# Chinese mass surveillance systems: insights and export

Reference: Memo [190516-2] Date: 16/05/2019 - Version: 1.0
Keywords: personal data, GDPR, mass surveillance, exportation
Sources: publicly available information

## Key Points

- A database containing personal data of Chinese citizens was left unprotected on the Internet.
- These personal data were purportedly collected using smart cities and mass surveillance technologies.
- Human Rights Watch released a report detailing how the Chinese government is using such technologies as a means to invade their citizens' privacy.
- Chinese companies and start-ups are exporting these technologies to foreign countries.

## Summary

According to open sources, an Elasticsearch database related to a smart city system was left unattended and publicly accessible. The analysis of the 'gigabytes of data' it contains put into light information related to a person's behaviour and facial recognition details like the presence of a beard, sunglasses, etc. Persons living or going through two parts of Beijing, including the embassy district, were being watched by the system this database belongs to. The repository appears to be hosted on the cloud platform of Alibaba, a Chinese company. Alibaba denied having any visibility into the content of the database.

In parallel to these revelations, Human Rights Watch (HRW) released a report describing a system dubbed 'Integrated Joint Operations Platform (IJOP)', one of the main systems Chinese authorities use for mass surveillance in Xinjiang. The report focuses on a mobile application police and other officials use to communicate with that system. According to HRW, IJOP is used in conjunction with so called 'data doors' in the autonomous province of Xinjiang in order to track and watch the population, including ethnic minorities like the Uyghurs. The report gives insight related to the data that is collected. This include whereabouts, vehicle records and usage, phone records and usage, general and IT behaviour, electricity consumption, religious and political preferences, etc. Moreover the report shows how it is being used to restrict people's movement (from a region to public places like a mall), start investigations, etc. The 'data doors' mentioned in the report refer to specific checkpoints used to control people's ID and collect phone data such as IMEI and MAC addresses for – supposed – tracking purposes. Finally, this report raises concerns regarding identity control prior to buying gas and to random smartphone control by the local authorities in order to look for 'inappropriate' behaviour or 'suspicious' applications like WhatsApp or a VPN client.

Several Chinese companies have been seen exporting mass surveillance systems abroad, the last example being the telecom company ZTE in Venezuela. The country's authorities have asked the Chinese company to install a system capable of monitoring medical records, social media and citizen participation to elections using smart cards. Zimbabwe also bought a system using facial recognition from the CloudWalk company in order to build a national database of faces. Mexico, Ecuador, Malaysia also contracted with Chinese companies in order to install such systems.

## Comments

The fact that the Chinese government used technologies like AI and facial recognition in order to track its population's precise movements was well known as well as their use of a 'social credit' mechanism for 'social discipline'. The HRW report however provides details related to the extent of the mechanisms and equipment that are put in place, but also about the data that has been collected and queried using IJOP. These findings emphasize how technological developments are actually and specifically being used for the massive collection of personal data.

The several export cases of similar systems may raise concerns as regards the spread of such Chinese technologies in the world.