***Pervasive State Surveillance***

In 2018, the Chinese government continued to implement the far-reaching and draconian Cybersecurity Law (2017), which authorizes invasive cyber surveillance and gives authorities broad powers to restrict and penalize online expression. In January, [authorities announced](http://cn.rfi.fr/%E4%B8%AD%E5%9B%BD/20180130-%E4%B8%AD%E5%9B%BD%E6%94%BF%E5%BA%9C%E5%8A%A0%E5%A4%A7%E6%8E%A7%E5%88%B6%E7%BF%BB%E5%A2%99%E8%BD%AF%E4%BB%B6%E5%8A%9B%E5%BA%A6-%E5%A4%A7%E9%99%86%E6%B0%91%E4%BC%97%E6%9B%B4%E9%9A%BE%E8%8E%B7%E5%BE%97%E5%A2%83%E5%A4%96%E4%BF%A1%E6%81%AF?ref=tw) that businesses could only use government-approved Virtual Private Network (VPN) software to access the global Internet. On March 31, the [ban](https://www.nchrd.org/wp-content/uploads/2018/02/CHRD-2017-Annual-Report-of-Situation-of-HRDs-in-China_Feb-2018.pdf) on VPNs without government pre-approval went into force. Though many Chinese found ways to circumvent the ban and continued to use VPNs, authorities selectively enforced the law and punished some individuals to frighten others. A court in Shanghai handed down a [3-year suspended prison sentence](http://rmfyb.chinacourt.org/paper/html/2018-10/09/content_144238.htm) to a software developer in October for developing a VPN. Guangdong authorities [fine](http://www.globaltimes.cn/content/1134724.shtml)d a VPN user 1,000 RMB (approx. 150 USD) in December.

In November, the “[Public Security Bureau Internet Security Control Inspection Provisions](http://www.xinhuanet.com/legal/2018-10/04/c_1123519817.htm)” came into force, which authorizes police to conduct on-site inspection of Internet Service Providers (ISPs). Any company that refuses the inspection could face criminal prosecution.

The government [announced](http://www.legaldaily.com.cn/index_article/content/2018-02/13/content_7474994.htm) that “full coverage, connectivity, and control” by police video surveillance will reach every corner of the entire country by 2020 under the 13th Five-Year Plan. In implementing the plan, authorities expanded video surveillance beyond the cities and installed surveillance cameras in small towns and villages as a part of the “Sharp Eyes” (雪亮) program. Though more than half of the trial projects were [concentrated in Xinjiang](https://www.nchrd.org/2018/08/civil-society-follow-up-report-submitted-to-un-committee-on-the-elimination-of-racial-discrimination-july-2018/), the rest were introduced elsewhere. In Sichuan province, for example, local officials [had extended](http://www.legaldaily.com.cn/index_article/content/2018-02/13/content_7474994.htm) the surveillance system into 14,087 villages, installing and activating 41,695 cameras by the end of 2017.

“Grid management,” a highly invasive system of police surveillance, which authorities have been [developing](https://chinachange.org/2013/08/08/the-urban-grid-management-and-police-state-in-china-a-brief-overview/) for over a decade has become much more sophisticated and widely implemented in Tibet, Xinjiang and select Han majority provinces. The system, divides up a city, town, village or neighbourhood into geometric zones for police monitoring, and these zones are [equipped with](https://www.nchrd.org/2018/08/civil-society-follow-up-report-submitted-to-un-committee-on-the-elimination-of-racial-discrimination-july-2018/) an interconnected network of cameras, mobile Internet technologies, and big data analytics, in addition to police patrols, checkpoints, and live-in cadres in local residencies in minority areas. The system monitors all individuals and activities in each and every zone. State media [reported](http://legal.people.com.cn/n1/2017/1104/c42510-29626978.html) on the grid system in Yueqing City in Zhejiang, which recruited 1,600 new agents in the summer of 2017.

In June, the Chinese railway corporation [publicised](http://www.xinhuanet.com/politics/2018-06/01/c_1122924358.htm) a list of individuals deemed “untrustworthy,” which police and railway security would use to identify and block passengers from boarding trains. Those named on the list would have to raise objections with authorities during a seven-day publicity period, otherwise face sanctions automatically.

Announcements of new technology being developed or tested raised further concerns over privacy rights and abuse by police. China’s Xiamen Meiya Pico Information Co Ltd promoted its XDH-CF-5600 phone scanner at the China International Exhibition on Police Equipment [held](http://www.ciepe.com/) in May, which [reportedly](https://www.reuters.com/article/us-china-monitoring-tech-insight/at-beijing-security-fair-an-arms-race-for-surveillance-tech-idUSKCN1IV0OY) would be able to crack phone passwords, extract data from apps, and scan contacts. Police stations in every Chinese province reportedly purchased [data extracting technology](https://www.reuters.com/article/us-china-monitoring-insight/from-laboratory-in-far-west-chinas-surveillance-state-spreads-quietly-idUSKBN1KZ0R3), already in use in Xinjiang and some Han majority areas, to scan phones for so-called “illegal content.”

In January 2018, Shanghai Baihong Software Technology Co Ltd [announced a new software](https://www.zaobao.com.sg/realtime/china/story20180102-823695) that could identify adults through old photos of them as teens. In February, police in Zhengzhou began testing [facial recognition glasses](https://www.wsj.com/articles/chinese-police-go-robocop-with-facial-recognition-glasses-1518004353) made by Beijing LLVision Technology Co in train stations to identify “criminal suspects.” Another company called Watrix developed “[gait recognition](http://www.watrix.ai/portfolio-item/gait-recognition/)” technology to identify individuals by the way they walked, which reportedly was [already in use](https://www.apnews.com/bf75dd1c26c947b7826d270a16e2658a) by police in Beijing and Shanghai. Starting January 2019, [all new cars](http://auto.sina.com.cn/zz/7x24/2018-06-14/detail-ihcwpcmq8707381.shtml) in China must install a radio frequency chip (RFID) to allow authorities to track their movement.

Foreign tech companies were complicit in complying and cooperating with the Chinese state’s big data surveillance. In February, Apple [moved](http://www.xinhuanet.com/fortune/2018-01/10/c_129787810.htm) all of its Chinese users’ iCloud information to a state-run Chinese company, which allowed police to access any content under the Cybersecurity Law and other regulations. Leaked plans of a censored Google search app called [Project Dragonfly](https://www.nchrd.org/2018/12/open-letter-response-to-google-on-project-dragonfly-china-and-human-rights/) indicated that the app would allow Chinese authorities access to virtually all users’ information, including searches for government censored content. LinkedIn [censored](https://www.buzzfeednews.com/article/meghara/linkedin-censorship-peter-humphrey) the pages of two overseas critics of the Chinese government in December.

Submission date: 21 February 2019