BUSINESS AND HUMAN RIGHTS

Findings

- As the Chinese Communist Party and government engage in increasingly egregious human rights violations, domestic and international businesses are increasingly at risk of complicity in abuses committed by the Chinese government. Of particular concern are: reports that companies are involved in the government's suppression of ethnic minorities in the Xinjiang Uyghur Autonomous Region (XUAR), including through the use of forced labor; companies' complicity in government surveillance of individuals throughout China; and companies engaging in censorship on behalf of Chinese authorities.
- In the XUAR, the actions of the Party and government may constitute crimes against humanity according to scholars and rights groups, and companies that work in the region are at great risk of complicity in those crimes. Experts have documented the rapid expansion of a network of mass internment camps in which authorities have arbitrarily detained over a million individuals from predominantly Muslim ethnic minority groups. Commercial entities have been directly involved in the construction of these camps and supplied them with a wide range of goods and services. The company **Hangzhou Hikvision Digital Technology,** in particular, has supplied surveillance systems to the camps as part of a public-private partnership with XUAR authorities. U.S.-based firms such as **Intel, Ambarella,** and **Nvidia** reportedly continue to supply Hikvision with critical components. According to a March 2019 report, the **California State Teachers' Retirement System** and the **New York State Teachers' Retirement System** both continued to own Hikvision stock.
- The Commission observed numerous reports this past year of forced labor associated with government repression of ethnic minority groups in the XUAR. In some cases, detainees performed forced labor within the camps. In other cases, detainees were "released" in order to perform forced labor. In still other cases, XUAR authorities reportedly assigned individuals from ethnic minority groups to forced labor directly, without first sending them to the camps. A Wall Street Journal investigation found that materials from firms using forced labor in the XUAR had entered the supply chains of major international clothing companies including **Adidas, H&M, Nike,** and **Patagonia.**
- Chinese security authorities continued to work with domestic companies to expand the reach and analytical power of government surveillance systems. Chinese technology firms **ZTE, Hikvision, iFlytek, Huawei Technologies, SenseTime, Megvii, CloudWalk, Yitu,** and **Tiandy** all reportedly sold technology to Chinese authorities for use in surveillance systems. This surveillance is used to target rights advocates and others whom the government views as a threat. For example, police in at least 16 provinces and regions were reportedly using artificial intelligence (AI) to track the movement of Uyghurs, an ethnic minority group.

- Companies in China collect large amounts of data on Chinese citizens and are required under Chinese law to make this data available to authorities. In the wake of rising domestic concerns over data collection and misuse, the government has already begun to revise recent regulations governing consumer data collection. While the government has punished companies over the collection of consumer data in some instances, the government has simultaneously expanded its own data collection powers.
- Chinese government restrictions on freedom of expression increased this past year, and companies—particularly tech companies—were both targets and enablers of Chinese government censorship. For example, **Tencent's WeChat**—a ubiquitous social media app in China—regularly filters and censors content and turns over user information to authorities. In 2018, media reports revealed that **Google** was developing a censored version of its search engine in an attempt to re-enter the Chinese market. Following employee protests and media attention, Google's Vice President for Government Affairs and Public Policy informed the Congress in July 2019 that Google had "terminated" the search engine project.

Recommendations

Members of the U.S. Congress and Administration officials are encouraged to:

- Take the necessary steps to prohibit the export of U.S. goods and services to Chinese entities—including government agencies and companies—that have been directly involved in building and supplying the system of internment camps in the Xinjiang Uyghur Autonomous Region (XUAR). Specifically, the video surveillance company **Hangzhou Hikvision Digital Technology,** which has supplied the camps with surveillance equipment and is complicit in state surveillance of ethnic minorities more generally, should be placed on the Entity List of the Bureau of Industry and Security (BIS) within the U.S. Department of Commerce.
- Impose Global Magnitsky sanctions on both Chinese government officials carrying out severe human rights abuses in the XUAR as well as the companies directly complicit in those abuses. U.S. Customs and Border Protection should examine the import of goods made in the XUAR—or containing materials made in the XUAR—and determine whether such imports violate Section 1307 of the Tariff Act of 1930 (19 U.S.C. 1307).
- The Department of Labor should update its list of goods produced with child labor or forced labor to reflect the recent reports of forced labor in the XUAR.
- Hold public hearings and private meetings with companies from their districts to raise awareness of the risks of complicity in human rights abuses that U.S. companies working in China may face, including complicity in possible crimes against humanity in the XUAR; the possibility of goods made with forced labor entering supply chains; and the use of AI technology and

surveillance equipment to monitor human rights advocates, religious believers, and ethnic minorities.

○ Encourage companies in their districts to engage in appropriate due diligence with regard to potential complicity in human rights abuses. For additional resources on best practices, companies may consult the UN Guiding Principles on Business and Human Rights, the Organization for Economic Cooperation and Development (OECD) Guidelines for Multinational Enterprises, and the OECD Due Diligence Guidance for Responsible Business Conduct.

BUSINESS AND HUMAN RIGHTS

Introduction

During the Commission's 2019 reporting year, the Chinese Communist Party and government engaged in increasingly egregious human rights violations, as detailed by international human rights organizations and in the other sections of this report.[1] In this environment, domestic and international businesses are directly complicit in or at risk of complicity in human rights abuses committed by the Chinese government, including the severe repression of minority groups in the Xinjiang Uyghur Autonomous Region (XUAR), government surveillance of citizens without adequate privacy protections, and government censorship. Technology companies, in particular, play a major role in government surveillance and censorship, and Human Rights Watch warned companies operating in China that "the authorities might deploy [their] technology to commit serious abuses."[2] Although the Chinese government requires companies to comply with domestic laws and regulations that infringe on internationally recognized rights such as the right to privacy and freedom of expression, the UN Guiding Principles on Business and Human Rights state that businesses have a responsibility to respect human rights and should seek to avoid "contributing to adverse human rights impacts . . .."[3] Whereas the preceding sections of this report examine in detail Chinese government violations of human rights and relevant international human rights standards, this section focuses on the risk domestic and international companies face of complicity in these human rights violations.

Corporate Involvement in Possible Crimes Against Humanity in the XUAR

The actions of the Chinese Communist Party and government in the XUAR may constitute crimes against humanity[4] according to scholars and rights groups.[5] This past year, experts documented the expansion of a network of mass internment camps in which authorities have arbitrarily detained over a million individuals from predominantly Muslim ethnic minority groups.[6] Outside the camps, members of ethnic minority groups in the XUAR face extreme levels of surveillance, restrictions on freedom of movement, and forced political indoctrination.[7] Companies that work in the XUAR are at great risk of complicity in the human rights abuses being committed in the region.[8] [For more information on human rights violations in the XUAR, including a discussion of possible crimes against humanity committed by Chinese authorities, see Section IV—Xinjiang.]

COMPANIES USING FORCED LABOR IN THE XUAR

The Commission observed numerous reports this past year of forced labor associated with government repression of ethnic minority groups in the XUAR. In some cases, detainees performed forced labor in factories within internment camps.[9] In other cases, authorities released individuals from the camps to perform forced labor in factories elsewhere in the XUAR.[10] In still other cases,

XUAR authorities reportedly assigned individuals from ethnic minority groups to forced labor directly, without first sending them to the camps.[11] Radio Free Asia (RFA) reported in January 2019 that authorities had also sent Uyghurs and Kazakhs from the XUAR to other provinces in China for forced labor.[12] Comments from the president of the China National Textile and Apparel Council in March 2018 suggested that textile manufacturers, in particular, were working with XUAR authorities to exploit detainee labor.[13] More recent reports found that authorities used tax exemptions and subsidies to encourage Chinese garment manufacturers to move production to the XUAR.[14] German scholar Adrian Zenz warned that "[s]oon, many or most products made in China that rely at least in part on low-skilled, labor-intensive manufacturing, could contain elements of involuntary ethnic minority labor from Xinjiang."[15] [For more information on forced labor in the XUAR and elsewhere in China, see Section II—Human Trafficking.]

Products reportedly produced with forced labor by current and former camp detainees included:

- textiles, such as yarn, clothing, gloves, bedding, and carpet;[16]
- electronics, including cell phones and computer hardware and software;[17]
- food products, including noodles and cakes;[18]
- shoes;[19]
- tea;[20] and
- handicrafts.[21]

Companies that used forced labor in the XUAR this past year included:

- Hetian Taida Apparel,[22] a supplier of the U.S. company Badger Sportswear;[23]
- Yili Zhou Wan Garment Manufacturing Company;[24]
- Zhihui Haipai Internet of Things Technology Company;[25]
- Urumqi Shengshi Hua'er Culture Technology Limited Company;[26]
- Litai Textiles;[27]
- Huafu Fashion Company, whose yarn reportedly entered the supply chains for H&M, Esprit, and Adidas;[28]
- Esquel Group, headquartered in Hong Kong, which reportedly supplied clothing to Calvin Klein, Tommy Hilfiger, Nike, and Patagonia;[29] and
- Cofco Tunhe Company, which supplied tomato paste to Kraft Heinz and Campbell Soup, and sugar to Coca-Cola.[30]

Clothing Made With Forced Labor Imported Into United States

In January 2019, U.S. company **Badger Sportswear**[31] (Badger) stopped importing clothing from **Hetian Taida Apparel** (Hetian Taida), following media reports that the clothing was made with forced labor by internment camp detainees.[32] The Associated Press (AP) tracked shipments from Hetian Taida workshops located within an internment camp to Badger, and the U.S.-based Worker Rights Consortium independently confirmed that the Hetian Taida factory supplying Badger was located inside a camp.[33] The chairman of Hetian Taida confirmed to the AP that his workforce included "trainees" from the camp.[34] Badger said it relied on the U.S.-based social compliance nonprofit **Worldwide Responsible Accredited Production** (WRAP) to certify that its suppliers met certain standards.[35] Following media reports, WRAP conducted its own investigation, concluding that "this facility is not engaged in the use of forced labor."[36] WRAP later admitted to the AP, however, that it had not visited the facility in question, but rather a separate Hetian Taida workshop located elsewhere.[37]

SURVEILLANCE STATE IN THE XUAR

Outside the network of extrajudicial internment camps, ethnic minority groups in the XUAR faced near-constant government surveillance in their daily lives,[38] in violation of the internationally recognized right to privacy.[39] Numerous companies—both Chinese and international—have facilitated what Human Rights Watch describes as "Orwellian surveillance" in the XUAR.[40]

- In October 2018, the video surveillance research firm IPVM provided evidence that the video surveillance company **Hangzhou Hikvision Digital Technology** was directly involved in the construction, operation, and ongoing maintenance of the Integrated Joint Operations Platform (IJOP) in the XUAR.[41] Human Rights Watch has described the IJOP as a "predictive policing" system that aggregates and analyzes large amounts of individuals' data, flagging "those it deems potentially threatening."[42] In addition to tracking them, authorities may arbitrarily detain individuals flagged by the IJOP in the internment camps or other detention facilities.[43] Hikvision also reportedly contracted with local XUAR authorities to build surveillance systems to install in mosques in some localities in the XUAR as part of a public-private partnership.[44]
- Despite Hikvision's involvement in both the XUAR's network of extrajudicial camps and the IJOP, foreign suppliers such as **Intel, Ambarella,** and **Nvidia** reportedly sold computer processing chips and graphics chips to Hikvision, and the U.S. data storage company **Seagate** provided the company with "custom storage solutions" for its surveillance systems, according to a November 2018 Financial Times report.[45] Foreign Policy further reported in March 2019 that the U.S.-based company **Amax,** which provides advanced computing technology, had formed a partnership with Hikvision.[46] Hikvision is listed on the Shenzhen stock exchange and is 41.88 percent owned by two subsidiaries of the Chinese state-owned enterprise **China Electronics Technology Corporation** (CETC).[47] CETC is

also involved in managing government surveillance systems in the XUAR, including the IJOP.[48]

- Hikvision was one of the Chinese companies that index provider **MSCI** included in its emerging markets index, which means that funds investing in the index are investing in Hikvision.[49] MSCI announced plans in February 2019 to quadruple the weight of mainland Chinese shares in the index.[50] According to a March 2019 Financial Times article, the **California State Teachers' Retirement System** and the **New York State Teachers' Retirement System** both owned stock in Hikvision.[51] In addition, U.S. public relations firms **Burson-Marsteller**[52] and **Mercury Public Affairs** are registered with the U.S. Department of Justice as foreign agents working on behalf of Hikvision in the U.S.[53]
- In February 2019, a cybersecurity researcher discovered that the Chinese firm **SenseNets** had left a database tracking over 2.5 million people in the XUAR exposed online.[54] The database tracked individuals' GPS coordinates—seemingly in real time—and also contained government identification numbers, dates of birth, photos, home addresses, and employers.[55] According to experts, the information in this database suggested that authorities in the XUAR were working with SenseNets to monitor residents.[56]
- Bloomberg and the Financial Times reported that **SenseTime** had set up a "smart policing" joint venture in the XUAR with Urumqi-based **Leon Technology** (Leon) called **Xinjiang SenseTime Leon Technology.**[57] According to Leon's website and the company's page on a job-listing website, among Leon's main customers were XUAR government agencies, including the XUAR public security bureau.[58] In March 2019, SenseTime sold its stake in the joint venture with Leon, possibly to avoid negative publicity in preparation for its planned initial public offering (IPO).[59] According to Bloomberg, with investors such as **Qualcomm, Fidelity International,** and **Alibaba,** SenseTime was "the world's most valuable AI startup."[60] A May 2019 BuzzFeed News investigation found that private equity firms **IDG Capital** and **Silver Lake** both owned shares in SenseTime.[61] Those firms' clients reportedly included 14 public pension funds.[62]
- Reports emerged this past year that XUAR authorities purchased a video management system from **Infinova,** a U.S.-based company that is listed on the Shenzhen stock exchange, for use in urban surveillance systems in the XUAR.[63] According to IPVM, XUAR authorities have purchased the company's surveillance technology in the past.[64]
- In April 2019, the Wall Street Journal reported that U.S. firms, including **Boeing** and **Carlyle Group,** had "indirectly facilitated" the Chinese government's use of American-made satellites to aid in communications during protests and strife in the XUAR in 2009.[65] The Hong Kong-based intermediary that sold the satellite bandwidth to Chinese authorities, **AsiaSat,** "declined to comment directly" when asked if police in the XUAR continued to use the satellites.[66]

OTHER COMMERCIAL CONNECTIONS TO XUAR AUTHORITIES

The Commission observed additional instances of connections between companies and XUAR authorities that raised human rights concerns. For example, the U.S.-based firm **Thermo Fisher Scientific** sold DNA analysis equipment to XUAR authorities until February 2019, ending sales following criticism from Human Rights Watch (HRW) and members of the U.S. Congress.[67] According to the New York Times, procurement documents showed that Chinese authorities intended for some of Thermo Fisher's equipment to be used by XUAR police.[68] A 2017 HRW article highlighted Thermo Fisher's sales of DNA sequencers to XUAR police, with HRW's China Director calling the mass, involuntary collection of DNA from Uyghurs in the region "a gross violation of international human rights norms."[69] In addition, in January 2019, the Hong Kong-based security services company **Frontier Services Group** (FSG) announced on its website that it had signed an agreement with local XUAR officials to build a training facility in Kashgar prefecture, XUAR.[70] The announcement, since removed, noted that the agreement was part of a "strategic cooperation framework agreement" (*zhanlue xiezuo kuangjia xieyi*) between the state-owned company **CITIC Group,** which owns controlling shares in FSG, and the Xinjiang Production and Construction Corps, a Han-Chinese led paramilitary institution that operates across the XUAR.[71] FSG's American co-founder, Erik Prince, who remains a minority shareholder and deputy chairman of the board, claimed "no knowledge" of the company's plans to build a training center in the XUAR.[72]

Commercial Firms' Role in Government Data Collection and Surveillance Across China

EVOLVING REGULATORY REGIME

Chinese law allows the government to collect personal data from companies without adequate protections for the internationally recognized right to privacy.[73] For example, the PRC Cybersecurity Law requires companies to store user data inside mainland China[74] and to provide technical support to authorities conducting criminal investigations or "protecting state security,"[75] without specifying what such technical support entails.[76] The PRC National Intelligence Law similarly requires entities operating in China—including companies—to provide support and assistance to authorities engaged in "intelligence work" without defining what the government considers "intelligence work."[77]

In September 2018, the Ministry of Public Security issued implementing provisions that further detailed the government's authority under the Cybersecurity Law.[78] The new provisions allow police to inspect data centers, internet service providers, and others, providing for both on-site and remote inspections and allowing police to copy "relevant information" from the companies they inspect.[79] Experts note that companies typically must comply with government demands to provide information.[80] Chapter 4 of the implementing regulations stipulates potential criminal penalties for failure to comply.[81]

In the wake of rising domestic concerns over data collection and misuse, the government has already begun to revise recent regulations governing consumer data collection.[82] Observers noted that while the government has punished companies over the collection of consumer data in some instances, the government has simultaneously expanded its own data collection powers—in some cases leading to conflicting guidance for businesses over whether and when to retain user data.[83]

SOCIAL CREDIT SYSTEM

The Chinese government continued to work with Chinese companies to develop and implement a social credit system that aimed to aggregate and monitor the data that the government and companies collect. Legal scholars and observers warned that the system could increase the government's capacity for social control and potentially violate the internationally recognized rights to privacy, due process, and freedom of expression.[84] In 2014, the State Council released an outline for the creation of a national social credit system by 2020 to measure and improve the credibility of government agencies, organizations, and individuals.[85] All Chinese individuals and organizations must now have a unique social credit code, including multinational companies operating in China.[86] Private companies such as **Ant Financial** also offer private credit scoring services that collect large amounts of customer data.[87] While these services are separate from the government system, the government has the authority to access the companies' data.[88] In the case of Ant Financial's **Sesame Credit,** the company is reportedly providing information directly to the entity that oversees the government's social credit system.[89]

CONTINUED EXPANSION OF SURVEILLANCE NETWORKS

Chinese security authorities continued to work with domestic companies to expand the reach and analytical power of government surveillance systems. In February 2019, the Chinese Communist Party Central Committee called for the expansion of the rural surveillance system dubbed "Sharp Eyes."[90] According to the Nikkei Asian Review, numerous Chinese firms have supplied equipment and services to the government for the Sharp Eyes project, including **Hikvision, ZTE, iFlytek, Inspur, Huawei Technologies,** and **Alibaba Group Holding.**[91] In addition to the Sharp Eyes surveillance project, Chinese technology firms **SenseTime, Megvii,** and **Tiandy** all reportedly sold technology to Chinese authorities for use in other surveillance systems.[92] For example, SenseTime sold artificial intelligence (AI) technology to police in China in the form of SenseTotem and SenseFace surveillance systems.[93] In April 2019, the New York Times revealed that police departments in at least 16 provinces and regions were using AI to track the movement of Uyghurs, an ethnic minority group.[94] Chinese companies **CloudWalk, Megvii, Yitu,** and **SenseTime** assisted authorities in this surveillance.[95] The head of China equity strategy for Credit Suisse noted that for many Chinese AI firms, their "biggest business" was government surveillance projects.[96] As one human rights advocate noted, while the Chinese government claims these surveillance projects target criminals, "police treat those that exercise

basic civil liberties like peaceful assembly or freedom of association as criminals."[97]

U.S. firms have also assisted in the development of Chinese government surveillance systems. According to a November 2018 Wall Street Journal report, the U.S. chipmaker **Nvidia** has sold chips to SenseTime.[98] Nvidia has also sold chips to **Hikvision,** one of the Chinese firms that has been integral to the construction of government surveillance systems.[99] The U.S. consulting firm **McKinsey & Company** reportedly assisted local governments in China to implement "smart cities" surveillance systems.[100] In the words of one expert, these "smart cities" projects are "about political control."[101]

Role of Commercial Firms in Government Censorship

Chinese government restrictions on freedom of expression increased this past year, and companies—particularly tech companies—were both targets and enablers of Chinese government censorship. The international non-governmental organization Freedom House called the Chinese government "the worst abuser of internet freedom in 2018,"[102] and Human Rights Watch reported that the government continued to censor "politically sensitive information" online.[103] The PRC Cybersecurity Law requires companies to monitor content their customers create or share, censor content that violates laws and regulations, and report such content to authorities.[104] New regulations,[105] censorship campaigns,[106] and increasing restrictions on the use of virtual private networks (VPNs)[107] this past year have further circumscribed online expression. In 2018, regulators reportedly shut down over 6,000 websites.[108] From January 3 to 21, 2019, the Cyberspace Administration of China shut down 733 websites and 9,382 mobile apps, and deleted over 7 million pieces of online information.[109] [For more information on censorship in China, see Section II—Freedom of Expression.]

Faced with the possibility of lost revenue and other forms of punishment, both domestic and international companies engaged in self-censorship. For example, **Tencent's WeChat**—a ubiquitous social media app in China—regularly filters and censors content and turns over user information to authorities.[110] In 2018, online news outlet The Intercept revealed that **Google** was developing a censored version of its search engine, called "Project Dragonfly," in an attempt to re-enter the Chinese market.[111] Work on the project appeared to end in late 2018 following employee protests and media attention.[112] Google's Vice President for Government Affairs and Public Policy told the Senate Judiciary Committee in July 2019 that Google had "terminated" Project Dragonfly.[113]

Not only do companies engage in self-censorship, censorship itself can be a lucrative business in China. The online version of the Party-run newspaper People's Daily, **People.cn,** contracts with companies such as the news aggregator **Jinri Toutiao** to censor content that contravenes government censorship directives.[114] Revenue from People.cn's censorship services reportedly rose 166 percent in 2018.[115] Another censorship service, **Rainbow Shield,** owned by the company **Beyondsoft,** employs over 4,000 people in multiple cities to review online content.[116] In Chengdu municipality, Sichuan province, 160 Beyondsoft employees reportedly monitor a single news-aggregating app for politically sensitive con-

tent.[117] [For more information on censorship in China, see Section II—Freedom of Expression.]

Notes to Section II—Business and Human Rights

[1] Freedom House, "China," in *Freedom in the World 2019,* February 2019; Human Rights Watch, "China," in *World Report 2019: Events of 2018,* 2019, 135–36.

[2] Sophie Richardson, Human Rights Watch, "Thermo Fisher's Necessary, but Insufficient, Step in China," February 22, 2019.

[3] UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, HR/PUB/11/04, June 16, 2011, principle 13.

[4] Rome Statute of the International Criminal Court, adopted by the United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, A/CONF.183/9, July 17, 1998, entry into force July 1, 2002, art. 7.

[5] Kate Cronin-Furman, "China Has Chosen Cultural Genocide in Xinjiang—For Now," *Foreign Policy,* September 19, 2018; Kate Cronin-Furman, "About Me," Personal Website of Kate Cronin-Furman, accessed April 18, 2019; Uyghur Human Rights Project, "Universal Children's Day 2018: China Must Reunite Uyghur Children and Parents. Forcible Placement of Children of Living Parents in State-Run Facilities Constitutes a Crime against Humanity," November 19, 2018; Gene A. Bunin, "Detainees Are Trickling Out of Xinjiang's Camps," *Foreign Policy,* January 18, 2019; Michael Caster, "At Davos, the Message of 'Globalization 4.0' Must Include a Rebuke of China's Ethnic Cleansing in Xinjiang," *Hong Kong Free Press,* January 21, 2019; Global Centre for the Responsibility to Protect, "The Persecution of the Uighurs and Potential Crimes against Humanity in China," April 2019.

[6] See, e.g., Stephanie Nebehay, "1.5 Million Muslims Could Be Detained in China's Xinjiang: Academic," *Reuters,* March 13, 2019; Adrian Zenz, "Xinjiang's Re-Education and Securitization Campaign: Evidence from Domestic Security Budgets," *China Brief,* Jamestown Foundation, November 5, 2018; Fergus Ryan, Danielle Cave, and Nathan Ruser, "Mapping Xinjiang's 'Re-Education' Camps," International Cyber Policy Centre, Australian Strategic Policy Institute, November 1, 2018; Human Rights Watch, "China," in *World Report 2019: Events of 2018,* 2019, 142. For information from the previous reporting year, see CECC, *2018 Annual Report,* October 10, 2018, 273–83.

[7] Human Rights Watch, "China," in *World Report 2019: Events of 2018,* 2019, 142; Amnesty International et al., "Joint Statement Calling for Xinjiang Resolution at the United Nations Human Rights Council," February 13, 2019.

[8] See, e.g., Eva Dou and Chao Deng, "Western Companies Get Tangled in China's Muslim Clampdown," *Wall Street Journal,* May 16, 2019; Human Rights Watch, "China's Algorithms of Repression," May 1, 2019.

[9] Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018; Emily Feng, "Forced Labour Being Used in China's 'Re-Education' Camps," *Financial Times,* December 15, 2018; Dake Kang, Martha Mendoza, and Yanan Wang, "US Sportswear Traced to Factory in China's Internment Camps," *Associated Press,* December 19, 2018.

[10] Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018; Emily Feng, "Forced Labour Being Used in China's 'Re-Education' Camps," *Financial Times,* December 15, 2018; Dake Kang, Martha Mendoza, and Yanan Wang, "US Sportswear Traced to Factory in China's Internment Camps," *Associated Press,* December 19, 2018.

[11] Eva Dou and Chao Deng, "Western Companies Get Tangled in China's Muslim Clampdown," *Wall Street Journal,* May 16, 2019; Adrian Zenz, "Beyond the Camps: Beijing's Grand Scheme of Forced Labor, Poverty Alleviation and Social Control in Xinjiang," SocArXiv, July 12, 2019, 1–4; Sophie McNeill et al., "Cotton On and Target Investigate Suppliers after Forced Labour of Uyghurs Exposed in China's Xinjiang," *Australian Broadcasting Corporation,* July 16, 2019. For the definition of forced labor, see International Labour Organization, ILO Convention (No. 29) Concerning Forced or Compulsory Labour, June 28, 1930, art. 2.1; International Labour Organization, "Ratifications of CO29–Forced Labour Convention, 1930 (No. 29)," accessed August 28, 2019. Article 2.1 defines forced or compulsory labor as "all work or service which is exacted from any person under the menace of any penalty and for which the said person has not offered himself voluntarily." China has not ratified this convention.

[12] "Neidi gu Xinjiang Hasakeren yaoqiu xue Hanyu ru Dang" [Inland China employs Kazakhs from Xinjiang, asks them to learn Chinese and join the Party], *Radio Free Asia,* January 22, 2019.

[13] Sun Ruizhe, China National Textile and Apparel Council, "Sun Ruizhe fenxiang shi da hangye fazhan redian" [Sun Ruizhe shares ten major industry developments], reprinted in China Cotton Textile Association, March 4, 2018; Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018.

[14] Eva Dou and Chao Deng, "Western Companies Get Tangled in China's Muslim Clampdown," *Wall Street Journal,* May 16, 2019; Adrian Zenz, "Beyond the Camps: Beijing's Grand Scheme of Forced Labor, Poverty Alleviation and Social Control in Xinjiang," SocArXiv, July 12, 2019, 8–10.

[15] Adrian Zenz, "Beyond the Camps: Beijing's Grand Scheme of Forced Labor, Poverty Alleviation and Social Control in Xinjiang," SocArXiv, July 12, 2019, 2.

[16] See, e.g., Eva Dou and Chao Deng, "Western Companies Get Tangled in China's Muslim Clampdown," *Wall Street Journal,* May 16, 2019; Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018; Nathan VanderKlippe, "'I Felt Like a Slave:' Inside China's Complex System of Incarceration and Control of Minorities," *Globe and Mail,* March 31, 2019.

[17] Li Zaili, "Camps for Uyghurs, 'Schools' or Jails? Exclusive Report, Photos, and Footage from Bitter Winter," *Bitter Winter,* November 12, 2018; Emily Feng, "Forced Labour Being Used in China's 'Re-Education' Camps," *Financial Times,* December 15, 2018; "Neidi gu Xinjiang

Hasakeren yaoqiu xue Hanyu ru Dang" [Inland China employs Kazakhs from Xinjiang, asks them to learn Chinese and join the Party], *Radio Free Asia,* January 22, 2019.

[18] Li Zaili, "Uyghur Women Forced to Labor in Camp," *Bitter Winter,* September 28, 2018; Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018.

[19] Emily Feng, "Forced Labour Being Used in China's 'Re-Education' Camps," *Financial Times,* December 15, 2018.

[20] Ibid.

[21] Li Zaili, "Uyghur Women Forced to Labor in Camp," *Bitter Winter,* September 28, 2018.

[22] Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018.

[23] Badger Sportswear is a part of Founder Sport Group which is owned by CCMP Capital Advisors LP. "About Us," Badger Sport, accessed September 6, 2019; Iris Dorbian, "CCMP to Buy Uniforms Maker Badger Sportswear," The PE Hub Network, August 23, 2016.

[24] "Businesses in China's Xinjiang Use Forced Labor Linked to Camp System," *Radio Free Asia,* January 1, 2019; Nathan VanderKlippe, "'I Felt Like a Slave:' Inside China's Complex System of Incarceration and Control of Minorities," *Globe and Mail,* March 31, 2019; "Yili Zhuo Wan Garment Manufacturing Co., Ltd.," Alibaba.com, accessed April 9, 2019.

[25] "Neidi gu Xinjiang Hasakeren yaoqiu xue Hanyu ru Dang" [Inland China employs Kazakhs from Xinjiang, asks them to learn Chinese and join the Party], *Radio Free Asia,* January 22, 2019.

[26] Sophie McNeill et al., "Cotton On and Target Investigate Suppliers after Forced Labour of Uyghurs Exposed in China's Xinjiang," *Australian Broadcasting Corporation,* July 16, 2019.

[27] Ibid.

[28] Eva Dou and Chao Deng, "Western Companies Get Tangled in China's Muslim Clampdown," *Wall Street Journal,* May 16, 2019.

[29] Ibid.

[30] Ibid.

[31] Badger Sportswear is a part of Founder Sport Group which is owned by CCMP Capital Advisors LP. "About Us," Badger Sport, accessed September 6, 2019; Iris Dorbian, "CCMP to Buy Uniforms Maker Badger Sportswear," The PE Hub Network, August 23, 2016.

[32] "Sourcing Update," Founder Sport Group (previously Badger Sport), accessed April 10, 2019; Martha Mendoza and Yanan Wang, "US Apparel Firm Cuts Off Chinese Factory in Internment Camp," *Associated Press,* January 10, 2019.

[33] Dake Kang, Martha Mendoza, and Yanan Wang, "US Sportswear Traced to Factory in China's Internment Camps," *Associated Press,* December 19, 2018; Martha Mendoza and Yanan Wang, "US Apparel Firm Cuts Off Chinese Factory in Internment Camp," *Associated Press,* January 10, 2019.

[34] Dake Kang, Martha Mendoza, and Yanan Wang, "US Sportswear Traced to Factory in China's Internment Camps," *Associated Press,* December 19, 2018.

[35] Chris Buckley and Austin Ramzy, "China's Detention Camps for Muslims Turn to Forced Labor," *New York Times,* December 16, 2018.

[36] Arthur Friedman, "WRAP Says Chinese Factory Accused of Using Forced Labor Is Compliant," *Sourcing Journal,* December 24, 2018.

[37] Martha Mendoza and Yanan Wang, "US Apparel Firm Cuts Off Chinese Factory in Internment Camp," *Associated Press,* January 10, 2019.

[38] See, e.g., "An Internment Camp for 10 Million Uyghurs: Meduza Visits China's Dystopian Police State," *Meduza,* October 1, 2018; Sophie Richardson, Human Rights Watch, "Thermo Fisher's Necessary, but Insufficient, Step in China," February 22, 2019.

[39] Universal Declaration of Human Rights, adopted and proclaimed by UN General Assembly resolution 217A (III) of December 10, 1948, art. 12; International Covenant on Civil and Political Rights (ICCPR), adopted by UN General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23, 1976, arts. 17; United Nations Treaty Collection, Chapter IV, Human Rights, International Covenant on Civil and Political Rights, accessed May 29, 2019. China has signed but not ratified the ICCPR. See also UN Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, A/HRC/37/62, October 25, 2018, para. 4; UN General Assembly, Resolution Adopted by UN General Assembly on December 18, 2013: 68/167. The Right to Privacy in the Digital Age, A/RES/68/167, January 21, 2014.

[40] Sophie Richardson, Human Rights Watch, "Thermo Fisher's Necessary, but Insufficient, Step in China," February 22, 2019.

[41] Charles Rollet, "Evidence of Hikvision's Involvement with Xinjiang IJOP and Re-Education Camps," IPVM, October 2, 2018. For a discussion of the IJOP in the previous reporting year, see CECC, *2018 Annual Report,* October 10, 2018, 108–09, 278–80.

[42] Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region," February 26, 2018. See also Darren Byler, "Ghost World," *Logic,* accessed April 5, 2019.

[43] Human Rights Watch, "China's Algorithms of Repression," May 1, 2019; Darren Byler, "Ghost World," *Logic,* accessed April 5, 2019; Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region," February 26, 2018.

[44] Charles Rollet, "Evidence of Hikvision's Involvement with Xinjiang IJOP and Re-Education Camps," IPVM, October 2, 2018; Isaac Stone Fish, "Why Are U.S. Companies Working for a Chinese Firm That's Implicated in Ethnic Cleansing?," editorial, *Washington Post,* September 21, 2018.

[45] Emily Feng, "Chinese Surveillance Group Faces Crippling US Ban," *Financial Times,* November 18, 2018.

[46] Lindsay Gorman and Matt Schrader, "U.S. Firms Are Helping Build China's Orwellian State," *Foreign Policy,* March 29, 2019.

[47] "Hikvision Global," About, Hikvision, accessed April 8, 2019; Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *New York Times,* May 22, 2019.

[48] Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *New York Times,* May 22, 2019; Human Rights Watch, "China's Algorithms of Repression," May 1, 2019.

[49] James Kynge and Demetri Sevastopulo, "US Pressure Building on Investors in China Surveillance Group," *Financial Times,* March 29, 2019; Rodrigo Campos and Samuel Shen, "MSCI to Quadruple Weighting of China A-Shares in Its Global Benchmarks," *Reuters,* February 28, 2019.

[50] James Kynge and Demetri Sevastopulo, "US Pressure Building on Investors in China Surveillance Group," *Financial Times,* March 29, 2019; Rodrigo Campos and Samuel Shen, "MSCI to Quadruple Weighting of China A-Shares in Its Global Benchmarks," *Reuters,* February 28, 2019.

[51] James Kynge and Demetri Sevastopulo, "US Pressure Building on Investors in China Surveillance Group," *Financial Times,* March 29, 2019.

[52] "WPP Announces the Merger of Burson-Marsteller and Cohn & Wolfe," WPP, February 27, 2018; "Our Companies," WPP, accessed April 8, 2019. Although the Foreign Agents Registration Act database on the U.S. Department of Justice website uses the name Burson-Marsteller, LLC, in February 2018, the firm merged with Cohn & Wolfe to form BCW (Burson Cohn & Wolfe), which itself is a subsidiary company of the communications services holding company WPP.

[53] "Active Foreign Principals by Country or Location as of 04/08/2019," Active Foreign Principals by Country or Location, Quick Search, U.S. Department of Justice, accessed April 8, 2019. See also Isaac Stone Fish, "Why Are U.S. Companies Working for a Chinese Firm That's Implicated in Ethnic Cleansing?," editorial, *Washington Post,* September 21, 2018.

[54] Cate Cadell and Philip Wen, "China Surveillance Firm Tracking Millions in Xinjiang: Researcher," *Reuters,* February 17, 2019; Yanan Wang and Dake Kang, "Exposed Chinese Database Shows Depth of Surveillance State," *Associated Press,* February 19, 2019; Caitlin Cimpanu, "Chinese Company Leaves Muslim-Tracking Facial Recognition Database Exposed Online," ZDNet, February 14, 2019.

[55] Cate Cadell and Philip Wen, "China Surveillance Firm Tracking Millions in Xinjiang: Researcher," *Reuters,* February 17, 2019; Yanan Wang and Dake Kang, "Exposed Chinese Database Shows Depth of Surveillance State," *Associated Press,* February 19, 2019; Caitlin Cimpanu, "Chinese Company Leaves Muslim-Tracking Facial Recognition Database Exposed Online," ZDNet, February 14, 2019.

[56] Lindsay Gorman and Matt Schrader, "U.S. Firms Are Helping Build China's Orwellian State," *Foreign Policy,* March 29, 2019; Caitlin Cimpanu, "Chinese Company Leaves Muslim-Tracking Facial Recognition Database Exposed Online," ZDNet, February 14, 2019. The Chinese firms NetPosa Technologies and SenseTime set up SenseNets in 2015, though SenseTime sold its stake in the company in July 2018. Li Tao, "SenseNets: The Facial Recognition Company That Supplies China's Skynet Surveillance System," *South China Morning Post,* April 12, 2019. For additional reporting on the relationship between SenseTime and suppliers Nvidia and Qualcomm, see Ryan Mac, Rosalind Adams, and Megha Rajagopalan, "US Universities and Retirees Are Funding the Technology behind China's Surveillance State," *BuzzFeed News,* June 5, 2019.

[57] David Ramli and Mark Bergen, "This Company Is Helping Build China's Panopticon. It Won't Stop There," *Bloomberg,* November 19, 2018; Christian Shepherd, "China's SenseTime Sells Out of Xinjiang Security Joint Venture," *Financial Times,* April 15, 2019; "Shouye" [Homepage], Li'ang Jishu [Leon Technology], accessed April 16, 2019.

[58] "Li'ang Jishu pai ren canjia de 'Xinjiang Weiwu'erzu Zizhiqu Tianshan Wang xin jihua xinxihua youxiu guanli rencai peixun ban' yuanman jieshu" [Perfect ending to "Xinjiang Uyghur Autonomous Region Tianshan internet information planning [and] informatization excellent managers personnel training class" that Leon Technology staff attended], Li'ang Jishu [Leon Technology], accessed April 16, 2019; "Li'ang Jishu Gufen Youxian Gongsi" [Leon Technology Company Limited], Xinjiang Rencai Wang [Xinjiang Human Resources Net], accessed April 16, 2019.

[59] Christian Shepherd, "China's SenseTime Sells Out of Xinjiang Security Joint Venture," *Financial Times,* April 15, 2019.

[60] David Ramli and Mark Bergen, "This Company Is Helping Build China's Panopticon. It Won't Stop There," *Bloomberg,* November 19, 2018.

[61] Ryan Mac, Rosalind Adams, and Megha Rajagopalan, "US Universities and Retirees Are Funding the Technology Behind China's Surveillance State," *BuzzFeed News,* May 30, 2019.

[62] Ibid.

[63] Charles Rollet, "Infinova's Xinjiang Business Examined," IPVM, December 7, 2018; Ryan Mac, Rosalind Adams, and Megha Rajagopalan, "US Universities and Retirees Are Funding the Technology Behind China's Surveillance State," *BuzzFeed News,* May 30, 2019.

[64] Charles Rollet, "Infinova's Xinjiang Business Examined," IPVM, December 7, 2018.

[65] Brian Spegele and Kate O'Keeffe, "China Exploits Fleet of U.S. Satellites to Strengthen Police and Military Power," *Wall Street Journal,* April 23, 2019. For more information on the protests and strife in the Xinjiang Uyghur Autonomous Region in 2009, see CECC, *2009 Annual Report,* October 10, 2009, 249–53.

[66] Brian Spegele and Kate O'Keeffe, "China Exploits Fleet of U.S. Satellites to Strengthen Police and Military Power," *Wall Street Journal,* April 23, 2019.

[67] Natasha Khan, "American Firm, Citing Ethics Code, Won't Sell Genetic Sequencers in Xinjiang," *Wall Street Journal,* February 20, 2019; Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *New York Times,* February 21, 2019; Human Rights Watch, "China: Minority Region Collects DNA from Millions," December 13, 2017.

[68] Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *New York Times,* February 21, 2019.
[69] Human Rights Watch, "China: Minority Region Collects DNA from Millions," December 13, 2017.
[70] "Xianfeng Jituan Xinjiang Kashi peixun zhongxin qianyue yishi zai Jing juxing" [Signing ceremony for Frontier Services Group Training Center in Kashgar, Xinjiang, held in Beijing], Frontier Services Group, January 22, 2019; "Erik Prince Company to Build Training Centre in China's Xinjiang," *Reuters,* January 31, 2019. The Commission did not observe reports regarding what kind of training facility would be built.
[71] "Xianfeng Jituan Xinjiang Kashi peixun zhongxin qianyue yishi zai Jing juxing" [Signing ceremony for Frontier Services Group Training Center in Kashgar, Xinjiang, held in Beijing], Frontier Services Group, January 22, 2019; "Erik Prince Company to Build Training Centre in China's Xinjiang," *Reuters,* January 31, 2019. For more information on the Xinjiang Production and Construction Corps, see Uyghur Human Rights Project, "The Bingtuan: China's Paramilitary Colonizing Force in East Turkestan," April 26, 2018.
[72] Anna Fifield, "Blackwater Founder Erik Prince's New Company Is Building Training Center in Xinjiang," *Washington Post,* February 1, 2019.
[73] Human Rights Watch, "China," in *World Report 2019: Events of 2018,* 2019, 136; Universal Declaration of Human Rights, adopted and proclaimed by UN General Assembly resolution 217A (III) of December 10, 1948, art. 12; International Covenant on Civil and Political Rights (ICCPR), adopted by UN General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23, 1976, art. 17; United Nations Treaty Collection, Chapter IV, Human Rights, International Covenant on Civil and Political Rights, accessed May 29, 2019. China has signed but not ratified the ICCPR. See also UN Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, Joseph Cannataci, A/HRC/37/62, Advance Unedited Version, February 28, 2018, para. 4; UN General Assembly, Resolution Adopted by UN General Assembly on December 18, 2013: 68/167. The Right to Privacy in the Digital Age, A/RES/68/167, January 21, 2014.
[74] *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* [PRC Cybersecurity Law], passed November 7, 2016, effective June 1, 2017, art. 37.
[75] For more information on the Chinese government's use of "state security" charges to target rights advocates, see, e.g., Bureau of Democracy, Human Rights, and Labor, U.S. Department of State, "2018 Human Rights Report: China (Includes Tibet, Hong Kong and Macau)," March 13, 2019; Human Rights Watch, "China: State Security, Terrorism Convictions Double," March 16, 2016; CECC, *2017 Annual Report,* October 5, 2017, 103–4.
[76] *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* [PRC Cybersecurity Law], passed November 7, 2016, effective June 1, 2017, art. 28; Donald C. Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," available at Social Science Research Network, March 28, 2019, 9–11; Amnesty International, "When Profits Threaten Privacy—5 Things You Need to Know about Apple in China," 27 February 18.
[77] *Zhonghua Renmin Gongheguo Guojia Qingbao Fa* [PRC National Intelligence Law], passed June 27, 2017, effective June 28, 2017, arts. 7, 14; Donald C. Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," available at Social Science Research Network, March 28, 2019, 9–11; Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare* (blog), July 20, 2017.
[78] Ministry of Public Security, *Gong'an Jiguan Hulianwang Anquan Jiandu Jiancha Guiding* [Provisions on Internet Security Supervision and Inspection by Public Security Organizations], issued September 5, 2018, effective November 1, 2018.
[79] Ministry of Public Security, *Gong'an Jiguan Hulianwang Anquan Jiandu Jiancha Guiding* [Provisions on Internet Security Supervision and Inspection by Public Security Organizations], issued September 5, 2018, effective November 1, 2018, arts. 9, 15–16. See also Laney Zhang, "China: New Regulations on Police Cybersecurity Supervision and Inspection Powers Issued," *Global Legal Monitor* (blog), Library of Congress, November 13, 2018; "China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems," Insikt Group, February 8, 2019.
[80] Donald C. Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," available at Social Science Research Network, March 28, 2019, 3–4; Claudia Biancotti, Peterson Institute for International Economics, "The Growing Popularity of Chinese Social Media Outside China Poses New Risks in the West," January 11, 2019; Perrin Grauer, "Beijing's Denial of Huawei Control Bucks Expert Analysis," *Star Vancouver,* February 18, 2019.
[81] Ministry of Public Security, *Gong'an Jiguan Hulianwang Anquan Jiandu Jiancha Guiding* [Provisions on Internet Security Supervision and Inspection by Public Security Organizations], issued September 15, 2018, effective November 1, 2018, chap. 4.
[82] Yuan Yang, "China's Data Privacy Outcry Fuels Case for Tighter Rules," *Financial Times,* October 2, 2018; Samm Sacks and Lorand Laskai, "China's Privacy Conundrum," *Slate,* February 7, 2019; Samm Sacks et al., "Public Security Ministry Aligns with Chinese Data Protection Regime in Draft Rules," *DigiChina* (blog), New America, December 3, 2018.
[83] Samm Sacks and Lorand Laskai, "China's Privacy Conundrum," *Slate,* February 7, 2019. See also Claudia Biancotti, Peterson Institute for International Economics, "The Growing Popularity of Chinese Social Media Outside China Poses New Risks in the West," January 11, 2019.
[84] Jeremy Daum, "Social Credit Overview Podcast," *China Law Translate* (blog), October 31, 2018; Adrian Shahbaz, Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism,* October 2018; Yu-Jie Chen, Ching-Fu Lin, and Han-Wei Liu, "'Rule of Trust': The Power and Perils of China's Social Credit Megaproject," *Columbia Journal of Asian Law,* 32, no. 1 (2018), reprinted in Social Science Research Network, December 20, 2019, 3, 32–3.
[85] State Council, "Shehui Xinyong Tixi Jianshe Guihua Gangyao (2014–2020 nian)" [Social Credit System Construction Program Outline (2014–2020)], June 14, 2014. For an unofficial

English translation, see "Planning Outline for the Construction of a Social Credit System (2014–2020)," translated in *China Copyright and Media* (blog), April 25, 2015. For more information on the social credit system, see, e.g., Jeremy Daum, "China Through a Glass, Darkly," *China Law Translate* (blog), December 24, 2017; Mareike Ohlberg et al., Mercator Institute for China Studies, "Central Planning, Local Experiments: The Complex Implementation of China's Social Credit System," *MERICS China Monitor,* December 12, 2017; Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control," available at Social Science Research Network, May 9, 2018.

[86] Kirsty Needham, "China's All-Seeing Social Credit System Stops Actresses and Academics," *Sydney Morning Herald,* March 6, 2019; Samantha Hoffman, "Social Credit: Technology-Enhanced Authoritarian Control with Global Consequences," Australian Strategic Policy Institute, June 28, 2018.

[87] Yuan Yang, "Does China's Bet on Big Data for Credit Scoring Work?," *Financial Times,* December 20, 2018; Adrian Shahbaz, Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism,* October 2018.

[88] Yuan Yang, "Does China's Bet on Big Data for Credit Scoring Work?," *Financial Times,* December 20, 2018; Adrian Shahbaz, Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism,* October 2018.

[89] Yuan Yang, "Does China's Bet on Big Data for Credit Scoring Work?," *Financial Times,* December 20, 2018.

[90] CCP Central Committee and State Council, *Guanyu Jianchi Nongye Nongcun Youxian Fazhan Zuo Hao "San Nong" Gongzuo de Ruogan Yijian* [Various Opinions on Supporting and Prioritizing Agriculture and Village Development and Effectively Doing "3 Rurals" Work], issued February 19, 2019, sec. 6(3).

[91] Lauly Li, Coco Liu, and Cheng Ting-Fang, "China's 'Sharp Eyes' Offer Chance to Take Surveillance Industry Global," *Nikkei Asian Review,* June 5, 2019.

[92] David Ramli and Mark Bergen, "This Company Is Helping Build China's Panopticon. It Won't Stop There," *Bloomberg,* November 19, 2018; Blake Schmidt and Venus Feng, "China's Powerful Surveillance State Has Created at Least Four Billionaires," *Bloomberg,* February 21, 2019.

[93] David Ramli and Mark Bergen, "This Company Is Helping Build China's Panopticon. It Won't Stop There," *Bloomberg,* November 19, 2018.

[94] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times,* April 14, 2019.

[95] Ibid.

[96] Huileng Tan, "The Business of Government Surveillance in China Could Boost Some Tech Firms: Credit Suisse," *CNBC,* March 26, 2019.

[97] Robyn Dixon, "China's New Surveillance Program Aims to Cut Crime. Some Fear It'll Do Much More," *Los Angeles Times,* October 27, 2018.

[98] Dan Strumpf and Wenxin Fan, "A Silicon Valley Tech Leader Walks a High Wire between the U.S. and China," *Wall Street Journal,* November 19, 2018.

[99] Dan Strumpf and Wenxin Fan, "A Silicon Valley Tech Leader Walks a High Wire Between the U.S. and China," *Wall Street Journal,* November 19, 2018; Iris Deng, "Here's What You Need to Know about Hikvision, the Camera Maker Behind China's Mass Surveillance System," *South China Morning Post,* February 7, 2019; Lauly Li, Coco Liu, and Cheng Ting-Fang, "China's 'Sharp Eyes' Offer Chance to Take Surveillance Industry Global," *Nikkei Asian Review,* June 5, 2019.

[100] Walt Bogdanich and Michael Forsythe, "How McKinsey Has Helped Raise the Stature of Authoritarian Governments," *New York Times,* December 15, 2018.

[101] Ibid.

[102] Adrian Shahbaz, Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism,* October 2018, 1.

[103] Human Rights Watch, "China," in *World Report 2019: Events of 2018,* 2019, 138–39.

[104] *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* [PRC Cybersecurity Law], passed November 7, 2016, effective June 1, 2017, art. 47. See also Amnesty International, *China 2017/2018,* accessed April 26, 2019.

[105] Freedom House, "China Media Bulletin: 2018 Key Trends, Beijing's Global Influence, Tech Firm Backlash (No. 131)," December 13, 2018. For recent regulations restricting freedom of speech online, see, e.g., Cyberspace Administration of China and Ministry of Public Security, *Juyou Yulun Shuxing Huo Shehui Dongyuan Nengli De Hulianwang Xinxi Fuwu Anquan Pinggu Guiding* [Provisions for the Security Assessment of Internet Information Services Having Public Opinion Attributes or Social Mobilization Capacity], issued November 15, 2018, effective November 30, 2018.

[106] Phoebe Zhang, "China's Cyber Police Take Aim at 'Negative Information' in New Internet Crackdown," *South China Morning Post,* January 4, 2019; "China Deletes 7 Million Pieces of Online Information, Thousands of Apps," *Reuters,* January 23, 2019.

[107] Josh Horwitz, "China Steps Up VPN Blocks Ahead of Major Trade, Internet Shows," *Reuters,* October 30, 2018; James Griffiths, "China Is Exporting the Great Firewall as Internet Freedom Declines around the World," *CNN,* November 2, 2018; Yuan Yang, "China Turns Up Heat on Individual Users of Foreign Websites," *Financial Times,* January 7, 2019.

[108] Li Yuan, "No Earrings, Tattoos or Cleavage: Inside China's War on Fun," *New York Times,* March 27, 2019.

[109] Shi Jingnan and Bai Ying, "Wangluo shengtai zhili zhuanxiang xingdong yi qingli youhai xinxi 709.7 wan yu tiao" [Internet ecology governance special action already cleaned up 70.97 million pieces of information], *Xinhua,* January 23, 2019.

[110] "Censored on WeChat: A Year of Content Removals on China's Most Powerful Social Media Platform," Wechatscope, University of Hong Kong, reprinted in *Global Voices,* February 11,

2019; Sarah Cook, "Worried About Huawei? Take a Closer Look at Tencent," *The Diplomat,* March 26, 2019.

[111] Ryan Gallagher and Lee Fang, "Google Suppresses Memo Revealing Plans to Closely Track Search Users in China," *The Intercept,* September 21, 2018. The Chinese government banned Google in 2010 after the company refused to continue censoring search results. See, e.g., Kaveh Waddell, "Why Google Quit China—and Why It's Heading Back," *Atlantic,* January 19, 2016.

[112] Ryan Gallagher, "Google's Secret China Project 'Effectively Ended' After Internal Confrontation," *The Intercept,* December 17, 2018; Ryan Gallagher, "Google Employees Uncover Ongoing Work on Censored China Search," *The Intercept,* March 4, 2019.

[113] *Google and Censorship Through Search Engines, Hearing of the Subcommittee on the Constitution, Committee on the Judiciary, U.S. Senate,* 116th Cong. (2019) (testimony of Karan Bhatia, Vice President for Government Affairs and Public Policy, Google, Inc.). Note that discussion of Project Dragonfly can be found at 1:14:38 in the hearing video on the Judiciary Committee's website.

[114] Lusha Zhang and Ryan Woo, "Censorship Pays: China's State Newspaper Expands Lucrative Online Scrubbing Business," *Reuters,* March 28, 2019.

[115] Ibid.

[116] Li Yuan, "Learning China's Forbidden History, So They Can Censor It," *New York Times,* January 2, 2019.

[117] Ibid.