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.
Business and Human Rights

- 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. 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.” 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 . . . .” 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 according to scholars and rights groups. 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. 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. Companies that work in the XUAR are at great risk of complicity in the human rights abuses being committed in the region. [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. In other cases, authorities released individuals from the camps to perform forced labor in factories elsewhere in the XUAR. In still other cases,
XUAR authorities reportedly assigned individuals from ethnic minority groups to forced labor directly, without first sending them to the camps.\textsuperscript{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.\textsuperscript{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.\textsuperscript{13} More recent reports found that authorities used tax exemptions and subsidies to encourage Chinese garment manufacturers to move production to the XUAR.\textsuperscript{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.”\textsuperscript{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;\textsuperscript{16}
- electronics, including cell phones and computer hardware and software;\textsuperscript{17}
- food products, including noodles and cakes;\textsuperscript{18}
- shoes;\textsuperscript{19}
- tea;\textsuperscript{20} and
- handicrafts.\textsuperscript{21}

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

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

<table>
<thead>
<tr>
<th>Clothing Made With Forced Labor Imported Into United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>In January 2019, U.S. company Badger Sportswear stopped importing clothing from Hetian Taida Apparel, following media reports that the clothing was made with forced labor by internment camp detainees. 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. The chairman of Hetian Taida confirmed to the AP that his workforce included “trainees” from the camp. 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. Following media reports, WRAP conducted its own investigation, concluding that “this facility is not engaged in the use of forced labor.” 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.</td>
</tr>
</tbody>
</table>

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, in violation of the internationally recognized right to privacy. 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. 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.” In addition to tracking them, authorities may arbitrarily detain individuals flagged by the IJOP in the internment camps or other detention facilities. 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.

- 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. 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. 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). 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-Marsteller52 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. 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. 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.” 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. The announcement, since removed, noted that the agreement was part of a “strategic cooperation framework agreement” (zhanyue 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. 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.

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. For example, the PRC Cybersecurity Law requires companies to store user data inside mainland China and to provide technical support to authorities conducting criminal investigations or “protecting state security,” without specifying what such technical support entails. 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.”

In September 2018, the Ministry of Public Security issued implementing provisions that further detailed the government’s authority under the Cybersecurity Law. 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. Experts note that companies typically must comply with government demands to provide information. Chapter 4 of the implementing regulations stipulates potential criminal penalties for failure to comply.
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. 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.

**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. 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. All Chinese individuals and organizations must now have a unique social credit code, including multinational companies operating in China. Private companies such as Ant Financial also offer private credit scoring services that collect large amounts of customer data. While these services are separate from the government system, the government has the authority to access the companies’ data. 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.

**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.” 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. 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. For example, SenseTime sold artificial intelligence (AI) technology to police in China in the form of SenseTotem and SenseFace surveillance systems. 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. Chinese companies CloudWalk, Megvii, Yitu, and SenseTime assisted authorities in this surveillance. The head of China equity strategy for Credit Suisse noted that for many Chinese AI firms, their “biggest business” was government surveillance projects. As one human rights advocate noted, while the Chinese government claims these surveillance projects target criminals, “police treat those that exercise...
Business and Human Rights

basic civil liberties like peaceful assembly or freedom of association as criminals.”

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. **Nvidia** has also sold chips to **Hikvision**, one of the Chinese firms that has been integral to the construction of government surveillance systems. The U.S. consulting firm **McKinsey & Company** reportedly assisted local governments in China to implement “smart cities” surveillance systems. In the words of one expert, these “smart cities” projects are “about political control.”

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,” and Human Rights Watch reported that the government continued to censor “politically sensitive information” online. 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. New regulations, censorship campaigns, and increasing restrictions on the use of virtual private networks (VPNs) this past year have further circumscribed online expression. In 2018, regulators reportedly shut down over 6,000 websites. 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. [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. 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. Work on the project appeared to end in late 2018 following employee protests and media attention. Google’s Vice President for Government Affairs and Public Policy told the Senate Judiciary Committee in July 2019 that Google had “terminated” Project Dragonfly.

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. Revenue from People.cn’s censorship services reportedly rose 166 percent in 2018. Another censorship service, Rainbow Shield, owned by the company Beyondsoft, employs over 4,000 people in multiple cities to review online content. In Chengdu municipality, Sichuan province, 160 Beyondsoft employees reportedly monitor a single news-aggregating app for politically sensitive con-
Business and Human Rights

tent.\textsuperscript{117} [For more information on censorship in China, see Section II—Freedom of Expression.]
Notes to Section II—Business and Human Rights


11 Eva Dou and Chao Deng, “Western Companies Get Tangled in China’s Muslim Clampldown,” 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 ILO 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 yaqsue 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.


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.


14 Ibid.


17 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 Sportwear,” The PE Hub Network, August 23, 2016.


19 “ ‘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.


21 Ibid.


23 Ibid.

24 Ibid.

25 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 Sportwear,” The PE Hub Network, August 23, 2016.


30 Ibid.

31 Ibid.


45 Lindsay Gorman and Matt Schrader, “U.S. Firms Are Helping Build China’s Orwellian State,” Foreign Policy, March 29, 2019.
Business and Human Rights

67“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.
68“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.
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.
73Zhonghua Renmin Gongheguo Wangluo Anquan Fa [PRC Cybersecurity Law], passed November 7, 2016, effective June 1, 2017, art. 37.
Business and Human Rights


70 CCP Central Committee and State Council, Guanyu Jianchi Nongye Nongcun Youxian Fazhan Zao 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. 6.31.


75 Ibid.


81 Ibid.


89 Yuan Yang, “Does China’s Bet on Big Data for Credit Scoring Work?,” Financial Times, December 20, 2018, sec. 6(3).


91 Ibid.

92 Ibid.


95 Ibid.


101 Ibid.

102 Ibid.


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.
Business and Human Rights

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.
115 Ibid.
117 Ibid.