



How Mass Surveillance Works in Xinjiang, China

‘Reverse Engineering’ Police App Reveals Profiling and Monitoring Strategies

AVAILABLE IN 简体中文 ENGLISH العربية BAHASA INDONESIA
DEUTSCH ESPAÑOL FRANÇAIS TÜRKÇE

New York, May 2, 2019

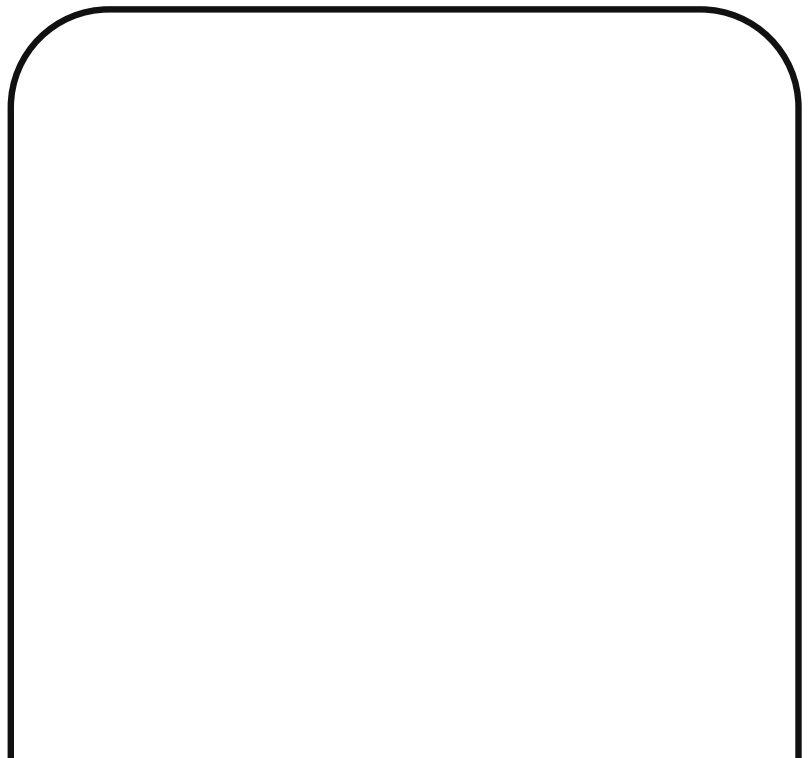
Chinese authorities are using a mobile app to carry out illegal mass surveillance and arbitrary detention of Muslims in China's western Xinjiang region.

The Human Rights Watch report, “**China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App**,” presents new evidence about the surveillance state in Xinjiang, where the government has subjected 13 million Turkic Muslims to heightened repression as part of its “Strike Hard Campaign against Violent Terrorism.” Between January 2018 and February 2019, Human Rights Watch was able to reverse engineer the mobile app that officials use to connect to the Integrated Joint Operations Platform (IJOP), the Xinjiang policing program that aggregates data about people and flags those deemed potentially threatening. By examining the

design of the app, which at the time was publicly available, Human Rights Watch revealed specifically the kinds of behaviors and people this mass surveillance system targets.

“Our research shows, for the first time, that Xinjiang police are using illegally gathered information about people’s completely lawful behavior – and using it against them,” said Maya Wang, senior China researcher at Human Rights Watch. “The Chinese government is monitoring every aspect of people’s lives in Xinjiang, picking out those it mistrusts, and subjecting them to extra scrutiny.”

Human Rights Watch published screenshots from the IJOP app, in the original Chinese and translated into English.





The app prompts government officials to collect a wide array of information from ordinary people in Xinjiang.

From a drop-down menu,

officials are prompted to
choose the circumstances
under which information is
being collected.

The information it gathers
ranges from people's blood
type to their height,

from their “religious
atmosphere” to their
political affiliation.

The app's source code also reveals that the police platform targets 36 types of people for data collection. Those include people who have stopped using smart phones, those who fail to "socialize with neighbors," and those who "collected money or materials for mosques with enthusiasm."

The IJOP platform tracks everyone in Xinjiang. It monitors

people's movements by tracing their phones, vehicles, and ID cards. It keeps track of people's use of electricity and gas stations.

Human Rights Watch found that the system and some of the region's checkpoints work together to form a series of invisible or virtual fences. People's freedom of movement is restricted to varying degrees depending on the level of threat authorities perceive they pose, determined by factors programmed into the system.

A former Xinjiang resident told Human Rights Watch a week after he was released from arbitrary detention: "I was entering a mall, and an orange alarm went off." The police came and took him to a police station. "I said to them, 'I was in a detention center and you guys released me because I was innocent.'... The police told me, 'Just don't go to any public places.'... I said, 'What do I do now? Just stay home?' He said, 'Yes, that's better than this, right?'"

The authorities have programmed the IJOP so that it treats many ordinary and lawful activities as indicators of suspicious behavior. For example:

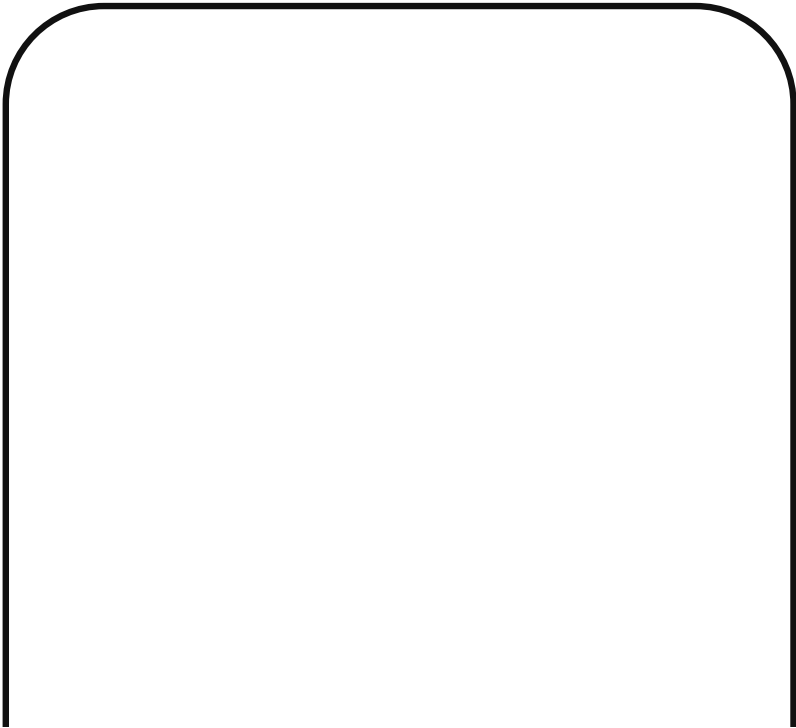




Officials are prompted to

investigate those
determined to have used
an “unusual” amount of
electricity.

Officials can select from a list of reasons for unusual electricity consumption, such as: “purchased new electronics for domestic use” or “doing renovations.”

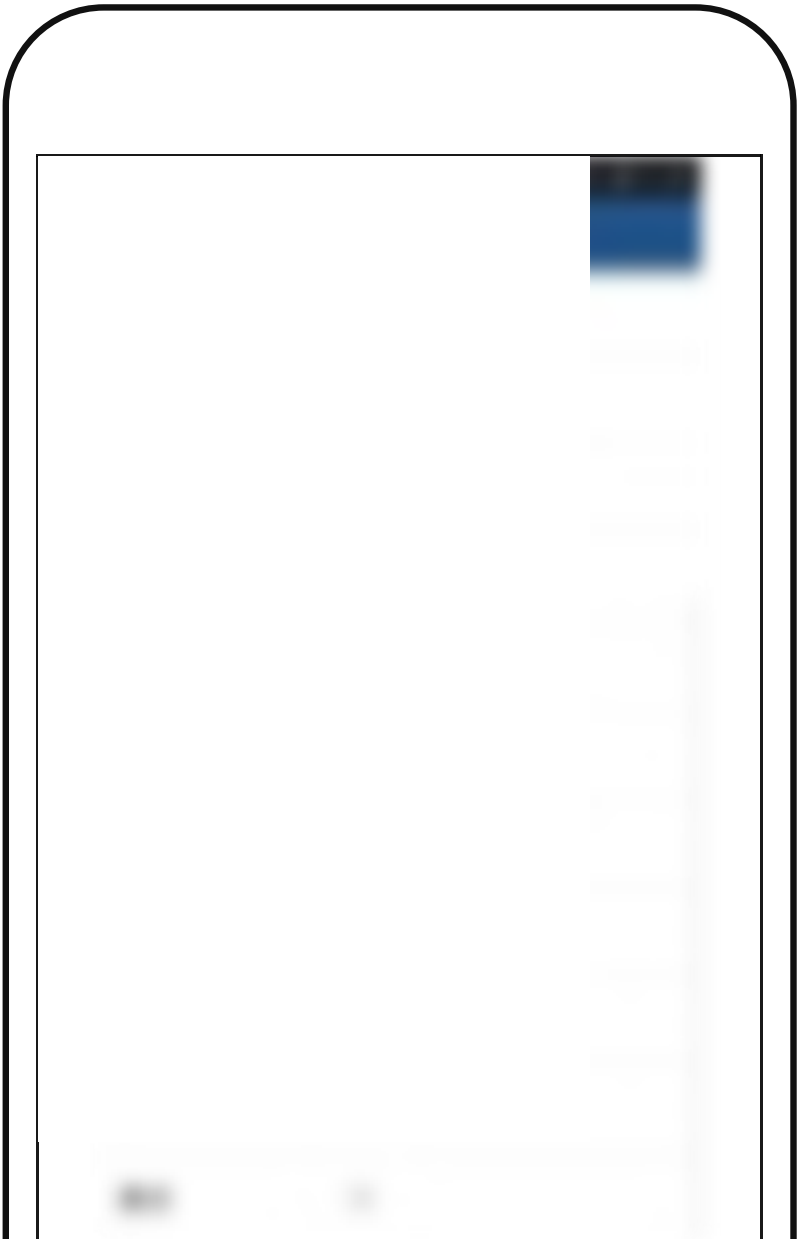




The system detects when the registered owner of the car is not the same as the person who is buying gasoline.

The app's source code suggests that nearby officials are required to investigate by logging the reasons for the mismatch,

and deciding whether this case seems suspicious and requires further police investigation.






The app alerts officials to
people who took trips
abroad that it considers
excessively long,

then prompts officials to interrogate the “overdue” person or their relatives and other acquaintances, asking them for details about the travel.







The system alerts officials if it has lost track of someone's phone, to determine whether the owner's actions are suspicious and require investigation.

Some of the investigations involve checking people's phones for any one of the 51 internet tools that are considered suspicious, including WhatsApp, Viber, Telegram, and Virtual Private Networks (VPNs), Human Rights Watch found. The IJOP system

also monitors people's relationships, identifying as suspicious travelling with anyone on a police watch list, for example, or anyone related to someone who has recently obtained a new phone number.

Based on these broad and dubious criteria, the system generates lists of people to be evaluated by officials for detention. Official documents state individuals "who ought to be taken, should be taken," suggesting the goal is to maximize detentions for people found to be "untrustworthy." Those people are then interrogated without basic protections. They have no right to legal counsel, and some are tortured or otherwise mistreated, for which they have no effective redress.

The IJOP system was developed by China Electronics Technology Group Corporation (CETC), a major state-owned military contractor in China. The IJOP app was developed by Hebei Far East Communication System Engineering Company (HBFEC), a company that, at the time of the app's development, was fully owned by CETC.

Under the Strike Hard Campaign, Xinjiang authorities have also collected biometrics, including DNA samples, fingerprints, iris scans, and blood types of all residents in the region ages 12 to 65. The authorities require residents to give voice samples when they apply for passports. All of this data is being entered into centralized, searchable government databases. While Xinjiang's systems are particularly intrusive, their basic designs are similar to those the police are planning and implementing throughout China.

The Chinese government should immediately shut down the IJOP platform and delete all the data that it has collected from individuals in Xinjiang, Human Rights Watch said. Concerned foreign governments should impose targeted sanctions, such as under the US Global Magnitsky Act, including visa bans and asset freezes, against the Xinjiang Party Secretary, Chen Quanguo, and other senior officials linked to abuses in the Strike Hard Campaign. They should also impose appropriate export control mechanisms to prevent the Chinese government from obtaining technologies used to violate basic rights. United Nations member countries should push for an international fact-finding mission to assess the situation in Xinjiang and report to the UN Human Rights Council.

Read the full report.

Read an interview with senior researcher Maya Wang.

More on Human Rights Watch's work on China.