data. Furthermore, individual states must develop comprehensive transnational sanction regimes that target those international corporate entities that facilitate human rights abuses. This push for widespread initiatives on the domestic level could realistically form customary international legal obligations and would encourage the creation of stronger multilateral legal instruments.

II. BACKGROUND

A. Internet Regulation, Digital Surveillance, and Human Rights Violations in China

i. Internet Regulation by the Chinese State

The Chinese State's expansive regime of internet regulation has received increasingly heavy criticism by nations and other international actors in recent years. Freedom House, an independent watchdog organization that "amplif[ies] the voices of those struggling for freedom in repressive societies and counter authoritarian efforts to weaken international scrutiny,"[9] declared China "the world's worst abuser of internet freedom" in its 2019 Freedom on the Net report, *The Crisis of Social Media*.[10] China has implemented a number of domestic laws and policies that not only heavily restrict the ability of domestic and foreign corporations to conduct work within the State, but also require companies to expressly support the Chinese government in its repression of civil rights and

[9] *About Us*, FREEDOM HOUSE, https://freedomhouse.org/about-us (last visited Mar. 24, 2021).

[10] Adrian Shahbaz & Allie Funk, *Freedom on the Net 2019: The Crisis of Social Media*, FREEDOM HOUSE, https://www.freedomhouse.org/report/freedom-net/2019/crisis-social-media (last visited Apr. 5, 2021).

political dissident within the State.[11] As "[t]he community of Chinese Internet users continues to grow," the Chinese State has "simultaneously increase[d] its capacity to restrict content that might threaten social stability or state control."[12] China's sophisticated internet censorship regime is known informally as the "Great Firewall," largely due to its automated blocking of many websites and services based outside China.[13] This regime largely targets those that criticize the leadership or policies of the Chinese Communist Party.[14] Both domestic and international companies also face pressure to support the Chinese government's stance on disputed terms and policies, such as territorial claims.[15] Chinese authorities use both publicly announced rules as introduced by regulatory bodies and special measures that are "aimed at creating a stable online environment during a major [political] event" to tighten internet regulation when the Chinese State feels the potential for political instability.[16]

International companies based outside of China face intense pressure to comply with the Chinese government's policies or risk complete censorship of their platforms and technology within China. The Chinese State has blocked internet access to many international news outlets, especially those that host Chinese-language websites.[17] Most international social media platforms are completely blocked in China, which has corresponded with exponential growth of Chinese platforms such as Tencent's WeChat.[18] Other international internet platforms, such as Google, have worked to develop platforms that comply with China's expansive censorship requirements.[19] Apple and Microsoft, both of which censor

---

[11] *See* Alexandra Stevenson, *China's Communists Rewrite the Rules for Foreign Businesses*, N.Y. TIMES (Apr. 13, 2018), https://www.nytimes.com/2018/04/13/business/china-communist-party-foreign-businesses.html.

[12] *China,* OPENNET INITIATIVE, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf (last visited Mar. 24, 2021)

[13] *Freedom on the Net 2019: China*, FREEDOM HOUSE, https://freedomhouse.org/country/china/freedom-net/2019 (last visited Apr. 5, 2021) [hereinafter *Freedom on the Net 2019: China*].

[14] *See* Adrian Shahbaz & Allie Funk, *Freedom on the Net 2020: The Pandemic's Digital Shadow*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow (last visited Apr. 5, 2021).

[15] *China: Events of 2018*, HUM. RTS. WATCH, https://www.hrw.org/world-report/2019/country-chapters/china-and-tibet#eaa21f (last visited Apr. 6, 2021) ("In January [2018], US-based Marriott International apologized for listing Taiwan and Tibet as separate countries on its website after authorities shut down the website and app in China for a week.").

[16] Cheang Ming & Saheli Roy Choudhury, *China Has Launched Another Crackdown on the Internet – but It's Different This Time*, CNBC (Oct. 26, 2017, 8:06 PM), https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html.

[17] *Freedom on the Net 2019: China*, *supra* note 13.

[18] *Id.*

[19] *China: Events of 2018*, *supra* note 15 ("Google, which suspended its search service in China in 2010 citing censorship concerns, had been developing a censored search engine app

certain conduct on their Chinese networks, have faced criticism from lawmakers in the United States and from international groups for "helping to suppress rights they declare as essential in their home markets."[20] Both Apple and Microsoft have justified their participation in the Chinese market as helping promote opportunity and civil rights for the Chinese populace, but critics instead view this compliance as making it "easier for the authorities to convince other foreign companies to do the same."[21] Apple and Facebook additionally removed apps and developed unique software to respectively conform with the Chinese State's policies in 2016.[22] Critics argue that China's internet policies, specifically those enforced against foreign companies, represent a blatant violation of China's commitment "to a broad liberalization of trade in services, including data processing and telecommunications" that the State took on when it joined the World Trade Organization in 2001.[23]

The Chinese government's intensive internet regulations have resulted in a growth of Chinese companies, many owned or at least partially controlled by the State, that must comply with these restrictive rules and promote the Chinese government's policies.[24] Locally hosted websites in China must "proactively monitor content on their platforms and remove banned material from their platforms" or "may face severe punishment for failure to comply."[25] In August of 2013, the Chinese government issued a set of regulations called the "seven baselines," which forced Chinese companies to immediately shut down more than 100,000 accounts on their websites that did not comply with these rules.[26] Sina Weibo, a Chinese blogging platform similar to Twitter, experienced a seventy percent drop in the number of posts on its platform between 2011 and 2013.[27]

The Cyberspace Administration of China (CAC) oversees the telecommunications sector and regulates internet content.[28] The CAC reports in turn to the

for the Chinese market. The app would reportedly comply with China's expansive censorship requirements by automatically identifying and filtering sites blocked by the Great Firewall, China's internet filtering system.").

[20] Tom Simonite, *US Companies Help Censor the Internet in China, Too*, WIRED (June 3, 2019, 7:00 AM), https://www.wired.com/story/us-companies-help-censor-internet-china/.

[21] *Id.* (quoting Charlie Smith, cofounder of Greatfire.org, which monitors Chinese censorship).

[22] *Freedom on the Net 2017: China*, FREEDOM HOUSE, https://freedomhouse.org/country/china/freedom-net/2017 (last visited Apr. 6, 2021).

[23] *See, e.g.*, Tim Wu, *China's Online Censorship Stifles Trade, Too*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/opinion/china-censorship-internet.html.

[24] *Freedom on the Net 2019: China*, *supra* note 13.

[25] *Id.*

[26] Elizabeth C. Economy, *The Great Firewall of China: Xi Jinping's Internet Shutdown*, GUARDIAN (June 29, 2018, 1:00 EDT), https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown (reporting that one Chinese company "shut down or 'handled' 100,000 Weibo accounts found to not comply with the new rules").

[27] *Id.* (referring to a study of 1.6 million Weibo users).

[28] *Freedom on the Net 2019: China*, *supra* note 13.

Central Cyberspace Affairs Commission, which is headed directly by Xi Jinping,[29] creating a direct line of communication from China's leader to internet regulators. The Chinese Communist Party also uses its Central Propaganda Department to oversee ideological trends in online content.[30] Under this regime, censorship decisions often "are arbitrary and inconsistent, largely because of the amount of individuals and processes involved."[31] In June 2016, the CAC released a "mobile internet apps information service regulation," which requires companies that offer digital apps to manage content produced and posted by users.[32]

There are numerous examples of recently passed regulations by the Chinese State that have further restricted the ability for businesses to host and produce internet content in China. China's Cybersecurity Law (CSL), which took effect in 2017, imposed a myriad of guidelines and restrictions for Chinese and multinational companies engaged in internet business in China.[33] These include increased requirements to censor, mandated data localization, real-name registration rules, and the obligation to assist security agencies with investigations.[34] Additionally, the law requires that foreign companies store Chinese user data in mainland China.[35] In response to the heavy censorship requirements, companies such as Beyondsoft have begun offering censorship services for other Chinese platforms in order to ensure that these clients comply with Chinese domestic laws.[36] Other companies, such as Sina Weibo and China's top news app, Jinri Toutiao, have hired thousands of in-house content reviewers within the last few years to comply with increasing pressure from the Chinese government.[37] Furthermore, China issued regulations in May 2017 banning the publishing of online news or information services by sites not licensed by the Chinese government.[38] Under the CSL, businesses engaged in internet activities face a variety of monetary penalties and even detention for failing to comply with the various requirements of the law.[39]

---

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Freedom on the Net 2017: China*, *supra* note 22.

[33] *Freedom on the Net 2019: China*, *supra* note 13.

[34] *Id.*

[35] *Freedom on the Net 2017: China*, *supra* note 22.

[36] Li Yuan, *Learning China's Forbidden History, So They Can Censor It*, N.Y. TIMES (Jan. 2, 2019), https://www.nytimes.com/2019/01/02/business/china-internet-censor.html ("Beyond-soft employs over 4,000 workers . . . at its content reviewing factories. That is up from about 200 in 2016.").

[37] *Freedom on the Net 2019: China*, *supra* note 13.

[38] *Freedom on the Net 2017: China*, *supra* note 22.

[39] Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 59–70, 2016 STANDING COMM. NAT'L PEOPLE'S CONG.

Most relevant to this Note, however, are the Chinese internet laws that inordinately impact activists, minority groups, and other individuals that the Chinese government deems dissident. The CAC and other Chinese governmental bodies have routinely introduced new rules and guidelines that increasingly restrict user-generated content.[40] Human rights activists and their families have been subjected to targeted network disconnections during times of domestic turmoil.[41] Article 12 of the CSL dictates that individuals "must not use the Internet to engage in activities endangering national security, national honor, and national interests."[42] Article 58 of the CSL allows the CAC "to take temporary measures regarding network communications in a specially designated region" when a "need to protect national security and the social public order" exists or when a "major security incident[]" occurs.[43] Furthermore, Article 24 mandates that "network operators," or those companies and actors who engage in internet business, require users to provide their real identity in order to use that service.[44] User data from social media accounts and other platforms are processed by the "Police Cloud" system used by the Chinese government to track and predict the activities of human rights activists, ethnic minorities, and political dissidents.[45] When Chinese authorities conduct investigations based on some communication or content perceived to be harmful to the interests of the Chinese State, these authorities have the power to punish users for even private conversations between a small number of people.[46]

Many of the Chinese companies that directly engage in production of surveillance tools for the Chinese State have received international criticism for their role in the suppression of minority and dissident groups in China, with states

---

[40] *See Freedom on the Net 2019: China*, *supra* note 13.

[41] *Id.* ("Ding Zilin, one of the founders of Tiananmen Mothers, a group of activists who lost loved ones during the Tiananmen Square protests, was closely monitored in the weeks leading up to the June 4 anniversary in 2019, and her mobile phone connection was reportedly cut off.").

[42] Cybersecurity Law of the People's Republic of China, art. 12.

[43] *Id.* art. 58 (allowing the government to "limit[]" network communications that threaten national security or the social public order).

[44] *Id.* art. 24 ("Network operators . . . shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.").

[45] *China: Police 'Big Data' Systems Violate Privacy, Target Dissent*, HUM. RTS. WATCH (Nov. 19, 2017, 7:50 PM), https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent#.

[46] *See Freedom on the Net 2019: China*, *supra* note 13 ("In April 2018, . . . [police were instructed to] investigate an individual who had criticized Xi Jinping in a WeChat group with only eight members. Though the individual had used a pseudonym, the instructions identified him with his real name, address, and phone number.").

such as the United States putting Chinese companies on "trading blacklists."[47] Despite this international pressure, the sheer size of China's population, in combination with the government's restrictions on foreign businesses and content, have helped cultivate the domestic Chinese tech industry. This domestic industry is heavily influenced and controlled by the Chinese State, and the government arguably utilizes this power dynamic to promote political stability and the Communist Party's interests.

ii. The Role of Social Media and Digital Surveillance in the Persecution of the Uyghur People in the Xinjiang Region of China

Since early 2017, Chinese authorities have detained at least 800,000 and possibly more than two million Uyghurs and members of other Muslim minorities in internment camps.[48] This policy of detainment continues the pattern of human rights abuses against these communities by the Chinese State in the Xinjiang Uyghur Autonomous Region.[49] As a part of this pattern of acts against the Uyghur population, the Chinese State has required that social media platforms such as the Chinese platform WeChat allow the government to monitor the activity of its users.[50] WeChat now actively requires users to provide voice samples and facial scans in order to use the platform.[51] Government officials have targeted some users for their communication via WeChat with relatives living abroad.[52] Other companies, such as Chinese artificial intelligence giant iFlytek, have supplied technology to officers of the Chinese State that is utilized to heavily monitor the Uyghur populace.[53] The government has also forced residents of the Xinjiang province to download an app, JingWang, that scans devices for particular

---

[47] Isobel Asher Hamilton, *The US Blacklisted Some of China's Most Valuable AI Startups over Human Rights Issues in a Dramatic Trade War Escalation*, BUS. INSIDER (Oct. 8, 2019, 5:49 AM), https://www.businessinsider.com/us-blacklists-china-ai-startups-2019-10.

[48] Megan Keller, *State Dept. Official: China Holding 800k Muslim Minorities in Internment Camps*, HILL (Dec. 5, 2018, 12:09 PM), https://thehill.com/homenews/administration/419855-state-dept-official-china-holding-800k-uighurs-others-in-internment.

[49] *The China Challenge: Hearing Before the Subcomm. on E. Asia, the Pac., & Int'l Cybersecurity Pol'y of the S. Comm. on Foreign Rels.*, 115th Cong. 85–91 (2018) (statement of Scott Busby, Deputy Assistant Sec'y, Hum. Rts. & Lab., U.S. Dep't of State).

[50] Isobel Cockerell, *Inside China's Massive Surveillance Operation*, WIRED (May 9, 2019, 7:00 AM), https://www.wired.com/story/inside-chinas-massive-surveillance-operation/.

[51] *See* Stephen McDonell, *China Social Media: WeChat and the Surveillance State*, BBC NEWS (June 7, 2019), https://www.bbc.com/news/blogs-china-blog-48552907.

[52] *See Freedom on the Net 2019: China*, *supra* note 13.

[53] Isobel Cockerell, *supra* note 50.

files and collects data from users.[54] This program is designed to search for files that match content blacklisted by the Chinese State.[55] The Chinese government also has the power to disable popular social media apps in Xinjiang and does so in order to "clean" religious content and other material deemed extremist by the State.[56] It further detained Muslim residents of Xinjiang for privately celebrating the independence of Kazakhstan from the Soviet Union.[57] While the Chinese government has denied the existence of these camps, observers have cited public projects and expenditures by the Chinese government in the Xinjiang region as well as steady development of China's "re-education" systems in the region as clear evidence supporting their existence.[58]

States and organizations have begun responding to the Chinese State's repressive tactics in Xinjiang with sanctions against those Chinese security and surveillance firms that aid the State in committing human rights abuses. In October of 2019, the U.S. government decided to blacklist top Chinese-based surveillance companies in response to reports of the ongoing human rights abuses in Xinjiang.[59] However, these sanctions constitute export controls on U.S. origin goods, instead of the more onerous Magnitsky sanctions that the U.S. government can impose on foreign actors for human rights abuses.[60] The United States had previously banned U.S. technology companies from selling products to Huawei, the

---

[54] Joseph Cox, *Chinese Government Forces Residents to Install Surveillance App with Awful Security*, VICE (Apr. 9, 2018, 12:00 PM), https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang.

[55] *Freedom on the Net 2019: China*, *supra* note 13.

[56] *See, e.g.*, Wenxin Fan, *China Appears to Block Social-Media Platform Clubhouse After Brief Flourishing of Debate*, WALL ST. J. (Feb. 8, 2021, 11:51 PM), https://www.wsj.com/articles/china-appears-to-block-social-media-platform-clubhouse-after-brief-flourishing-of-debate-11612810286 ("Beijing's censors appeared to slam the door on Clubhouse, Silicon Valley's latest social-media hit, after a frenzied week in which the audio-only chat app helped spark a rare outpouring of freewheeling debate on taboo topics in the Chinese-speaking world.").

[57] *Freedom on the Net 2018: China*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2018/china (last visited Apr. 7, 2021) ("In December 2017, around 40 ethnic Kazakhs were arrested for disseminating content in WeChat groups that celebrated the independence of Republic of Kazakhstan from the Soviet Union.").

[58] Adrian Zenz, *New Evidence for China's Political Re-education Campaign in Xinjiang*, JAMESTOWN FOUND. (May 15, 2018, 7:00 AM), https://jamestown.org/program/evidence-for-chinas-political-re-education-campaign-in-xinjiang/ ("This article demonstrates that there is, in fact, a substantial body of PRC governmental sources that prove the existence of the camps. Furthermore, the PRC government's own sources broadly corroborate some estimates by rights groups of number of individuals interred in the camps.").

[59] Charles Rollet, *Xinjiang Backlash Is Hitting Chinese Firms Hard*, FOREIGN POL'Y (Oct. 18, 2019, 11:58 AM), https://foreignpolicy.com/2019/10/18/xinjiang-sanctions-chinese-firms-surveillance/ ("The entities affected include the world's two largest security camera manufacturers and three multibillion-dollar facial recognition start-ups.").

[60] *Id.* (explaining that Magnitsky sanctions "would ban all transactions between covered entities and the United States").

Chinese telecommunication giant, but in 2019 the United States began issuing licenses to some firms to allow them to sell to the Chinese company.[61]

In June of 2020, the United States passed the Uyghur Human Rights Policy Act of 2020, which requires various U.S. government bodies to report human rights abuses by the Chinese government against the Uyghur population in Xinjiang.[62] In this Act, the United States specifically cited the policies and detentions in Xinjiang as violating China's international human rights law obligations under the International Convention on the Elimination of All Forms of Racial Discrimination, the Convention Against Torture and Other Cruel Inhuman or Degrading Treatment or Punishment, the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights.[63] Politicians in the United Kingdom, Germany, and the Netherlands are also raising concerns about Chinese firms that either produce products for the European market or design intensive security apparatuses for the Chinese State authorities.[64]

While U.S. sanctions have had some effect on the market performance of Chinese firms that assist in human rights abuse, some U.S. politicians have argued that forming multilateral sanction regimes with partners such as the EU would more effectively deter such conduct by these Chinese companies and influence the conduct of the Chinese State by association.[65] Although the EU has decried China for some of its human rights abuses, it has received criticism for not more firmly pressing China on the human rights violations in Xinjiang during the 2019 EU-China Summit.[66]

China's influence on the global stage, extensive financial capital, and increasing domestic technology sector have arguably hampered the efforts of individual states and the international community at large to hold Chinese corporations and their controlling governmental actors liable for human rights violations in Xinjiang. Both the Council on Foreign Relations and Freedom House, two major non-governmental organizations (NGOs) that focus on international issues, have cited a report by the New York Times that China has exported its artificial

---

[61] Sherisse Pham, *Huawei Will Soon Be Able to Buy from Some U.S. Suppliers Again*, CNN BUS. (Nov. 22, 2019, 2:21 AM), https://www.cnn.com/2019/11/21/tech/huawei-us-licenses/index.html.

[62] Uyghur Human Rights Policy Act of 2020, Pub. L. No. 116–145, § 1, 134 Stat. 648, 652.

[63] *Id.* § 3(2)–(3).

[64] Rollet, *supra* note 59.

[65] *Id.* ("If U.S. allies like the European Union were to join such a new trade regime, the potential to affect China's actual domestic policies would be much greater than by blacklisting a few surveillance companies.").

[66] Keegan Elmer, *EU Calls Out Beijing on Human Rights but Activists Want Harder Line Against China's Xinjiang and Tibet Policy*, S. CHINA MORNING POST (Apr. 10, 2019, 2:30 PM), https://www.scmp.com/news/china/diplomacy/article/3005510/eu-calls-out-china-human-rights-stops-short-pressing-beijing ("European Council President Donald Tusk said the union raised human rights with China, but he did not say which issues were brought up.").

intelligence and surveillance technology to various States in South America and Africa.[67] The widespread use of these advanced surveillance systems promotes the type of monitoring that the Chinese State has used on its population and could arguably increase the chance of serious human rights violations against the population by the State and its powerful corporate allies.

The Chinese State has hired private companies and groups to create virtual accounts, including bot accounts, on social media sites such as Twitter to spread disinformation and to amplify messages beneficial to the interests of the Chinese Community Party.[68] The Chinese State has continually pushed for an increased presence of Communist Party members within the leadership of Chinese private firms, leading to increased alignment of these firms' objectives and policies with those of the State.[69] In 2016, China's leader, Xi Jinping, instructed the top official media organizations in China to modify their platforms and narratives to increase global influence.[70] These concerted efforts to spread Chinese State propaganda and technology, combined with China's position on the U.N. Security Council and overall influence on the global stage, have made it difficult for the international community to hold Chinese corporations liable for their complicity and assistance in the human rights abuses against the Uyghur population of the Xinjiang region.[71]

---

[67] Olivia Enos, *Responding to the Crisis in Xinjiang*, HERITAGE FOUND. (June 7, 2019), https://www.heritage.org/asia/report/responding-the-crisis-xinjiang (citing Arthur Gwagwa & Lisa Garbe, *Exporting Repression? China's Artificial Intelligence Push into Africa*, COUNCIL ON FOREIGN RELS. (Dec. 17, 2018, 10:00 AM); Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, FREEDOM HOUSE (last visited Apr. 7, 2021)) (referencing evidence of Chinese investment and exportation of Chinese surveillance technology in Zimbabwe, Angola, Ethiopia, and Ecuador).

[68] *See* Joyce Huang, *Observers Urge Social Media Platforms to Keep Scrutinizing China-Backed Accounts*, VOICE AM. (Aug. 26, 2019, 11:14 AM), https://www.voanews.com/east-asia-pacific/observers-urge-social-media-platforms-keep-scrutinizing-china-backed-accounts.

[69] *See Freedom in the World 2019: China*, FREEDOM HOUSE, https://freedomhouse.org/country/china/freedom-world/2019 (last visited Apr. 7, 2021) ("In June 2018, regulators pressured private firms listed on the country's stock exchanges to 'strengthen party-building' within their ranks; official sources reported in 2017 that 70 percent of private companies in China had internal party organizations.").

[70] *See* Li Yuan, *China's Soft-Power Failure: Condemning Hong Kong's Protests*, N.Y. TIMES (Aug 20, 2019), https://www.nytimes.com/2019/08/20/business/china-hong-kong-social-media-soft-power.html ("Xinhua, CCTV, Global Times and the rest have bolstered their presence in the United States and elsewhere and taken to the very same social media outlets like Facebook and Twitter that Beijing blocks at home. Some accounts have amassed followers of over 10 million.").

[71] Sophie Richardson, *China's Influence on the Global Human Rights System*, HUM. RTS. WATCH (Sept. 14, 2020, 2:51 PM), https://www.hrw.org/news/2020/09/14/chinas-influence-global-human-rights-system.

B. The Development of International and Transnational Regulations of the Internet and Corporate Conduct Regarding Data Privacy

i. Internet Governance, Data Surveillance, and Corporate Conduct as Addressed by the United Nations, the International Court of Justice, and the International Criminal Court

While there are sparse examples of major international regulations or customs regarding data privacy and corporate liability in the social media context, the U.N. has adopted major initiatives and resolutions regarding data privacy and the use of the internet in general. Given the rapid development of the online sector in the late 20th and early 21st centuries, the U.N. did not take concrete steps to address international legal issues inherent in internet use until the 2000s. In 2001, the U.N. General Assembly passed a resolution endorsing a World Summit on the Information Society (WSIS) in two sessions in 2003 and 2005.[72] This resolution encouraged all state governments, international organizations, non-governmental organizations, and private sector actors to participate in the preparatory process of the WSIS and to participate at the Summit itself.[73] The 2005 WSIS was held in Tunis, and the agenda asked the U.N. Secretary-General to convene the first Internet Governance Forum (IGF) in 2006, which mandated discussion of public policy concerns and emerging issues related to internet governance.[74]

In 2015, the U.N. General Assembly passed a resolution that extended the existing mandate of the IGF for ten years[75] and reaffirmed that "the same rights that people have offline must also be protected online."[76] The Resolution called upon all Member States to review their policies "regarding the surveillance of communications . . . including mass surveillance, with a view to upholding the right to privacy as set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights for States that are party to the Covenant."[77] The Resolution more broadly called on Member States to "ensur[e] the full and effective implementation of all [States'] obligations under international human rights law."[78] Most relevant to this Note, the 2015 Resolution called

---

[72] G.A. Res. 56/183, ¶ 1 (Dec. 21, 2001).

[73] *Id.* ¶¶ 4–5.

[74] World Summit on the Info. Soc'y [WSIS], *Tunis Agenda for the Information Society*, ¶ 72, WSIS-05/TUNIS/DOC/6(Rev. 1)-E (Nov. 18, 2005).

[75] G.A. Res. A.70/125, ¶ 63 (Dec. 16, 2015).

[76] *Id.* ¶ 43.

[77] *Id.* ¶ 46.

[78] *Id.*

upon Member States to cooperate with one another on "transnational issues of information and communications technologies and the use thereof, including capacity-building and cooperation in combating the criminal misuse of the technologies and preventing the use of technology, communications and resources for criminal or terrorist purposes."[79]

While the IFG presents a useful forum for state and non-state actors to meet and discuss current and anticipated public policy issues related to internet governance, systemic issues inherent in existing international legal regimes have arguably made it difficult for states to hold corporate actors accountable for their conduct violating international human rights law (IHRL). One major roadblock to ensuring corporate compliance with the principles of IHRL is that corporate entities do not face international criminal liability under the Rome Statute, which only grants the International Criminal Court (ICC) jurisdiction over "natural persons."[80] While superiors may be held criminally responsible for acts committed by subordinates under the Rome Statute,[81] the option to authorize the ICC to pursue criminal charges directly against corporate entities as juridical persons was rejected during the U.N. talks leading up to the signing of the Rome Statute in July of 1998.[82]

Traditionally, States are the primary actors and subjects under international law, while far fewer guiding treaties and customary international legal rules create individual private liability for breaches of international law.[83] In a 1949 Advisory Opinion, the International Court of Justice (ICJ) explained that while a non-state actor may be "an international person" and thus may be "a subject of international law and capable of possessing international rights and duties," this does not mean that the non-state actor's "legal personality and rights and duties are the same as those of a State."[84] While not a binding decision on state actors, this Advisory Opinion supports the theory that while a non-state organizational actor may have international legal rights and duties as a result of its "capacity to operate upon an international plane."[85] However, it does not necessarily follow that the international legal rules which apply to state actors, specifically those based in custom and general practice, apply equally to non-state actors.

---

[79] *Id.* ¶ 53.

[80] Rome Statute of the International Criminal Court art. 25, July 17, 1998, 2187 U.N.T.S. 90.

[81] *Id.* at art. 28.

[82] David Scheffer, *Corporate Liability Under the Rome Statute*, 57 HARV. INT'L L. J. 35, 38 (2016). At least one scholar has pointed to the "insufficient number of national jurisdictions that held corporations liable under criminal law, as opposed to civil tort liability" as a reason for the rejection. *Id.*

[83] *States in International Law*, BRITANNICA, https://www.britannica.com/topic/international-law/States-in-international-law (last visited Oct. 8, 2020).

[84] Reparation of Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. 174, 179 (Apr. 11).

[85] *Id.*

In 2011, a Special Representative to the Secretary General developed the U.N. Guiding Principles on Business and Human Rights, which was unanimously endorsed by the U.N. Human Rights Council in June of 2011.[86] The Human Rights Council also established an Open-Ended Intergovernmental Working Group to draft a legally binding treaty on business activities by transnational corporations and human rights.[87] This draft treaty specifically invokes the Universal Declaration of Human Rights and "the nine core International Human Rights Instruments" adopted by the U.N., [88] and defines "[h]uman rights violation or abuse" as "any harm committed by a State or a business enterprise . . . against . . . any persons or group of persons . . . including physical or mental injury, emotional suffering, economic loss or substantial impairment of their human rights, including environmental rights."[89] Despite the legal considerations pushing for international legal personality attaching to non-state actors, actual application in international legal frameworks lags due to policy concerns.[90]

ii. Internet Governance, Data Surveillance, and Corporate Conduct as Addressed by Regional Organizations

While the development of comprehensive regulations pertaining to utilization of user data and corporate accountability at the global level remains difficult given clashing interests among the U.N.'s members, practical considerations may indicate that regional and domestic regulatory regimes are better equipped to address these issues. For instance, states who share borders and occupy distinct regions of the world may share common policy interests tied to that region. Furthermore, the development of similar transnational policies and laws by multiple

---

[86] *OHCHR and Business and Human Rights*, U.N. HUM. RTS. OFF. HIGH COMM'R, https://www.ohchr.org/EN/Issues/Business/Pages/BusinessIndex.aspx (last visited Mar. 28, 2021).

[87] *Open-Ended Intergovernmental Working Group on Transnational Corporations and Other Business Enterprises with Respect to Human Rights*, U.N. HUM. RTS. COUNCIL, https://www.ohchr.org/EN/HRBodies/HRC/WGTransCorp/Pages/IGWGOnTNC.aspx (last visited Mar. 28, 2021).

[88] U.N. Open-Ended Intergovernmental Working Grp., Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises, pmbl. (June 8, 2020), https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/Session6/OEIGWG_Chair-Rapporteur_second_revised_draft_LBI_on_TNCs_and_OBEs_with_respect_to_Human_Rights.pdf.

[89] *Id.* at art. 1.2.

[90] Alexandra Garcia, *Corporate Liability for International Crimes: A Matter of Legal Policy Since Nuremberg*, 24 TUL. J. INT'L & COMPAR. L. 97, 129 (2015).

states may facilitate multilateral agreements or even the emergence of customary international law over time.

One regional organization that has arguably developed more effective legal mechanisms relating to internet governance, data use, and corporate liability is the EU. The European Dialogue on Internet Governance (EuroDIG), launched in 2008 and supported by the executive branch of the EU, "fosters dialogue and collaboration with the Internet community on public policy for the Internet."[91] The EuroDIG serves to "support the general objectives of the global Internet Governance Forum," while also facilitating discussions aimed at "overcom[ing] digital divides in Europe."[92] EuroDIG membership "is open to any natural or legal person interested in supporting the purposes of EuroDIG," and the powers of members within the EuroDIG organization depend on the timing of when they joined the Association.[93] Such a structure incentivizes both state and non-state actors to continually engage in EuroDIG discussions to better voice their opinions on certain policy issues and identify common ground.[94]

The most comprehensive internet regulatory scheme by the EU and arguably by any international body, however, is the General Data Protection Regulation (GDPR). Passed in April of 2016 by the European Parliament and Council of the EU, the GDPR aims to "ensure a consistent level of protection" for the privacy and data of "natural persons throughout the [EU]," as well as to "provide legal certainty and transparency for economic operators."[95] While the GDPR suggests that administrative fines should be imposed for infringement of the regulation's provisions, it leaves "the rules on criminal penalties for infringements" of the GDPR to Member States.[96] Furthermore, the GDPR does not apply to the processing of personal data "by competent authorities for . . . the prevention of threats to public security."[97] Thus, should a state actor declare that a threat to public security exists and that circumstances require heavier monitoring of the population's personal data, then the GDPR would arguably not apply.

Despite these weaknesses—allowing state actors to conduct surveillance over individuals in certain situations and limiting criminal accountability for such conduct—the GDPR exerts extraterritorial reach in some situations.[98] Specifically, it may apply to "a controller or processor not established in the Union" when that actor is processing "personal data of data subjects who are in the

---

[91] About EuroDIG, EURODIG, https://www.eurodig.org/index.php?id=74 (last visited Mar. 28, 2021).

[92] *Statutes*, EURODIG SUPPORT ASSOCIATION, § 2 (June 20, 2019), https://www.eurodig.org/about/who-we-are/#tab-eurodig-statutes.

[93] *Id.* § 4.

[94] About EuroDIG, *supra* note 91.

[95] Council Regulation 2016/679, pmbl. ¶ 13, 2016 O.J. (L 119) 3.

[96] *Id.* at pmbl. ¶¶ 148–49.

[97] *Id.* at art. 2(2)(d).

[98] *Id.* at art. 3.

Union," albeit in limited circumstances.[99] The GDPR says that both "controller[s]"—those with "the purposes and means of processing personal data"—as well as a "processor[s]"—those who "process[] personal data on behalf of the controller"—include "natural or legal person[s]," as well as "public authorit[ies]."[100]

As of 2019, critics of the GDPR have noted that while the regulation has found "success as a breach notification law," it has not been as effective "when it comes to imposing fines on companies that fail to adequately protect their customers' data."[101] Additionally, three Member States of the EU have still not fully adapted their national legislation to implement the GDPR.[102] At the national level, Member States of the EU must "set up and allocate powers to the national data protection authorities, lay down rules on specific issues . . . and amend or repeal sectoral legislation with data protection aspects" to satisfy the GDPR.[103] Despite the apparent burdens that the GDPR places on corporations who fall under its purview, the European Commission has argued that the GDPR actually "encourages the development of new technologies while respecting the fundamental right to protection of personal data," as businesses "have started developing . . . new, more privacy-friendly services" and "have promoted respect for personal data as a competitive differentiator and a selling point."[104]

Furthermore, a "growing number of companies" have "extend[ed] . . . the rights created by [GDPR] to their non-EU based customers" in response to increasing concerns worldwide regarding internet security.[105] In addition to the direct reach of the GDPR, the Commission to the European Parliament and the Council has "intensified its engagement with third countries and other international partners" in reaching agreements on internet privacy policies.[106] One example of these agreements, the "EU-Japan mutual adequacy arrangement" that

---

[99] *Id.* at art. 3(2) (explaining that controllers or processors who are "not established in the Union" may be held under the standards of the GDPR when the processing activities of those entities are related to either the offering of goods or services or the monitoring of the behavior of subjects of the EU "as far as their behavior takes place within the Union").

[100] *Id.* at arts. 4(7)–(8).

[101] *See, e.g.*, Josephine Wolff, *How Is the GDPR Doing?*, SLATE: FUTURE TENSE (Mar. 20, 2019, 5:42 PM), https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html (noting that while penalties under the GDPR totaled over fifty-five million euros during the first nine months that the GDPR was in effect, a single fifty million euro fine levied against Google in January of 2019 accounts for nearly 90% of that sum).

[102] *GDPR in Numbers*, EUR. DATA PROT. BD., https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf (May 12, 2018).

[103] *Communication from the Commission to the European Parliament and the Council*, at 3, COM (2019) 374 final (July 24, 2019).

[104] *Id.* at 9 ("For instance, search engines which do not track users or use behavioural advertising are progressively gaining market shares in some Member States.").

[105] *Id.* at 10–11.

[106] *Id.* at 11.

entered into force in February of 2019, "created the world's largest area of free and safe data flows."[107] Member States of the EU have continued to develop similar "adequacy" measures with non-EU States across the globe and to adapt existing "adequacy decisions" with third countries to the newer GDPR framework.[108]

The European Court of Human Rights (ECHR) has also ruled on data privacy and the permissibility of surveillance regimes. In 1978, the ECHR ruled that under the Convention for the Protection of Human Rights and Fundamental Freedoms (CPHRFF), signed by members of the Council of Europe,[109] "Contracting States [to the Convention] may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[110] The ECHR stressed that despite the "certain discretion" that domestic legislatures have when creating surveillance systems, "this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance."[111] In a 2016 ruling, the ECHR explained that the proliferation of digital surveillance tools raises "the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards" that ensure the rights enshrined in the CPHRFF.[112] Given these specific decisions by the ECHR, along with others made pursuant to claims under the CPHRFF, the CPHRFF appears to protect the data rights of citizens of Member States.

One major regional organization in Eurasia, the Shanghai Cooperation Organization (SCO), arguably sacrificed the goals of user data protection and promotion of human rights in favor of promoting political stability and national security. China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan announced the SCO in 2001, signed the SCO Charter in June of 2002, and entered the agreement into force in September of 2003.[113] The SCO Charter expressly endorses "the strengthening of peace and ensuring of security and stability in the region in the environment of developing political multipolarity and economic and information globalization."[114] In 2009, Member States of SCO signed their own Agreement regarding "International Information Security." In

---

[107] *Id.*

[108] *Id.* at 11–12.

[109] Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Apr. 11, 1950, E.T.S. No. 005.

[110] Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) 18 (1978).

[111] *Id.* at 18.

[112] Szabó v. Hungary, App. No. 37138/14, 37 (2016), https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22001-160020%22]}.

[113] *The Shanghai Cooperation Organisation*, SHANGHAI COOP. ORG., http://eng.sectsco.org/about_sco/ (last visited Sept. 1, 2019).

[114] Charter of the Shanghai Cooperation Organization pmbl., June 15, 2001, 2896 U.N.T.S. I-50517.

contrast to the GDPR, this Agreement focuses more heavily on "limiting the spread and use of information weapons threatening defense capacity, national security and public safety"[115] than protecting personal user data. Under the Agreement, SCO Member States exchange "information, analysis and joint assessment of emerging threats to information security, as well as identification, reconciliation and coordination of joint responses to these threats."[116] Furthermore, the Agreement mandates SCO Member States to carry out its provisions "consistent with universally recognized principles and norms of the international law, including . . . respect for human rights."[117]

Critics of the SCO highlighted "human rights concerns raised by SCO structure, policies, and practices," namely those activities by the SCO carried out in the name of counterterrorism.[118] The SCO's "'come as you are' approach of non-interference in internal affairs," as well as its "prioritization of member state stability," garnered it international appeal from states who face internal security threats.[119] The SCO's approach to counter-terrorism reflects China's continual focus on fighting the "Three Evil Forces," typically defined as "terrorism, ethnic separatism, and religious extremism."[120] The SCO's focus has led to "crackdowns and abuses related to individual exercise of fundamental rights and freedoms" including "discrimination against and targeting of ethnic and other vulnerable groups."[121]

Despite the human rights concerns voiced against the SCO, the U.N. has "granted the SCO observer status and continues to pursue expanded cooperation" with the organization, which critics have warned may "contribute to the strengthening of a regional approach that is undermining international human rights."[122] The EU remains more skeptical of the legitimacy of some of the SCO's practices; one resolution from the European Parliament in 2014 recognized "the absence of any formal cooperation mechanism between the SCO and the EU," as well as "divergences in [the EU's and the SCO's] respective normative bases and

---

[115] Agreement on Cooperation in Ensuring International Information Security Between the Member States of the Shanghai Cooperation Organization art. 3(3), June 16, 2009, http://eng.sectsco.org/documents/ (click on "Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO" to download PDF).

[116] *Id.* at art. 5(2).

[117] *Id.* at art. 4(1).

[118] HUM. RTS. IN CHINA, COUNTER-TERRORISM AND HUMAN RIGHTS: THE IMPACT OF THE SHANGHAI COOPERATION ORGANIZATION i (Mar. 2011), https://www.hrichina.org/sites/default/files/publication_pdfs/2011-hric-sco-whitepaper-full.pdf.

[119] *Id.* at iii.

[120] Sam DuPont, *China's War on the "Three Evil Forces"*, FOREIGN POL'Y (July 25, 2007, 8:42 PM), https://foreignpolicy.com/2007/07/25/chinas-war-on-the-three-evil-forces; *see also* HUM. RTS. IN CHINA, *supra* note 118, at iv.

[121] HUM. RTS. IN CHINA, *supra* note 118, at iv.

[122] *Id.* at 7.

outlooks on global issues."[123] A Briefing from the European Parliament Research Service (EPRS) noted that while the SCO Charter mandates "the protection of human rights as an obligation of individual member states under international law," this voiced obligation "is clearly subordinated to the fight against separatist, extremist and terrorist groups."[124] The Briefing further noted that the SCO's focus on combatting these groups involves "the suppression of riots and uprisings, and even peaceful dissent," by the individual member states of the SCO.[125]

Outside observers have called the SCO's stances on internet governance, data surveillance, and the protection of human rights into question. In examining the International Code of Conduct for Information Security proposal that the SCO submitted to the U.N. General Assembly in 2011 and 2015, one NGO argued that "[t]he SCO states may view the Code as a vehicle to redefine application of international human rights law."[126] According to one critic, even after "taking into consideration" suggestions from the international community in 2011, the 2015 Code of Conduct proposal "still raise[d] serious concerns with respect to human rights," as the Code's narrative "emphasize[d] state sovereignty and territoriality in the digital space above all else, and [wa]s dominated by intelligence, national security, and regime stability imperatives."[127] Another critic of the SCO believes that the SCO is forwarding a "proposed norm" under international law through its vision of data surveillance and internet governance under the proposed Code.[128] They further believe that reactions to the acts of States such as Russia and China by actors such as the United States help perpetuate this "proposed norm" of territorial sovereignty in the digital space.[129] In short, the internet governance and data surveillance stances of the SCO and of its most influential member states, namely China, reflect a view of international human rights law that opposes the pro-individual rights view held by the EU, ECHR, and Council.

---

[123] European Parliament Resolution of 12 March 2014 on Pakistan's Regional Role and Political Relations with the EU (2013/2168(INI)), EUR. PARL. DOC. P7 TA(2014)0208 N(14) (2014).

[124] GISELA GRIEGER, EUR. PARLIAMENTARY RSCH. SERV., BRIEFING: THE SHANGHAI COOPERATION ORGANIZATION 4 (2015), http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564368/EPRS_BRI%282015%29564368_EN.pdf.

[125] *Id.* at 4.

[126] Sarah McKune, *An Analysis of the International Code of Conduct for Information Security*, CITIZEN LAB (Sept. 28, 2015), https://citizenlab.ca/2015/09/international-code-of-conduct/.

[127] *Id.*

[128] Milton Mueller, *A Farewell to Norms*, INTERNET GOVERNANCE PROJECT (Sept. 4, 2018), https://www.internetgovernance.org/2018/09/04/a-farewell-to-norms/.

[129] *Id.* (arguing that the regulation of internet speech by the United States in reaction to social media tactics by Russia helped reinforce the proposed norm by the SCO that States should promote their territorial sovereignty over the digital space).

iii. Internet Governance, Data Surveillance, and Corporate Conduct as Addressed by Transnational Laws and Policies

Several States have domestic legislation that imposes sanctions on foreign individuals and entities that are involved in human rights abuses. The Global Magnitsky Human Rights Accountability Act (Magnitsky Act), one major piece of such legislation, was passed by the United States Congress in 2016.[130] Under the Magnitsky Act as passed, foreign persons[131] could be sanctioned for "gross violations of internationally recognized human rights" based on credible evidence.[132] Further, the U.S. President may sanction corporations for committing human rights violations themselves, as well as for "act[ing] as an agent of or on behalf of a foreign person" who commits these violations.[133] In 2017, President Donald Trump modified the Magnitsky Act via executive order to broaden the scope of liability for foreign actors, namely changing the "gross" standard for violations to "serious."[134] Under the Magnitsky Act, the United States can bar foreign persons, both individuals and entities, from entering the country and can "block" transactions of property within the United States.[135]

The European Parliament of the EU, taking count of the Magnitsky Act and similar "Magnitsky laws" that enable governments to impose targeted sanctions, passed a resolution urging adoption of similar standards for all its Member States, as well as at the EU level.[136] In addition to providing deterrence for potential human rights abusers, some groups have noted that the Magnitsky Act and similar transnational laws provide incentives to foreign governments to improve their own accountability.[137]

---

[130] Global Magnitsky Human Rights Accountability Act, Pub. L. No. 114-328, §§ 1261–65 (codified as amended in scattered sections of 22 U.S.C.).

[131] *Id.* § 1262(1). Note that "foreign persons" was defined by CFR §595.304 to mean "any citizen or national of a foreign state . . . or any entity not organized solely under the laws of the United States or existing solely in the United States" until that regulation was removed with its Part of the Code in 2020. *See* Removal of Terrorism Sanctions Regulations, 85 Fed. Reg. 13,746 (Mar. 10, 2020) (to be codified at 31 C.F.R. pt. 595). As such, the term is currently undefined.

[132] *Id.* §1263(a)(1).

[133] *Id.* §1263(a)(2).

[134] Exec. Order. No. 13,818, 31 C.F.R. § 583, app. A (2018).

[135] Global Magnitsky Human Rights Accountability Act § 1263(b).

[136] Resolution on a European Human Rights Violations Sanctions Regime, EUR. PARL. DOC. P8 TA(2019/0215) (2019).

[137] *See, e.g.*, *The US Global Magnitsky Act: Questions and Answers*, HUM. RTS. WATCH (Sept. 13, 2017, 10:40 AM), https://www.hrw.org/news/2017/09/13/us-global-magnitsky-act ("By cooperating with the US on Global Magnitsky investigations, foreign leaders can show that they will not tolerate human rights abusers in their own countries.").

While laws such as the Magnitsky Act seem to offer a valid avenue for pursuing claims against foreign corporations and actors for human rights abuses, the ability for domestic courts to hear individual claims against foreign corporations remains in question. In 2018, the U.S. Supreme Court held that the Alien Tort Statute (ATS), which allows U.S. district courts to hear civil claims by aliens for torts "committed in violation of the law of nations or a treaty of the United States,"[138] should not extend liability to foreign corporations.[139] The U.S. Supreme Court had previously held that the ATS does not grant relief "for violations of the law of nations occurring outside the United States."[140]

In 2017, France passed a law that holds corporations liable under French law for human rights abuses committed by those companies, their subcontractors, and their suppliers.[141] The law mandates that certain companies, depending on their size and their presence in France, implement an "effective vigilance plan."[142] Penalties are imposed only in the instance that the corporation does not adopt "due diligence measures."[143] However, the penalty provision of the French law was struck down in March of 2017 by the French Constitutional Council due to vague language in the statute.[144] While observers have noted that other portions of the Constitutional Council's decision have deprived the French law of some of its "fundamental provisions," they also note that the current version's enforcement mechanisms have allowed interested parties to request compensation under French common civil law.[145] The domestic laws' limitation of domestic courts represent an ongoing struggle to reconcile the vastly different foundations and principles between domestic and international bodies of law, as well as the ability for domestic courts to successfully adjudicate claims against foreign defendants.

Many other States are currently developing laws that seek to ensure corporate accountability for human rights abuses in these contexts. In April of 2019, the United Kingdom announced the introduction of an independent regulator to

---

138 28 U.S.C.A. § 1350 (2019).

139 Jesner v. Arab Bank, PLC, 138 S.Ct. 1386, 1403 (2018) ("[A]bsent further action from Congress it would be inappropriate for courts to extend ATS liability to foreign corporations.").

140 Kiobel v. Royal Dutch Petroleum Co., 133 S.Ct. 1659, 1669 (2013).

141 Loi 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre [Law 2017-399 of March 27, 2017 Relating to the Duty of Care of Parent Companies and Contractors], JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Mar. 23, 2017, p. 1–2.

142 *Id.* at p. 1.

143 *Id.* at p. 2.

144 Conseil constitutionnel [CC] [Constitutional Court] decision No. 2017-750DC, Mar. 23, 2017, Rec. 13, ¶ 14 (Fr.).

145 Sandra Cossart, Opinion, *What Lessons Does France's Duty of Vigilance Law Have for Other National Initiatives?*, BUS. & HUM. RTS. RES. CTR. (June 27, 2019), https://www.business-humanrights.org/en/blog/what-lessons-does-frances-duty-of-vigilance-law-have-for-other-national-initiatives/.

ensure that social media companies and tech firms "protect their users and face tough penalties if they do not comply."[146] Under the proposed rules, companies could face substantial fines and senior management individuals could face personal liability.[147] Germany also passed its own "Network Enforcement Law" in 2017, which holds social media companies that have at least two million users in Germany liable for fines up to fifty million euros if they fail to delete comments and posts deemed to violate German law.[148] Both the German and British laws ensure harsh penalties for companies that violate domestic law, yet both apparently lack extraterritorial reach and have faced criticism for their elements of censorship.[149] Admittedly, domestic laws from various states do not perfectly ensure that foreign corporate entities can truly be held accountable for their complicity in or active perpetration of human rights violations. Nonetheless, they can be deployed relatively quickly and are more targeted in scope than existing international and other multilateral legal accountability mechanisms.

---

[146] Press Release, *UK to Introduce World First Online Safety Laws* (Apr. 8, 2019), https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws.

[147] Matthew S. Schwartz, *U.K. Regulators Propose Broad Social Media Regulations to Counter 'Online Harms'*, NPR (Apr. 8, 2019, 8:18 PM), https://www.npr.org/2019/04/08/711091689/u-k-regulators-propose-broad-social-media-regulations-to-counter-online-harms.

[148] Soraya Sarhaddi Nelson, *With Huge Fines, German Law Pushes Social Networks to Delete Abusive Posts*, NPR (Oct. 31, 2017, 7:44 AM), https://www.npr.org/sections/parallels/2017/10/31/561024666/with-huge-fines-german-law-pushes-social-networks-to-delete-abusive-posts.

[149] *Id.* ("[C]ritics of the new law call it an assault on free speech that is more likely to increase censorship than to decrease fake news and hate speech.").

III. ANALYSIS

A. Existing International Law, Transnational Accountability Mechanisms, and the Human Rights Violations in Xinjiang

i. China's Ability to Prevent Meaningful Action by U.N. Bodies and Growing Soft Power Severely Hinder International Legal Action Against Chinese Corporations and the Chinese State on the Global Level for the Atrocities in Xinjiang

China's position on the U.N. Security Council, as well as its ideological and economic influence over authoritarian-leaning regimes worldwide,[150] has made it difficult to develop a global consensus among states against the extensive human rights violations committed by the Chinese State and by corporations operating in the Xinjiang region. China and other nations on the U.N. Security Council have not reached a consensus over the treatment of the Uyghur and other minority groups in Xinjiang, and some states have rejected forms of U.N. action in Xinjiang that could validate China's justifications for the treatment of these minority groups.[151]

Under the U.N. Charter, action by the Security Council requires affirmative votes of nine of the fifteen members, including all five of the permanent members, for all non-procedural matters.[152] The Security Council has the power to impose sanctions in order to "give effect to its decisions,"[153] and through 2020 had sanctioned nearly 300 entities.[154] This has included sanctions against privately-owned companies who committed violations of Security Council

---

[150] *See Rule by Fear: 30 Years After Tiananmen Square: Hearing Before the S. Comm. on Foreign Rels.*, 116th Cong. 4–8 (2019) (statement of Christopher Walker, Vice President, Studies & Analysis, National Endowment for Democracy).

[151] *U.S., Germany Slam China at U.N. Security Council over Xinjiang: Diplomats*, REUTERS (July 2, 2019, 7:06 PM), https://www.reuters.com/article/us-china-usa-rights/us-germany-slam-china-at-un-security-council-over-xinjiang-diplomats-idUSKCN1TX2YZ ("Last month the United States, Britain and other western countries objected to a visit by the United Nations counterterrorism chief to Xinjiang, concerned the visit would validate China's argument that it was tackling terrorism.").

[152] U.N. Charter art. 27, ¶ 3.

[153] *Id.* at art. 41.

[154] *The UN Security Council,* COUNCIL ON FOREIGN RELS. (Sept. 16, 2020), https://www.cfr.org/backgrounder/un-security-council.

resolutions.[155] But given China's position as a permanent member of the Security Council,[156] it can veto any sort of non-procedural action that the Security Council could take to stop the ongoing human rights abuses in Xinjiang, which includes blocking any potential U.N. Security Council sanctions against violating Chinese companies.

In any instance, while the U.N. Security Council holds the power to take action against threats to international peace and security,[157] responsibility for the protection of equal rights and self-determination of the citizens of U.N. member States falls on the General Assembly and the Economic and Social Council.[158] Although the Security Council "at times[] deals with grave human rights violations," these investigations often are tied to "conflict areas."[159] Thus, even if the Security Council could recommend action against the Chinese State and Chinese corporations for the human rights abuses in Xinjiang, China may have a valid argument that the U.N. Security Council lacks the power to handle this sort of dispute.

Within the U.N. General Assembly, there are competing views on the situation in Xinjiang and its legality under international law. In October of 2019, a faction of twenty-three countries raised concerns over the human rights abuses at the U.N. General Assembly and called upon China to uphold its international obligations and to provide access to Xinjiang for international monitors.[160] In response, Belarus made a statement on behalf of fifty-four countries, voicing approval of China's "counter-terrorism" program in Xinjiang.[161] This represented an increase from the thirty-seven nations that supported China's Xinjiang policies in July of 2019.[162]

In its 2018 report on China, the U.N. Human Rights Council Working Group on the Universal Period Review called upon China to implement the recommendations made by the Committee on the Elimination of Racial Discrimination in

---

[155] *See*, *e.g.*, U.N. Sec. Council, Sanctions Against Butembo Airlines (BAL) (Mar. 29, 2007) (sanctioning a "[p]rivately-owned airline" for providing assistance to illegal armed groups in violation of Security Council resolutions).

[156] U.N. Charter art. 23, ¶ 1.

[157] U.N. Charter art. 39.

[158] U.N. Charter art. 60.

[159] *Protect Human Rights*, U.N., https://www.un.org/en/sections/what-we-do/protect-human-rights/ (last visited Apr. 9, 2021).

[160] Ben Westcott & Richard Roth, *UN Members Issue Dueling Statements over China's Treatment of Uyghurs in Xinjiang*, CNN (Oct. 29, 2019, 11:33 PM), https://www.cnn.com/2019/10/29/asia/china-xinjiang-united-nations-intl-hnk/index.html.

[161] *Id.* ("'The joint statement spoke positively of the results of counter-terrorism and de-radicalization measures in Xinjiang and noted that these measures have effectively safeguarded the basic human rights of people of all ethnic groups,' representatives for Belarus said in a press release.").

[162] *Id.*

August 2018 regarding Xinjiang.[163] The report also noted China's stance that the State "resolutely opposed and would never accept the practice of using human rights as an excuse to interfere in its internal affairs and undermine its sovereignty and territorial integrity."[164] Unsurprisingly, China declined to implement these recommendations and instead suggested that monitors and journalists could only enter Xinjiang in accordance with Chinese law, while affirming the State's strong opposition to "interference in its sovereignty and internal affairs under any pretext."[165]

This conditioning of human rights on Chinese domestic security interests should draw condemnation from top U.N. officials given the principles of equal rights and self-determination espoused in Article 55 of the U.N. Charter.[166] However, U.N. Secretary-General Antonio Guterres has refrained from commenting on growing evidence of the abuses in Xinjiang and instead has supported China's justifications for the surveillance and detention regime in Xinjiang.[167] Within the U.N., China has used its membership on the Economic and Social Council's NGO Committee to block U.N. accreditation for those NGOs critical of China.[168] China's position on the Security Council, as well as its active role in the U.N. as the head of the Department of Economic and Social Affairs and the second-largest funder of the U.N. regular budget,[169] have weakened the efforts of those U.N. Member States who oppose the ongoing human rights violations in Xinjiang. As China continues to find support from other autocratic regimes worldwide,

---

[163] Hum. Rts. Council, Rep. of the Working Group on the Universal Periodic Review of China in its Thirty-First Session, ¶ 28.23, U.N. Doc. A/HRC/40/6 (2018) (France calling on China to "[i]mplement all of the recommendations of the Committee on the Elimination of Racial Discrimination of August 2018 regarding Xinjiang, particularly on putting an end to mass internments in camps, and invite the Office of the United Nations High Commissioner for Human Rights and special procedure experts").

[164] *Id.* ¶ 27.

[165] Hum. Rts. Council, Rep. of the Working Group on the Universal Periodic Review of China in its Thirty-First Session Addendum, ¶ 28.22, U.N. Doc. A/HRC/40/6/Add.1 (2018).

[166] *See* U.N. Charter art. 55(c) (requiring promotion of "universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion").

[167] Daily Press Briefing by Stéphane Dujarric, Spokesman for the Secretary-General, Office of the Spokesperson for the Secretary-General (Nov. 18, 2019), https://www.un.org/press/en/2019/db191118.doc.htm ("[The Secretary-General's] position on the situation [in Xinjiang] is that there needs to be full respect for the unity and territorial integrity of China, condemnation of terrorist attacks, as no cause or grievances can justify them.").

[168] *The Costs of International Advocacy*, HUM. RTS. WATCH (Sept. 5, 2017), https://www.hrw.org/report/2017/09/05/costs-international-advocacy/chinas-interference-united-nations-human-rights.

[169] Courtney J. Fung, *Is China's Influence at the United Nations all it's Cracked Up to Be?*, WASH. POST (Oct. 7, 2019, 5:00 AM), https://www.washingtonpost.com/politics/2019/10/07/is-chinas-influence-united-nations-all-that-its-cracked-up-be/.

China's position in the U.N. has allowed it to use this growing support to legitimize its views despite the State's blatant disregard for the foundational human rights principles of the U.N.

ii. Current International Conventions and Legal Instruments Relating to Protection of Data Rights and Accountability of Corporations Are Insufficient in Deterring Human Rights Violations by China and Chinese Companies

China has signed but not ratified the International Covenant on Civil and Political Rights (ICCPR),[170] which obligates State parties to ensure equal rights for all individuals "without distinction of any kind."[171] The ICCPR prohibits parties who are acting "[i]n time of public emergency" to discriminate against individuals solely on the ground of certain statuses, including religion.[172] Thus, if China were a party to the ICCPR, the surveillance mechanisms deployed by the Chinese State against the Uyghur Muslim population of Xinjiang would violate China's obligations under the convention. China's justifications national security justifications would not avoid violation, as Chinese corporations detain Uyghur Muslims based on the presence of religious imagery and messages on their social networks.[173]

China has neither signed nor ratified the 1976 Optional Protocol to the ICCPR,[174] which allows parties to bring claims to the Human Rights Committee set up by the Covenant.[175] However, even under the Protocol, communications to the Committee are only admissible when they communicate a violation of the

---

[170] *Status of Ratification Interactive Dashboard*, U.N. HUM. RTS. OFF. OF THE HIGH COMM'R (Feb. 9, 2021), https://indicators.ohchr.org/ (click on the "Select a treaty" dropdown menu and select "International Covenant on Civil and Political Rights").

[171] International Covenant on Civil and Political Rights art. 2, Dec. 19, 1966, 999 U.N.T.S. 171.

[172] *Id.* at art. 4, ¶ 1.

[173] *See* Darren Byler, *How Technology Liberated China's Uighur Minority–and then Trapped Them*, QUARTZ (Oct. 1, 2019), https://qz.com/1719581/technology-liberated-chinas-uighur-minority-and-then-trapped-them/ (explaining that Chinese authorities have "mapped out [a] person's social network and history of Islamic practice, both in their local community and online," in assessing security threats).

[174] *Status of Ratification Interactive Dashboard*, *supra* note 170 (click on the "Select a treaty" dropdown menu and select "Optional Protocol to the International Covenant on Civil and Political Rights").

[175] *See* Optional Protocol to the International Covenant on Civil and Political Rights arts. 2, 5, Dec. 16, 1966, 999 U.N.T.S. 302 (allowing parties to overcome domestic remedy exhaustion requirements "where the application of the remedies is unreasonably prolonged").

ICCPR by the State, not violation by a private party such as a private company.[176] However, the Committee has interpreted the ICCPR as requiring States to regulate and adjudicate private corporate acts in order to protect against abuse.[177] Thus, the Human Rights Committee accepts communications where the State has "failed to take steps to prevent, investigate, punish or redress wrongdoing by private actors, including business enterprises."[178]

In the case of Xinjiang, were China party to the ICCPR and its Optional Protocol, communications from repressed minority groups to the Human Rights Committee would be admissible, given that the Chinese State not only forces Chinese companies to comply with its abusive policies but also places Chinese Communist Party officials within the management structures of rising Chinese companies.[179] Furthermore, the Human Rights Committee can hear communications under the Optional Protocol to the ICCPR regarding violations of the ICCPR not only in the territory of a State party, but also regarding abuses against individuals outside the State's territory.[180] However, the Committee has not explicitly addressed these situations where a corporation acts on the State's behalf outside the national territory of the State in question.[181]

While the above provisions of the ICCPR and the Optional Protocol to the ICCPR provide a route to holding private corporations accountable for human rights violations, China has indicated that its ratification of the ICCPR depends on "whether relevant conditions in China are in place."[182] Given that China signed the ICCPR in 1998, NGOs have called into question when these "relevant conditions" would be "in place."[183] Thus, so long as the ICCPR would allow the Human Rights Committee to investigate human rights violations committed by corporate actors influenced by a State, it remains highly unlikely that China will ratify the ICCPR. Regardless, given that China repeatedly advocates for limiting

---

[176] John G. Ruggie (Special Rapporteur on Human Rights and Transnational Corporations and Other Business Enterprises), *State Responsibilities to Regulate and Adjudicate Corporate Activities Under the United Nations' Core Human Rights Treaties*, 4 (June 2007).

[177] *Id.* at 19.

[178] *Id.* at 4.

[179] *See Freedom in the World 2019: China*, *supra* note 69. *But see* State Responsibilities to Regulate and Adjudicate Corporate Activities under the United Nations' Core Human Rights Treaties, *supra* note 176, p. 54, ¶ 179 ("It is unclear under which conditions the HRC considers that a company, while not part of the State apparatus, may nevertheless be considered to engage directly the responsibility of the State because it acts under the State's direction, control or instructions.").

[180] State Responsibilities to Regulate and Adjudicate Corporate Activities Under the United Nations' Core Human Rights Treaties, *supra* note 176, ¶ 147, at 46.

[181] *Id.* ¶ 155, at 48.

[182] Rep. of the Working Group on the Universal Periodic Review of China in its Thirty-First Session Addendum, *supra* note 165, ¶ 28.5.

[183] *See* Sophie Richardson, *Inconvenient Truths at China's UN Rights Review*, HUM. RTS. WATCH (Mar. 13, 2019, 5:28 AM), https://www.hrw.org/news/2019/03/13/inconvenient-truths-chinas-un-rights-review.

interpretations of human rights law to accommodate national security and sovereignty concerns,[184] the Chinese State would likely provide bad faith arguments to skirt its obligations under the ICCPR even if it were a party.

While a few multilateral legal instruments exist that effectively ensure the protection of user data from digital surveillance, these international legal obligations cannot currently hold Chinese tech and social media corporations liable for aiding the Chinese State in committing the human rights violations in Xinjiang. The GDPR does have extraterritorial application outside of the EU to organizations that either offer goods and services to people in the EU or monitor the behavior of individuals in the EU.[185] Specifically, if a corporation uses web tools that track cookies or IP addresses of those who visit the corporation's website from EU countries, then that corporation falls under the scope of the GDPR.[186] However, those involved in administering the GDPR have questioned how this extraterritorial reach based on monitoring would actually be enforced.[187] Furthermore, even under the GDPR a member state may limit the data rights of individuals by domestic legislative measure when necessary to safeguard national security or other crucial state interests.[188]

While both the GDPR and the the Chinese Cybersecurity Law (CSL) have similar conceptions of what constitutes "personal data,"[189] the CSL focuses heavily on tying the ideas of cybersecurity and data protection together.[190] Given China's aforementioned justifications for the surveillance and abuse of the Uyghur people in Xinjiang relating to national security concerns and anti-terrorism initiatives, China's promotion of data protection in the CSL rings hollow.

The SCO's approach to promoting strong cybersecurity mechanisms that ensure political stability, as previously discussed, reflect China's view that national political and security interests trump equal treatment of individuals regardless of

---

[184] Abbas Faiz, *China is Building a Global Coalition of Human Rights Violators to Defend its Record in Xinjiang – What is its Endgame?*, CONVERSATION (July 18, 2019, 9:05 AM), https://theconversation.com/china-is-building-a-global-coalition-of-human-rights-violators-to-defend-its-record-in-xinjiang-what-is-its-endgame-120546 ("China's approach has been to engage with the UN's human rights bodies to impose its own narrative, which misinterprets sovereignty as being distinct and above human rights.").

[185] Ben Wolford, *Does the GDPR Apply to Companies Outside of the EU?*, GDPR.EU, https://gdpr.eu/companies-outside-of-europe/ (last visited Nov. 25, 2019).

[186] *Id.*

[187] *See id.* ("Practically speaking, it's unclear how strictly this provision will be interpreted or how brazenly it will be enforced.").

[188] *See* Council Regulation 2016/679, *supra* note 95, at art. 23 (restrictions must "respect[] the essence of the fundamental rights and freedoms and is a necessary and proportionate measure").

[189] *See* Galaad Delval & Zhong Lin, *GDPR Matchup: China's Cybersecurity Law*, INT'L ASSOC. OF PRIV. PRO. (June 28, 2017), https://iapp.org/news/a/gdpr-matchup-chinas-cybersecurity-law/ (comparing the definition of personal data in Article 4.1 of the GDPR with the definition of personal information given in Article 76.5 of the CSL).

[190] *Id.*

their religious affiliation. The State parties to the SCO submitted a letter to the U.N. General Assembly in 2015, proposing an International Code of Conduct for application of "new information and communication technologies."[191] The proposal promotes recognition that "the rights of an individual in the offline environment must also be protected in the online environment," and then references Article 19 of the ICCPR,[192] which concerns the freedom of expression.[193] Both Article 19 and SCO's proposal to the U.N. assert that the freedom of expression may be curtailed "[f]or the protection of national security or of public order."[194] Nevertheless, China is not a party to the ICCPR,[195] and thus its participation in endorsing that portion of the 2015 proposed Code of Conduct appears to be in bad faith.

Additionally, the 2015 proposed Code of Conduct emphasizes a State's "right to independent control of information and communications technology goods."[196] This reflects China's intensive regulation of its domestic tech companies, specifically its control over what information Chinese platforms should censor or what digital materials are targeted for surveillance by the Chinese State. Given the Chinese State's heavy regulation of its domestic corporate actors in the tech and social media industries and the continued drive of the Communist Party's leadership to suppress political dissent and cement regime stability, it seems highly unlikely that the China would currently become a party to an instrument such as the GDPR.

The U.N. Human Rights Council contains a working group that has been developing an international convention "to regulate, in international human rights law, the activities of transnational corporations and other business enterprises."[197] China specifically voted in favor of establishing the working group.[198]

---

[191] Permanent Reps. of China, Kaz., Kyrg., Russ., Taj. & Uzb., Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015) [hereinafter Letter to the Secretary General].

[192] *Id.*

[193] International Covenant on Civil and Political Rights, *supra* note 171, at art. 19(2).

[194] *Id.* at art. 19(3)(b); Letter to the Secretary General, *supra* note 191, ¶ 7.

[195] *Status of Ratification Interactive Dashboard*, *supra* note 170.

[196] Letter to the Secretary General, *supra* note 191, ¶ 5.

[197] *Open-Ended Intergovernmental Working Group on Transnational Corporations and Other Business Enterprises with Respect to Human Rights*, U.N. HUM. RTS. COUNCIL, https://www.ohchr.org/en/hrbodies/hrc/wgtranscorp/pages/igwgontnc.aspx (last visited Apr. 10, 2021).

[198] Human Rights Council Res. 26/9, U.N. Doc. A/HRC/RES/26/9 (July 14, 2014) ("*In favour:* Algeria, Benin, Burkina Faso, China, Congo, Côte d'Ivoire, Cuba, Ethiopia, India, Indonesia, Kazakhstan, Kenya, Morocco, Namibia, Pakistan, Philippines, Russian Federation, South Africa, Venezuela (Bolivarian Republic of), Viet Nam; *Against*: Austria, Czech Republic, Estonia, France, Germany, Ireland, Italy, Japan, Montenegro, Republic of Korea, Romania, the former Yugoslav Republic of Macedonia, United Kingdom of Great Britain and Northern Ireland, United States of America; *Abstaining:* Argentina, Botswana, Brazil, Chile, Costa

The draft report of this legally binding instrument states that its regulation would apply to all business activities, "including but not limited to transnational corporations and other business enterprises that undertake business activities of a transnational nature."[199] Article 5 of the proposed instrument would oblige member States to ensure that their domestic laws require all persons conducting business activities to respect human rights and prevent human rights violations and abuses.[200] Furthermore, the draft instrument defines "[b]usiness activities" as "including but not limited to productive or commercial activity . . . including activities undertaken by electronic means."[201] However, the definition of "[h]uman rights violation or abuse" under Article 1 of the instrument does not present an exhaustive list[202] and therefore the exact situations where corporations would be held liable under the instrument remains unclear. Thus, even under the draft instrument it remains uncertain to what extent Chinese corporations could be held liable for the surveillance and censoring mechanisms in Xinjiang.

Even if China was potentially liable, there's a question as to whether China would become party to such a multilateral legal instrument in the first place. Article 12 of the proposed instrument allows defendants to refuse recognition and enforcement by a court with jurisdiction after a claim has been brought "where the judgment is manifestly contrary to the [public order] of the Party in which its recognition is sought."[203] The draft also affirms that State obligations under the proposed instrument should be carried out "in a manner consistent with, and fully respecting, the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States."[204] Thus, even if China became a party to this instrument, it likely would continue to shield its corporations from international liability on the grounds of sovereignty and non-intervention in domestic affairs.

Rica, Gabon, Kuwait, Maldives, Mexico, Peru, Saudi Arabia, Sierra Leone, United Arab Emirates[.]").

[199] U.N. Open-Ended Intergovernmental Working Grp. on Transnat'l Corps. & Other Bus. Enters. with Respect to Hum. Rts., Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and Other Business Enterprises, art. 3 § 1, (July 16, 2019), https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/Session6/OEIGWG_Chair-Rapporteur_second_revised_draft_LBI_on_TNCs_and_OBEs_with_respect_to_Human_Rights.pdf.

[200] *Id.* at art. 5(1).

[201] *Id.* at art. 1(3).

[202] *See id.* at art. 1(2) (defining violations as "acts or omissions in the context of business activities, against any person or group of persons, individually or collectively, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their human rights, including environmental rights").

[203] *Id.* at art. 12(9)(c).

[204] *Id.* at art. 14(1).

As evidenced above, existing and developing multilateral legal instruments relating to corporate accountability for human rights violations ineffectively ensure liability for those Chinese corporate actors that have aided the Chinese State in monitoring and detaining Uyghurs in Xinjiang on the basis of their religious and ethnic affiliations. The primacy of non-interference in domestic matters echoes in the majority of multilateral instruments that could apply to this situation, and China has increasingly cultivated a consensus of States that support the primacy of sovereignty over the protection of human rights and individual privacy.

B. Additional Considerations in Developing a Consensus on International Standards for Corporate Liability and Human Rights Instruments that Reach Corporate Actors Who Are Shielded by Powerful States

China's soft power on the international stage has severely hampered international consensus against China's use of domestic corporate actors to monitor the Xinjiang region and to persecute minority groups in the region. As previously discussed, various States have begun implementing their own versions of the Global Magnitsky Act, the transnational law that holds private individuals and corporations accountable for human rights violations.[205] While that Act in its current form can only prevent transactions between domestic and foreign companies,[206] should enough States adopt similar provisions they could increasingly restrict the ability of Chinese companies involved in the abuses in Xinjiang from conducting business outside of China. These types of measures would most effectively pressure those Chinese companies with major markets outside of China, such as Hikvision Digital Technology and Zhejiang Dahua Technology.[207] Even then, many Chinese firms are partially—or fully—controlled by Chinese State actors, such as the China Electronics Technology Corporation.[208] Some argue that sanctions by the United States have not driven China towards reforming its policies, but rather encourage the Chinese State to become more involved in

---

[205] *The US Global Magnitsky Act: Questions and Answers*, *supra* note 137.

[206] *Id.*

[207] *See* Olivia Carville & Jeremy Kahn, *China's Hikvision Has Probably Filmed You*, BLOOMBERG (May 24, 2019, 10:25 AM), https://www.bloomberg.com/news/articles/2019-05-22/china-s-hikvision-weighed-for-u-s-ban-has-probably-filmed-you ("Together, the two companies control one-third of the global market for video surveillance, according to a report by Deutsche Bank AG, with their cameras securing businesses, airports, schools and government offices in the U.S.—and around the world.").

[208] *See* Buckley & Mozur, *supra* note 5 ("Hikvision is a major manufacturer of video surveillance equipment, with customers around the world and across Xinjiang, where its cameras have been installed at mosques and detention camps. C.E.T.C. owns about 42 percent of the company through subsidiaries.").

growing the domestic Chinese tech market.[209] Thus, the pressure from these Magnitsky-type sections would not necessarily deter these types of firms as they might deter entirely-private firms.

Another issue with Magnitsky-type legal regimes is that the imposition of sanctions tend to harm the profits of domestic companies from the imposing State.[210] Additionally, Chinese firms can circumvent sanctions implemented under laws such as the Global Magnitsky Act by instead buying products from States that have not yet imposed similar laws.[211] Thus, while these types of sanctions may harm Chinese tech firms who wish to do business outside of China, they only do so to the extent that numerous States have imposed similar laws that effectively block a specific market for Chinese firms.

Given that organizations such as the EU have avoided concrete measures against China and Chinese firms for the human rights abuses in Xinjiang,[212] States must take initiative to craft domestic laws that specifically target these Chinese firms. However, States have been hesitant to pressure domestic companies from engaging in business in Xinjiang outside of formal sanction regimes.[213] Global marketplaces have additionally complicated efforts to harm the profits of Chinese tech companies that have participated in the abuses in Xinjiang, as Chinese companies can rely on complex chains of suppliers and vendors to avoid direct transactions that would violate sanction regimes.[214] Thus, States continue

---

[209] Reva Goujon, *By Mixing Tech and Human Rights Sanctions on China, the White House Crosses the Rubicon*, STRATFOR WORLDVIEW (Nov. 1, 2019, 9:30 GMT), https://worldview.stratfor.com/article/tech-human-rights-us-sanctions-china-trade-war.

[210] *See* Jenny Leonard & Ian King, *Five Months After Huawei Export Ban, U.S. Companies Are Confused*, L.A. TIMES (Oct. 24, 2019, 5:00 AM), https://www.latimes.com/business/story/2019-10-24/huawei-export-ban-us-companies-confusion (reporting that tech leaders and their lawyers argued for months in closed-door meetings with Trump administration officials that the blacklisting of Huawei—one of their biggest customers—is detrimental to their businesses).

[211] *See id.* ("One of the industry's main arguments for allowing shipments of non-national security-sensitive items is that Huawei can buy some of those components from competitors around the world, including South Korea, Japan and Taiwan.").

[212] *See* Rollet, *supra* note 59.

[213] *See, e.g., Germany's Maas: China Should Comply with Human Rights Obligations*, DEUTSCHE WELLE (Nov. 26, 2019), https://www.dw.com/en/germanys-maas-china-should-comply-with-human-rights-obligations/a-51416033 ("Chancellor Angela Merkel's chief spokesman, Steffen Seibert, told reporters on Monday that 'in a situation in which there are no sanctions in place . . . it is solely a decision of any given company' whether it wants to continue operating in the region.").

[214] *See*, *e.g.*, Rosalind Adams & Ryan Mac, *Amazon, Apple, and Google Are Distributing Products from Companies Building China's Surveillance State*, BUZZFEED NEWS (Nov. 4, 2019, 1:57 PM), https://www.buzzfeednews.com/article/rosalindadams/apple-amazon-google-apps-blacklist-china-xinjiang ("On Amazon, there are more than 700 products from Dahua or Dahua Technology ranging from security cameras to camera mounts to wires. While most, if not all, of the products are sold by third-party vendors, many are stored and shipped by Amazon.").

to face a variety of challenges related to the complexity of contemporary global markets, as well as the Chinese State's heavy drive to grow its domestic tech industry, in formulating their own sanctions regimes to address the human rights violations in Xinjiang.

Rapid technological advancement in the past two centuries further complicates the situation, as it has debatably left international law to catch up to these trends after serious international issues have emerged. Specifically, in the case of Xinjiang, it appears that very few international legal instruments effectively reach the digital surveillance and complex censorship tactics employed by Chinese corporations in furtherance of the Chinese Communist Party's goals. The emergence of social media in the twenty-first century specifically has called into question the state-centric approach to international law, as individuals worldwide have increasingly pushed for the right to express themselves and to maintain data privacy in the face of increasing government monitoring of social networks for political purposes.

IV. CONCLUSION

The situation in Xinjiang presents unique challenges to those international actors who seek to hold Chinese tech corporations accountable for their complicity and active aid in the human rights abuses against the Uyghur people by the Chinese State. These challenges cumulatively prevent expedited multilateral efforts to stop the abuses in Xinjiang, and instead force States to work from the ground up to form a consensus against the actions of these Chinese corporations. Only through building a strong consensus, facilitated through passing domestic laws and discussions with NGOs and important multinational corporations in the tech industry, can States effectively hold these Chinese corporations accountable for their role in the human rights abuses in Xinjiang.

First, China's immense influence on the global stage and role within the U.N. prevents meaningful inquiries into the violation of human rights in Xinjiang. China can formally block many forms of action through its position on the U.N. Security Council and through its participation in human rights-oriented U.N. bodies. Additionally, China's soft power, which China utilizes through foreign investment in and the sharing of surveillance technology with other authoritarian regimes, have resulted in a pushback against human rights protectors that frames China's Xinjiang abuses in terms of territorial sovereignty and the right to conduct internal affairs. States that seek to form consensus at the U.N. level against the surveillance and detention regime in Xinjiang must continue to push for the promotion of human rights over potential economic gain and political interests.

Second, existing multilateral legal instruments relating to corporate accountability and data protection cannot adequately address the conduct of the Chinese

tech firms that participate in the ongoing abuses in Xinjiang. China is not a party to many major multilateral regimes that would entail obligations to respect the rights of the Uyghur people, such as the ICCPR. Furthermore, international law, particularly in the form of customary international law, has not yet caught up to rapid development of technology in the twenty-first century and the recent emergence of social media as a major form of communication for societies across the globe. While some organizations, such as the EU, have developed their own regulatory regimes that aim to protect user data and ensure corporate accountability, others such as the SCO have developed competing conceptions of "data privacy" that make individual rights subordinate to the government's political interests.

Lastly, the interconnectedness of contemporary global markets has incentivized companies to continue to engage with Chinese tech firms in Xinjiang and with the Chinese market on the whole. China's rapidly developing domestic tech industry has resulted in an export of Chinese tech worldwide, and multinational corporations are incentivized to participate in the Chinese market due to its sheer size. Without broad multilateral efforts to boycott products from these Chinese tech companies and to refrain from engaging in the Chinese market, sanctions on the individual State level often end up harming that State's own markets, as Chinese companies can simply find another trade partner that lacks these formal sanctions.

Given these challenges, I believe effective action against the Chinese tech firms that facilitate the human rights abuses in Xinjiang starts at the individual level. States must pass their own domestic laws that specifically criminalize and punish foreign corporations for the types of conduct that have led to the human rights abuses in Xinjiang. Specifically, States must promote the protection of the freedom of expression and data privacy over economic gain and should restrict trade with foreign corporations to the extent that these corporations do not respect these individual rights.

Domestic laws such as the Global Magnitsky Act address human rights abuses by corporate actors to some extent, but these laws are not yet widely adopted. Corporations in the tech industry, including those that host social media platforms, must themselves develop internal codes of conduct that obligate corporate management to protect human rights over making a profit off human rights abuses. States cannot work at the U.N. level alone to develop these instruments, as China's position on the Security Council and ability to garner support from authoritarian regimes prevents meaningful consensus within U.N. bodies that could push for accountability. States should continue to engage in discussions with NGOs and tech corporations as to how to best protect human rights while conducting foreign businesses and should encourage other States to join in on these discussions.

States must actively and harshly rebuke the common "national security" and "anti-terrorism" justifications for these abuses as forwarded by authoritarian States such as China. While States should show restraint in directing the conduct

of its own domestic corporate actors in response to the crisis in Xinjiang, they should frame policies and sanction regimes against Chinese tech corporations involved in Xinjiang in terms of their own human rights and international legal obligations. Through developing a strong consensus against the corporate abuses in Xinjiang, States can not only more effectively negotiate for multilateral legal instruments that address corporate accountability for human rights abuses, but also may encourage the development of customary international law over time that addresses the type of conduct in question.