REGULATORY FRAMEWORK, SURVEILLANCE INDUSTRY IN CHINA
Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
February 15, 2019

As noted in previous reports by the Special Rapporteur and other special procedures, new surveillance technologies and their rapid expansion by states and private actors call for more effective analysis and policy responses that address the shifting national, regional, and global human rights issues. China, an authoritarian state ruled by the Communist Party of China (CPC) whose priorities are often at odds with international human rights standards, presents a particularly challenging case. The Chinese state, tasked with advancing CPC interests, plays a significant role in the development and domestic deployment of surveillance technologies. As China accelerates its drive to lead the world in artificial intelligence "theories, technologies, and applications" by 2030,[1] Chinese companies in the surveillance technologies industry will increasingly face the conflict between domestic imperatives and the responsibilities of global industrial leaders in compliance with international standards.

Chinese companies that develop, market, export, deploy, and facilitate surveillance technologies include: manufacturers of cameras, drones, and other hardware; database owners and operators, including cloud servers; manufacturers and developers of biometrics identification systems; artificial intelligence developers, including facial recognition and gait recognition; and urban transport management systems.[2] Chinese companies engaged in the surveillance industry are also some of the major actors marketing and exporting these technologies around the world.[3] The size, scope, and reach of the companies—whether they are private, state-owned enterprises (SOEs), or companies with state investment—underscore domestic and global human rights challenges.

This submission highlights the key role of the party-state in China, outlines relevant provisions of the domestic regulatory framework, and describes some company examples to illustrate specific human rights concerns presented by this regulatory framework in conjunction with the close ties between the state and companies in China. The submission concludes with some suggestions for further monitoring and study.

1. **China's legal framework, including laws and regulations relevant to the development and deployment of surveillance technologies by private and state-owned or state-invested companies, is subservient to the ideological and political imperatives of the party-state.**

The overall regulatory framework in China is shaped by and subordinate to the interests of the Communist Party of China (CPC or Party). The authorities have not only placed the CPC above the law, but have created *a fundamental conflict in the state's responsibility to create an enabling environment* for the exercise of rights guaranteed by international law and the state's international obligations. The recently issued *Regulation on the Communist Party of China's Political-Legal Work* (effective January 13, 2019)[4] highlights the policy that all political and legal work done by the government must heed the guidance of the CPC. Article 3 states: "Political and legal units are the specialized forces that carry out political and legal work under the leadership of the Party, chiefly, including judicial organs, procuratorial organs, public security organs, national security organs, judicial and administrative organs, etc."[5]

Within an international human rights framework that treats states and companies as distinct actors with different responsibilities, the *multiple roles of China's party-state as regulator, investor, and owner* of companies in the surveillance sector also create tensions for all types of companies operating in China.

HRIC advises caution in classifying Chinese companies as "private," a label that may obscure the extensive links that exist between nominally private companies and the party-state. Government and CPC control is made possible, informally, through opaque shareholding structures, more formally through state protection and support of these companies, and through Party committees that must be established within private firms and SOEs. The Party committee requirement extends to private and foreign companies operating in China.[6] According to official government data, over 91% of publicly-owned companies and over 73% of private companies in China have established these Party organizations.[7] According to media reports, these Party committees have put "political pressure" on joint ventures to allow the CPC final authority in major decisions.[8]

CPC influence and enforcing the surveillance requirements of PRC law are a given for state-owned enterprises. One example is Hikvision Digital Technology, a Hangzhou-based SOE[9] that manufactures security cameras and other video surveillance products. It began as a Chinese government research institute, and then was transformed into an SOE. Hikvision has global partners including branch R&D offices in the United Kingdom and Canada. For the past five years, Hikvision is the world's largest supplier of video surveillance equipment, used in at least 150 countries in both public and private sectors. Its products are equipped with AI technology and are linked with cloud data-sharing. According to media reports, Hikvision technology is alleged to include deliberate security flaws that allow the PRC government access to data without user permission[10] and is involved in the grid-style surveillance systems used in Xinjiang, and also possibly used in surveillance in the Xinjiang arbitrary detention camps.[11] Hikvision provides an example of a publicly-listed SOE that designs and manufactures equipment specifically for surveillance purposes by governments. The company has aggressively expanded

its services over time to provide not only the hardware, but also the entire surveillance package, including AI algorithms and analytics systems.

For comparison, SenseTime is a private, Hong Kong based, startup AI developer and algorithm provider that focuses on facial recognition software and machinery. It was begun by professors and researchers, and is now entrusted by the PRC's Ministry of Science and Technology to establish China's National Open Innovation Platform of Next-Generation Artificial Intelligence on Intelligent Vision. It has partners around the world, including branch offices in Beijing, Shenzhen, Kyoto, Tokyo, and Singapore. According to media reports, PRC government contracts make up 40% of SenseTime's revenue, and its co-founder attended a Politburo study session on leading global AI development, calling for closer ties between SOEs and private companies.[12] China Mobile, one of China's top three telecommunications SOEs, has contracted with SenseTime to develop its facial recognition applications;[13] a high-security prison in Inner Mongolia uses its facial recognition technology;[14] and the security bureaus of Guangzhou, Shenzhen, and Yunnan use SenseTime technology, supplying their data back to SenseTime to train its algorithms.[15] SenseTime is an example of a private company that has increased its PRC ties dramatically and worked in cooperation with the PRC government for market share. In addition, the AI algorithms that SenseTime provides are not inherently surveillance technology, but are developed and applied expressly for that purpose.

2. China's domestic regulatory framework *requires* companies to act as surveillance agents of the state, instead of ensuring an enabling environment to protect the exercise of rights.

China's legal regulatory framework applicable to surveillance technologies is premised on an over broad concept of national security that provides the rationale for a comprehensive scope for surveillance regulation.[16] The Chinese government has promulgated a series of laws under an overarching policy framework of comprehensive securitization, including the *National Security Law* (effective July 1, 2015),[17] the *Counterterrorism Law* (effective January 1, 2016),[18] the *Cybersecurity Law* (effective June 1, 2017),[19] and the *National Intelligence Law* (effective June 28, 2017).[20] These overarching laws lay out general requirements for private companies to cooperate with and provide necessary technological and law enforcement support for the state in the name of national security. For example:

- The *National Security Law* states: "enterprises and public institutions should, according to the demands of national security work, cooperate with relevant departments in adopting relevant security measures" (Art. 79).
- The *Cybersecurity Law* states that "network operators"[21] must "provide technical support and assistance to public security organs' and state security organs' lawful activities preserving national security and investigating crimes" (Art. 28).

- Under the *Counterterrorism Law*, "telecommunications operators and Internet service providers shall provide technical interfaces, decryption, and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law" (Art. 18).
- The *National Intelligence Law* authorizes national intelligence work institutions lawfully carrying out intelligence efforts to "request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation" (Art. 14). (Emphasis added)

In performing their roles, companies must develop and deploy a range of surveillance technologies including hardware, software, and code expertise such as algorithmic engineering and other AI applications. Specifically, companies must comply with various provisions related to *collecting, storing and analyzing data*; *real name registration for users*; *monitoring and removing user-generated content* deemed illegal; and *specific technological requirements*.

Collection of Content Data & Metadata

Under the Cyberspace Administration of China's (CAC) *Regulations for Internet Content Management Administration Law Enforcement Procedures*, effective June 1, 2017,[22] China's Internet regulators are authorized to gather certain "digital evidence" from relevant "units,"[23] which includes electronic data, audio-visual materials, documentary evidence, etc. Electronic data includes, but is not limited to, web pages, blogs, microblogs, instant messaging tools, forums, stickers, webs, E-mail, network background, and other means of carrying electronic information or documents (Art. 20). Units are required to assist and cooperate with any investigation, including by providing information published by ISPs and users, and daily logs (Art. 18). Private companies are also required to keep a record of metadata and to store the data for specified periods of time.[24] The purpose of these regulations is to *ensure that backend data is accessible to the government*.[25]

Monitoring Individuals and Groups

The PRC government has devoted substantial resources to establishing a comprehensive and systematic monitoring system for individuals and groups that track their communications and activities online and offline. Companies in the information ecosystem play a key role in these efforts through the following requirements.

- *Real name registration*

The *Cybersecurity Law* requires network operators to implement real name registration and request identity information from users before they provide network access, domain name

registration, landline and mobile phone network access, instant messaging and communication services (Art. 24). According to the National People's Congress Standing Committee *Cybersecurity Law* 2017 enforcement report,[26] over 300 million users who had not been registered previously were registered within the preceding five years to fulfill the legal requirement of real name registration. In addition, services for over 10 million users who refused to register were suspended.

Other service providers of news, online forums, microblogs, are also subject to regulations that impose on them the responsibility to implement real name registration.[27] In the increasingly restrictive political environment in which absolute loyalty to the CPC and to Xi Jinping Thought is required, these real name requirements undermine anonymity and privacy and contribute to the chilling of expression and opinion.

- *Credit systems*

Certain Internet service providers are obligated to establish a credit system for their users based on their online behavior. Users are divided into categories based on their credit scores and are then provided with different levels of access to services and functionalities according to their scores. For example, providers of Internet services with post and comment functionalities are required to "carry out credit assessments of users' conduct," blacklist "seriously untrustworthy" users, and prohibit them from re-registration to access the services again (*Internet Post and Comments Service Management Regulations*, Art. 9). Similarly, providers of public account information services are obligated to "establish a credit level management system for Internet user public account information service users, and provide services corresponding to credit levels (*Internet User Public Account Information Service Management Regulations*, Art.6)."

In addition to these credit systems, China has announced the construction of a national social credit system, reportedly on track for deployment on the country's 1.4 billion citizens by 2020. The system, often described by Western media as "big brother," "aims to centralize data platforms into a big data-enabled surveillance infrastructure to manage, monitor, and predict the trustworthiness of citizens, firms, organizations, and governments in China."[28]

- *Tiered management system*

Internet service providers are tasked with monitoring Internet groups through a "tiered management system." Companies are obligated to implement "hierarchical and categorical management" of Internet groups based on their nature, type, membership scale, and activity level (*Internet Group Information Service Management Regulations*, Art. 7). Each group must have a unique identification code. For groups that reach a certain scale, the provisions

require an information page listing the group's name, number of members, and its type (Art. 8).

Internet Filtering and Censorship

Internet service providers are tasked with closely monitoring content on their platforms, often by implementing a "real-time inspection" system. For example, the *Internet Post and Comments Service Management Regulations* require service providers to establish such a system for posts and comments, and implement "a screen-before-publishing system" for posts and comments of Internet news information (Art. 5). The *Internet User Public Account Information Service Management Regulations* require service providers to "conduct real-time management of user public accounts' messages, posts, comments, and other interactive elements" (Art. 12). The *Internet Forum Community Service Regulations* also set the requirement for inspection systems including "real-time public information patrol" (Art. 5).

In addition to monitoring, regulatory provisions place primary responsibility on the Internet service providers to control the dissemination of "illegal content." Service providers are responsible for keeping a record of censored content and reporting it to relevant departments. The process often follows a procedure in which service providers delete information, stop its transmission, create a record, and report it to relevant departments. Network operators who discover prohibited information must "immediately stop transmission of that information, adopt handling measures such as deleting it to prevent the information from spreading, keep relevant records, and report to the relevant competent departments" (*Cybersecurity Law*, Art. 47).

Recommendations

The subordination of law to CPC leadership, the global reach of Chinese surveillance industry companies, and the advanced surveillance technologies deployed and marketed present steep challenges to ensuring rights protections—in particular on freedom of opinion and expression, and the right to privacy—not only for the 1.4 billion people in China, but also for the entire global information ecosystem.

In that light, HRIC respectfully advances the following recommendations:

- Further research, conceptual work and analysis should be conducted on the conflicts and tensions presented by surveillance industry regulatory frameworks in authoritarian restrictive states, including developing a typology of the different forms of companies, including ownership structures and effective control elements.

- States should review and amend all relevant laws and regulations that impact on development and deployment of surveillance technologies to implement relevant treaty

body and special procedure recommendations to ensure conformity with international standards on the freedom of opinion and expression and privacy rights.

- States should set clear guidelines for all judicial and law enforcement agencies on the primacy of adhering to international standards on the protection of freedom of expression and privacy rights in relation to surveillance, including safeguards to prevent political interference in the judicial and criminal justice processes. Progress supported by specific benchmarks and indicators and challenges encountered should be described in state party treaty body reports and in the next UPR cycle.

- Companies, including private, state-owned, or companies with significant state investment should formulate company policies and operational guidelines to include human rights impact assessments during development and deployment of any surveillance technologies to ensure safeguarding individuals' right to opinion, expression and privacy in accordance with international standards. These policies, guidelines and results of HRIAs should be publicly available.

---

[1] "[B]y 2030, China's AI theories, technologies, and applications should achieve world-leading levels, making China the world's primary AI innovation center, achieving visible results in intelligent economy and intelligent society applications, and laying an important foundation for becoming a leading innovation-style nation and an economic power." From "State Council Notice on the Issuance of the Next Generation Artificial Intelligence Development Plan," State Council of the People's Republic of China (July 8, 2017) released July 20, 2017 (English translation by China Copyright and Media, https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/).

[2] HRIC conducted a survey, using publicly available information, of a number of key companies. They include the following: Hikvision, https://www.hikvision.com/en; Dahua Technology, https://www.dahuatech.com; Yitu Technology, http://www.yitutech.com/en; Megvii, https://megvii.com; SenseTime, https://www.sensetime.com; Eyecool, http://www.eyecool.cn; Intellifusion, http://www.intellif.com; Isvision Technologies, http://www.isvision.com; and SeetaTech, http://www.seetatech.com.

[3] For example, Dahua Technology is a publicly listed company on the Shenzhen Stock Exchange based in Zhejiang, with more than 16,000 employees, over 50% of which are engaged in R&D. Dahua Technology has more than 200 provincial offices as well as 54 overseas subsidiaries and representative offices covering the Asia Pacific, North America, Europe, Africa and other regions, with its products and services applied in over 180 countries and regions. Dahua, "About Us," https://www.dahuasecurity.com/aboutUs/introduction/0, last visited Feb. 11, 2019.

[4]《中国共产党政法工作条例》Regulation on the Communist Party of China's Political-Legal Work, promulgated by the Central Committee of the Communist Party of China, Jan. 18, 2019, http://www.gov.cn/zhengce/2019-01/18/content_5359135.htm (English translation available at China Law Translate, https://www.chinalawtranslate.com/en/中国共产党政法工作条例, last visited Feb. 15, 2019).

[5] Article 3 in the original is as follows: "政法单位是党领导下从事政法工作的专门力量，主要包括审判机关、检察机关、公安机关、国家安全机关、司法行政机关等单位。" *Id.*

[6]《《受权发布》 2017 年中国共产党党内统计公报》 (Authorized to Publish) 2017 Statistical Communiqué of the Communist Party of China, Xinhua, Jun. 30, 2018, http://www.xinhuanet.com/politics/2018-06/30/c_1123059570.htm.

[7] *Id.*

[8] Michael Martina, "Exclusive: In China, the Party's Push for Influence Inside Foreign Firms Stirs Fears," Reuters, Aug. 24, 2017, https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU.

[9] John Honovich, "Hikvision CEO Admits Hikvision is a State-Owned Company," IP Video Market Info Inc., Oct. 6, 2016, https://ipvm.com/reports/hik-state.

[10] Dylan Welch and Kyle Taylor, "Chinese Video Surveillance Network Used by the Australian Government," Australian Broadcasting Corporation, Sep. 12, 2018, https://www.abc.net.au/news/2018-09-12/chinese-video-surveillance-network-used-by-australian-government/10212600.

[11] "China's Hi-Tech Police State in Fractious Xinjiang a Boon for Security Firms," Agence France-Presse, Jun. 27, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2152749/chinas-hi-tech-police-state-fractious-xinjiang-boon.

[12] David Ramli and Mark Bergen, "This Company Is Helping Build China's Panopticon. It Won't Stop There," Bloomberg, Nov. 20, 2018, https://www.bloomberg.com/news/articles/2018-11-19/this-company-is-helping-build-china-s-panopticon-it-won-t-stop-there.

[13] Bien Perez, "Meet SenseTime, Hong Kong's First Hi-Tech Unicorn that No One's Heard Of," South China Morning Post, Oct. 23, 2017, https://www.scmp.com/tech/start-ups/article/2116490/meet-sensetime-hong-kongs-first-hi-tech-unicorn-no-ones-heard.

[14] Li Xu, "Making Sense of SenseTime," Jump Start Magazine, Apr. 6, 2018, https://jumpstartmag.com/blog/making-sense-of-sensetime.

[15] Josh Horwitz, "The billion-dollar, Alibaba-backed AI company that's quietly watching people in China," Quartz, Apr. 16, 2018, https://qz.com/1248493/sensetime-the-billion-dollar-alibaba-backed-ai-company-thats-quietly-watching-everyone-in-china/.

[16] 《中华人民共和国国家安全法》National Security Law of the People's Republic of China, promulgated by the Standing Committee of the 12th National People's Congress (July. 1, 2015), effective July. 1, 2015 (English translation available on China Law Translate, http://www.chinalawtranslate.com/2015nsl/?lang=en, last visited Feb. 15, 2019): political security (Art. 16), homeland security (Art. 17), military security (Art. 18), economic security (Art. 19), financial infrastructure security (Art. 20), energy security (Art. 21), food security (Art. 22), cultural security (Art. 23), scientific and technological information security (Art. 24), ethnic security (Art. 26), religious security (Art. 27), societal security (Art. 29), ecological security (Art. 30), and nuclear security (Art. 31), security against terrorism (Art. 28), and security of outer space, deep sea, and polar regions (Art. 32).

[17] *Id*.

[18] 《中华人民共和国反恐怖主义法》Counterterrorism Law of the People's Republic of China, promulgated by the Standing Committee of the 12th National People's Congress (Dec. 27, 2015), effective Jan. 1, 2016 (English translation available on China Law Translate, https://www.chinalawtranslate.com/en 反恐怖主义法 (2015), last visited Feb. 15, 2019).

[19] 《中华人民共和国网络安全法》Cybersecurity Law of the People's Republic of China, promulgated by the Meeting 24 of the 12th Standing Committee of the People's Republic of China (Nov. 7, 2016), effective June 1, 2017 (English translation available on China Law Translate, http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en, last visited Feb. 15, 2019).

[20] 《中华人民共和国国家情报法(2018 修正) 》National Intelligence Law of the People's Republic of China (2018 Amendment), promulgated by Order No. 69 of the President of the People's Republic of China (Jun. 27, 2017), amended according to the Decision of the Standing Committee of the National People's Congress (Apr. 27, 2018), effective Apr. 27, 2018 (English translation available on Peking University Law, http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law, last visited Feb. 15, 2019).

[21] "**Network operators** refers to network owners and managers, and network service providers," Cybersecurity Law, Art.76.

[22] 《互联网信息内容管理行政执法程序规定》 Regulations for Internet Content Management Administration Law Enforcement Procedures, promulgated by the Cyberspace Admin. of China (May 2, 2018), effective Jun. 1,

2017, P.R.C., (English translation by China Copyright and Media, https://chinacopyrightandmedia.wordpress.com/2017/05/02/regulations-for-internet-content-management-administration-law-enforcement-procedures/, last visited Feb. 14, 2019).

[23] "**Unit**" in Chinese is "单位," which includes private enterprises.

[24] Despite legal requirements to ensure data security, the recent incident of an online exposure of a facial recognition database maintained by SenseTime, highlights the actual risks in maintaining these massive databases without rigorous attention to ensuring privacy protection for individuals tracked. The company had reportedly left more than 2.5 million records containing personal information and locations logged (more than 6.8 million in a 24 hour period) without any password protection. Alfred Ng, "Chinese Facial Recognition Company Left Database of People's Locations Exposed," CNet, Feb. 13, 2019, https://www.cnet.com/news/chinese-facial-recognition-company-left-database-of-peoples-location-exposed/.

[25] For example, Article 21 of the Cybersecurity Law requires network operators to "adopt technological measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow relevant provisions to store network logs for at least six months." Under the Regulation on Security Assessment of Internet Information Services of Public Opinion Nature or with Social Mobilization Capacity (effective November 30, 2018), Internet information service providers with "public opinion nature and social mobilization capacity" must keep "log information for user accounts, operation times, operation types, network source and destination addresses, network source ports, client terminal hardware specifications, and so forth, as well as measures for retaining records of user-published information" (Art.5).

[26] "《全国人民代表大会常务委员会执法检查组关于检查《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强<网络信息保护的决定》实施情况的报告》 Dec. 24, 2017, http://www.npc.gov.cn/npc/zfjc/zfjcelys/2017-12/24/content_2036037.htm.

[27] 《互联新闻信息服务管理规定》Internet News Service Management Regulations, promulgated by the Cyberspace Admin. of China (May 2, 2017), effective Jun. 1, 2017, P.R.C., Art. 13, (English translation by China Copyright and Media, https://chinacopyrightandmedia.wordpress.com/2017/05/02/internet-news-information-service-management-regulations-2, last visited Feb. 15, 2019); 《互联网跟帖评论服务管理规定》Internet Post and Comments Service Management Regulations, promulgated by the Cyberspace Admin. of China (Aug. 25, 2017), effective Oct. 1, 2017, P.R.C., Art. 5, (English translation by China Law Translate, https://www.chinalawtranslate.com 互联网跟帖评论服务管理规定/?lang=en, last visited Feb. 15, 2019); 《互联网用户公众账号信息服务管理规定》Internet Group Information Service Management Regulations, promulgated by the Cyberspace Admin. of China (Sep. 7, 2017), effective Oct. 8, 2017, P.R.C. (English translation by China Law Translate, https://www.chinalawtranslate.com 互联网群组信息服务管理规定/?lang=en, last visited Feb. 15, 2019); 《互联网用户公众账号信息服务管理规定》Internet User Public Account Information Service Management Regulations, promulgated by the Cyberspace Admin. of China (Sep. 7, 2017), effective Oct. 8, 2017, P.R.C., Art. 6; 《互联网域名管理办法》Internet Domain Name Management Measures, promulgated by the Ministry of Indus. and Info. Tech. (Aug. 24, 2017), effective Nov. 1, 2017, P.R.C., Art. 30, (English translation by China Law Translate, https://www.chinalawtranslate.com 互联网域名管理办法/?lang=en, last visited Feb. 15, 2019). HRIC has modified the translation of the names of some of these regulations and passages quoted.

[28] Fan Liang et al., "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure," *Policy and Internet* 10 no.4 (2018); see also Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control," May 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792.