HUMAN RIGHTS WATCH

May 1, 2019

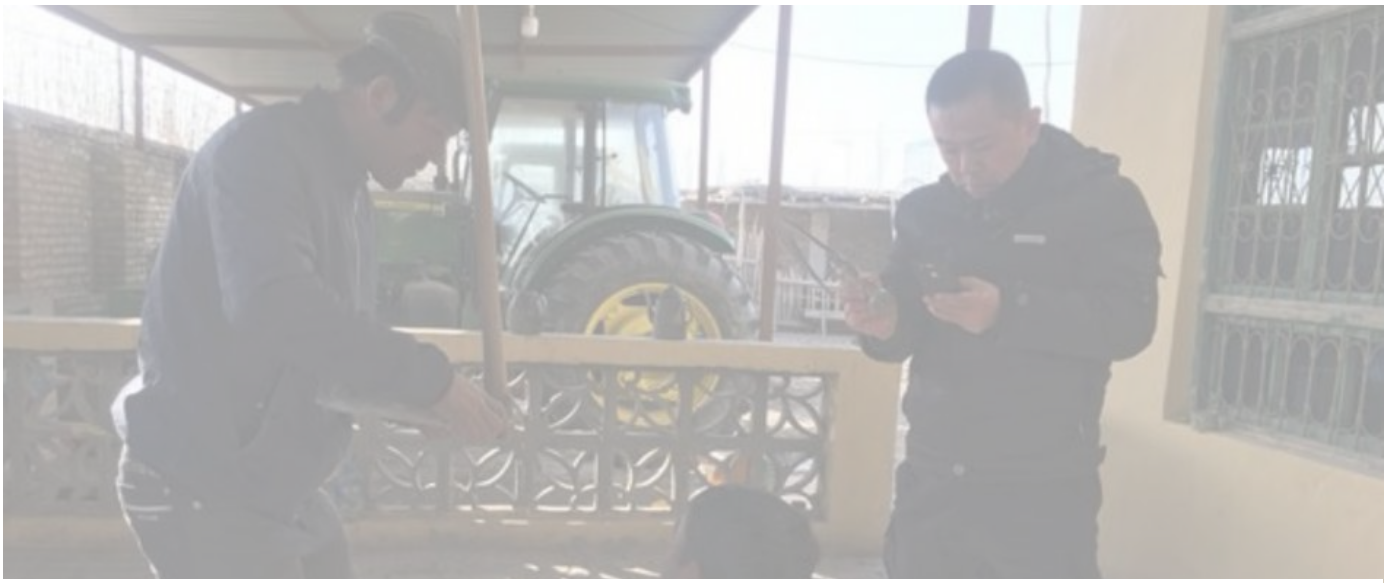
China's Algorithms of Repression

Reverse Engineering a Xinjiang Police Mass Surveillance App

Available In 简体中文 **English**

Summary

Since late 2016, the Chinese government has subjected the 13 million ethnic Uyghurs and other Turkic Muslims in Xinjiang to mass arbitrary detention, forced political indoctrination, restrictions on movement, and religious oppression. Credible estimates indicate that under this heightened repression, up to one million people are being held in "political education" camps. The government's "Strike Hard Campaign against Violent Terrorism" (Strike Hard Campaign, 严厉打击暴力恐怖活动专项行动) has turned Xinjiang into one of China's major centers for using innovative technologies for social control.



May 1, 2019 | Video

China's Mass Surveillance Phone App

"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."

This report provides a detailed description and analysis of a mobile app that police and other officials use to communicate with the Integrated Joint Operations Platform (IJOP, 一体化联合作战平台), one of the main systems Chinese authorities use for mass surveillance in Xinjiang. Human Rights Watch first reported on the IJOP in February 2018, noting the policing program aggregates data about people and flags to officials those it deems potentially threatening; some of those targeted are detained and sent to political education camps and other facilities. But by "reverse engineering" this mobile app, we now know specifically the kinds of behaviors and people this mass surveillance system targets.

The findings have broader significance, providing an unprecedented window into how mass surveillance actually works in Xinjiang, because the IJOP system is central to a larger ecosystem of social monitoring and control in the region. They also shed light on how mass surveillance functions in China. While Xinjiang's systems are particularly intrusive, their basic designs are similar to those the police are planning and implementing throughout China.

Many—perhaps all—of the mass surveillance practices described in this report appear to be contrary to Chinese law. They violate the internationally guaranteed rights to privacy, to be presumed innocent until proven guilty, and to freedom of association and movement. Their impact on other rights, such as freedom of expression and religion, is profound.

Human Rights Watch finds that officials use the IJOP app to fulfill three broad functions: collecting personal information, reporting on activities or circumstances deemed suspicious, and prompting investigations of people the system flags as problematic.

Analysis of the IJOP app reveals that authorities are collecting massive amounts of personal information—from the color of a person's car to their height down to the precise centimeter—and feeding it into the IJOP central system, linking that data to the person's national identification card number. Our analysis also shows that Xinjiang authorities consider many forms of lawful, everyday, non-violent behavior—such as "not socializing with neighbors, often avoiding using the front door"—as suspicious. The app also labels the use of 51 network tools as suspicious, including many Virtual Private Networks (VPNs) and encrypted communication tools, such as WhatsApp and Viber.

The IJOP app demonstrates that Chinese authorities consider certain peaceful religious activities as suspicious, such as donating to mosques or preaching the Quran without authorization. But most of the other behavior the app considers problematic are ethnic-and religion-neutral. Our findings suggest the IJOP system surveils and collects data on everyone in Xinjiang. The system is tracking the movement of people by monitoring the "trajectory" and location

data of their phones, ID cards, and vehicles; it is also monitoring the use of electricity and gas stations of everybody in the region. This is consistent with Xinjiang local government statements that emphasize officials must collect data for the IJOP system in a "comprehensive manner" from "everyone in every household."

When the IJOP system detects irregularities or deviations from what it considers normal, such as when people are using a phone that is not registered to them, when they use more electricity than "normal," or when they leave the area in which they are registered to live without police permission, the system flags these "micro-clues" to the authorities as suspicious and prompts an investigation.

Another key element of IJOP system is the monitoring of personal relationships. Authorities seem to consider some of these relationships inherently suspicious. For example, the IJOP app instructs officers to investigate people who are related to people who have obtained a new phone number or who have foreign links.

The authorities have sought to justify mass surveillance in Xinjiang as a means to fight terrorism. While the app instructs officials to check for "terrorism" and "violent audio-visual content" when conducting phone and software checks, these terms are broadly defined under Chinese laws. It also instructs officials to watch out for "adherents of Wahhabism," a term suggesting an ultra-conservative form of Islamic belief, and "families of those…who detonated [devices] and killed themselves." But many—if not most—behaviors the IJOP system pays special attention to have no clear relationship to terrorism or extremism. Our analysis of the IJOP system suggests that gathering information to counter genuine terrorism or extremist violence is not a central goal of the system.

The app also scores government officials on their performance in fulfilling tasks and is a tool for higher-level supervisors to assign tasks to, and keep tabs on the performance of, lower-level officials. The IJOP app, in part, aims to control government officials to ensure that they are efficiently carrying out the government's repressive orders.

In creating the IJOP system, the Chinese government has benefitted from Chinese companies who provide them with technologies. While the Chinese government has primary responsibility for the human rights violations taking place in Xinjiang, these companies also have a responsibility under international law to respect human rights, avoid complicity in abuses, and adequately remedy them when they occur.

As detailed below, the IJOP system and some of the region's checkpoints work together to form a series of invisible or virtual fences. Authorities describe them as a series of "filters" or "sieves" throughout the region, sifting out undesirable elements. Depending on the level of threat authorities perceive—determined by factors programmed into the IJOP system—, individuals' freedom of movement is restricted to different degrees. Some are held captive in Xinjiang's prisons and political education camps; others are subjected to house arrest, not allowed to leave their registered locales, not allowed to enter public places, or not allowed to leave China.

Government control over movement in Xinjiang today bears similarities to the Mao Zedong era (1949-1976), when people were restricted to where they were registered to live and police could detain anyone for venturing outside their locales. After economic liberalization was launched in 1979, most of these controls had become largely obsolete. However, Xinjiang's modern police state—which uses a combination of technological systems and administrative controls—empowers the authorities to reimpose a Mao-era degree of control, but in a graded manner that also meets the economy's demands for largely free movement of labor.

The intrusive, massive collection of personal information through the IJOP app helps explain reports by Turkic Muslims in Xinjiang that government officials have asked them or their family members a bewildering array of personal questions. When government agents conduct intrusive visits to Muslims' homes and offices, for example, they typically ask whether the residents own exercise equipment and how they communicate with families who live abroad; it appears that such officials are fulfilling requirements sent to them through apps such as the IJOP app. The IJOP app does not require government officials to inform the people whose daily lives are pored over and logged the purpose of such intrusive data collection or how their information is being used or stored, much less obtain consent for such data collection.

A checkpoint in Turpan, Xinjiang. Some of Xinjiang's checkpoints are equipped with special machines that, in addition to recognizing people through their ID cards or facial recognition, are also vacuuming up people's identifying information from their electronic devices. © 2018 Darren Byler

The Strike Hard Campaign has shown complete disregard for the rights of Turkic Muslims to be presumed innocent until proven guilty. In Xinjiang, authorities have created a system that considers individuals suspicious based on broad and dubious criteria, and then generates lists of people to be evaluated by officials for detention. Official documents state that individuals "who ought to be taken, should be taken," suggesting the goal is to maximize the number of people they find "untrustworthy" in detention. Such people are then subjected to police interrogation without basic procedural protections. They have no right to legal counsel, and some are subjected to torture and mistreatment, for which they have no effective redress, as we have documented in our September 2018 report. The result is Chinese authorities, bolstered by technology, arbitrarily and indefinitely detaining Turkic Muslims in Xinjiang en masse for actions and behavior that are not crimes under Chinese law.

And yet Chinese authorities continue to make wildly inaccurate claims that their "sophisticated" systems are keeping Xinjiang safe by "targeting" terrorists "with precision." In China, the lack of an independent judiciary and free press, coupled with fierce government hostility to independent civil society organizations, means there is no way to hold the

government or participating businesses accountable for their actions, including for the devastating consequences these systems inflict on people's lives.

The Chinese government should immediately shut down the IJOP and delete all the data it has collected from individuals in Xinjiang. It should cease the Strike Hard Campaign, including all compulsory programs aimed at surveilling and controlling Turkic Muslims. All those held in political education camps should be unconditionally released and the camps shut down. The government should also investigate Party Secretary Chen Quanguo and other senior officials implicated in human rights abuses, including violating privacy rights, and grant access to Xinjiang, as requested by the Office of the United Nations High Commissioner for Human Rights and UN human rights experts.

Concerned foreign governments should impose targeted sanctions, such as the US Global Magnitsky Act, including visa bans and asset freezes, against Party Secretary Chen 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.

Related Content

May 1, 2019 | News Release

China: How Mass Surveillance Works in Xinjiang

Methodology

This report is based on "reverse engineering" a copy of the IJOP app between January 2018 and February 2019.

Procurement notices for the IJOP system show it is supplied by the Xinjiang Lianhai Cangzhi Company (新疆联海创智公司).[1] That firm is a wholly owned subsidiary of China Electronics Technology Group Corporation (CETC, 中国电子科技集团公司), a major state-owned military contractor in China.[2] CETC announced, at a March 2016 press conference, the company had been awarded a government contract to build a big data program that would collate information about citizens' everyday behavior and flag unusual activities to predict terrorism.[3]

According to official media reports, government officials and police officers in Xinjiang use an IJOP app to communicate with the IJOP system.[4] Human Rights Watch obtained a copy of the IJOP app in early 2018. We enlisted Cure53, a Berlin-based security company, to "reverse engineer" the IJOP app in late 2018. Cure53's technical assessment, along with dozens of screenshots generated from the app's source codes, form the technical basis of this report. We showed the screenshots to a person who was familiar with the app, with whom we spoke during research about the IJOP system published in February 2018; he recognized the app.[5]

Human Rights Watch has released these screenshots, which are referenced throughout this report.

To reverse engineer an app means to disassemble it, looking at the data it contains and its design, to understand how it works. In this case, we sought specifically to understand how government officials and police officers are instructed to carry out surveillance tasks in Xinjiang. The version we examined was v2.1.2.7762, published on November 20, 2017.

We found that the IJOP app was developed by Hebei Far East Communication System Engineering Company (HBFEC, 河北远东通信系统工程有限公司), a company, at time of the app's development, fully-owned by CETC.[6] An important component of the app is the AcroPhone, a "unified communication system" listed on both CETC and HBFEC's websites as their products.[7] Human Rights Watch sent a letter to the chairmen of CETC and HBFEC seeking information on the app, the IJOP system, and related issues (see Appendix I), but had not received a response at time of writing.

Human Rights Watch did not log into the IJOP app, as we did not have a username and password to do so, nor did we connect to the IJOP system's servers to obtain data to populate the app. This limitation means that while we were able to recreate faithfully some of the pages and menus of the IJOP app, we were unable to do so for others. We also examined the app's source code, which provided insights into many of the pages and functions we were unable to recreate.

Statements from former Xinjiang residents used throughout this report were obtained through interviews Human Rights Watch conducted previously for our September 2018 report on Xinjiang.[8] To protect their identities, the names of all interviewees have been changed, and the location where they were interviewed, along with their place of origin and ethnicity, have been withheld. All those interviewed were informed of the purpose of the interview, its voluntary nature, and the ways in which the information would be used.

I. Background

> We must respond to the new ways in which hostile forces and terrorists are plotting crimes by implementing all-encompassing, round-the-clock, three-dimensional prevention and control [surveillance systems], to resolutely ensure that there are no blind spots, no gaps, no blanks unfilled [in our efforts].
> —Chen Quanguo, Xinjiang party secretary, in a directive issued on August 17, 2017[9]

Human Rights in China

The Chinese Communist Party (CCP, or "Party") has ruled China since it founded the People's Republic of China in 1949. The CCP controls the government bureaucracy, including the military, the police, and the judiciary. It also maintains a tight grip over many aspects of society and public life, including the mass media, internet, and academia. Human rights, including the rights to freedom of expression, association, assembly, and religion, are heavily curtailed. It is hostile towards human rights activists—from those who speak out against corruption to those who protest against environmental degradation—and punishes them with police harassment, detention, torture, and imprisonment. The CCP's level of social control has gone through harsh cycles with occasional periods of relative relaxation; the years under CCP Chairman Mao Zedong (1949-1976) were particularly tumultuous and brutal.

China's current leader, President Xi Jinping, has ushered in a period of escalating repression.[10] He scrapped term limits for the presidency in March 2018, indicating his intent to rule indefinitely.[11] He has instituted a slew of national security-related legislation that further restricts people's rights, has pushed to "Sinicize" religion (that is, exerting greater Party control), and initiated various campaigns to shore up loyalty to the Party.

In the ethnic minority regions of Xinjiang and Tibet, the cost of criticizing the government is enormous. The authorities regularly forcibly disappear and indefinitely detain perceived critics and opponents of the government. This is exemplified by the life sentence handed down to Uyghur economist Ilham Tohti in 2014, and the enforced disappearance of the Panchen Lama, an important Tibetan Buddhist figure, in 1995.[12]

Mass Surveillance in China

The CCP has long embraced mass surveillance. Since 1949, the state and the Party have relied on information gathering and social management tools, such as "*danwei*" work units, the "*hukou*" residency registration system, and "*dang'an*" secret political files, to monitor people and maintain tight social control.[13] Government agencies regularly collect a wide range of personal information about people, ranging from their political views to information about women's use of birth control, and link it to their national identification card number, without people having the ability to challenge such collection.

But since 1979, mass migration and privatization during the transition to a quasi-market economy have undermined the efficacy of these older practices.[14] The 1989 pro-democracy protests—which authorities repressed, killing untold numbers of peaceful protesters and bystanders—further jolted CCP leadership into the realization that it must bolster and broaden surveillance over an increasingly mobile and demanding society. Other changes in society, ranging from the advent of the internet, globalization, a wealthier state, and people's growing digital footprint, also contributed to the authorities' greater interest in developing technologies for social control.

The Ministry of Public Security significantly overhauled its intelligence-gathering infrastructure in the early 2000s to achieve "information dominance" for the purpose of social control and crime-fighting.[15] It launched the Golden Shield Project around 2000, which aimed to build a nationwide network of "information arteries" across the police force, "integrated information platforms" to consolidate such information, and command centers to analyze intelligence.[16] In 2003, the ministry began to adopt a policing model called "Intelligence-Led Policing" (情报指导警务), pioneered

by the British police in the 1990s, which entailed placing intelligence "at the center of all strategic and operational decision-making."[17] Intelligence-Led Policing relies on "seamless information sharing" among "strategic decision-makers, operational officers, and frontline cops."[18]

With the Golden Shield Project and Intelligence-Led Policing model, the Ministry of Public Security aimed to integrate information silos across the police force, reducing communication inefficiency between layers of police bureaucracy and enabling the police force to predict and respond quickly to threats.

CETC's "three-dimensional portrait and integrated data doors" – special machines that are used in some of Xinjiang's checkpoints to vacuum up people's identifying information from their electronic devices. This is placed at the entrance to the Aq Mosque, in Urumqi, 2018. Credit: Joanne Smith Finley

The 2008 Beijing Olympics gave the Chinese government, the CCP, and its mass surveillance agenda a further opportunity. The Party has increasingly treated "stability maintenance"—a euphemism for social control—as an overarching priority, and devoted enormous resources to security agencies for monitoring dissidents, breaking up protests, censoring the internet, and developing and implementing mass surveillance systems.[19] The 2008 protests by Tibetans across the Tibetan plateau on a range of issues including intrusive religious and cultural restrictions, and the 2009 riots in Urumqi, the capital of Xinjiang, prompted the government to step up mass surveillance and police recruitment in these minority regions.[20] Major meetings—such as the G20 in Hangzhou in 2016—are occasions for authorities to acquire new surveillance products and systems.[21]

It appears the Chinese government's dystopian projects are bearing fruit, as these mass surveillance systems have woven an ever-tightening net around people across the country. These systems are multi-layered and overlapping. The government issues every citizen a national identification card that is essential to accessing many public and private services. This "real name registration" requirement enables authorities to collect and compile vast databases of personal profiles linked to an individual's ID. At the same time, the government has been blanketing the country with closed-circuit surveillance cameras (CCTV).[22] Authorities have enlisted artificial intelligence technologies, provided by private companies—some with links to the state and the military—to help them automatically identify people from public surveillance footage streams and telephone calls; they are also using big data systems to identify individuals posing political threats.[23] All these systems are being developed and implemented without meaningful privacy protections against state surveillance. The depth, breath, and intrusiveness of the Chinese government's mass surveillance on its citizens maybe unprecedented in modern history.[24]

These mass surveillance systems remain unchallenged in China because there are few meaningful checks on government powers. The Ministry of Public Security is accountable to no one except to the CCP—it is not required to report surveillance activities to any other government agency, or to publicly disclose this information. It is all but impossible for people to know what personal information the government collects, and how the government uses, shares, or stores their data.[25]

Mass Surveillance in Xinjiang

While mass surveillance systems in Xinjiang are based on the same basic designs described above, Xinjiang authorities seem to have gone the furthest in China in implementing them, contending that aggressive use of such systems is necessary for countering "the three [evil] forces"—separatism, terrorism, and extremism.[26] There have been a number of reported violent incidents in Xinjiang—notably the Urumqi market bombing in 2014—and the Chinese government has characterized these incidents as terrorism, blaming some of them on foreign groups.[27] The Chinese government claimed in a March 2019 White Paper on Xinjiang, that it had arrested nearly 13,000 terrorists in Xinjiang since 2014.[28] However, obtaining accurate accounts of violence in Xinjiang is extremely difficult because the government keeps tight control over this information. To what extent these incidents in Xinjiang are linked to foreign groups—as opposed to domestic incidents triggered by local or even interpersonal grievances—is also unclear.[29] Chinese laws also define terrorism and extremism in an overly broad and vague manner, such that a large range of activity relevant to ethnic and religious expression and custom are punishable and prohibited, such as wearing "abnormal" beards or veils in public places or naming babies with names that "exaggerate religious fervor."[30]

Under the Strike Hard Campaign, Xinjiang authorities have collected biometrics, including DNA samples, fingerprints, iris scans, and blood types of all residents in the region between the ages of 12 and 65.[31] Additionally, authorities have required residents to give voice samples when they apply for passports.[32] All of this data is being entered into centralized, searchable databases.[33] The collection of these biometrics is part of the government's drive to form a "multi-modal" biometric portrait of individuals and to gather ever more data about its citizens. All of this data can be linked in police databases to the person's identification number, which in turn is linked to a person's other biometric and personal information on file, such as the kind of data described in this report. The use of mass surveillance extends beyond Xinjiang and into the Turkic Muslim diaspora as authorities pressure them to provide detailed information about themselves, including their address, phone number, and school or workplace.[34]

Xinjiang can best be described as one of several clusters of mass surveillance industries in China, each catering to the local governments where they are based, with ideas cross-fertilizing between these clusters. One hallmark of Xinjiang's mass surveillance infrastructure is "convenience police stations"—street-corner police stations that together form a dense network of control through the region—that were brought to Xinjiang when Party Secretary Chen Quanguo transferred to the region from Tibet.[35] Another basic building block of Xinjiang's mass surveillance infrastructure is the "grid system" of dividing populations into geometric units for tighter surveillance and service provision, which first underwent trials in Beijing in 2004.[36]

While many of the companies that enable mass surveillance in Xinjiang are Chinese companies, foreign technology, companies, and investment also play a role in supporting the Xinjiang authorities' abuses. US-based company Thermo Fisher Scientific supplied the Xinjiang police with some of the DNA sequencers at a time when those authorities were building large-scale infrastructure to process DNA samples of Xinjiang residents.[37] A Yale University geneticist collaborated—and shared DNA samples—with a Ministry of Public Security researcher in 2014. That collaboration enabled the ministry to identify Uyghurs' ethnicity by examining their genetic materials.[38]

The Central IJOP System

The findings of this report are based on an examination of the IJOP app interface—rather than the central system itself, which remains largely a black box. The current findings enrich what Human Rights Watch previously knew about the system, though many questions remain.

An article written by officials from the Xinjiang Bureau of Civil Affairs shows how they visited villagers and collected their information using the IJOP app in Akto County, Kizilsu Kirghiz Autonomous Prefecture, Xinjiang. Source: Xinjiang Minshengwang (新疆民生网)

Human Rights Watch's previous research into the IJOP central system, which was based on government procurement documents, indicated that it gathers information from multiple sources or machine "sensors."[39] One source is CCTV cameras, some of which have facial recognition or infrared capabilities (giving them "night vision"). Another source is "wifi sniffers," which collect the unique identifying addresses of computers, smartphones, and other networked

devices.[40] The IJOP system also receives information from some of the region's countless checkpoints and from "visitors' management systems" in access-controlled communities, such as residential areas and schools. In addition, these documents say some of these checkpoints "receive, in real time, predictive warnings pushed by the IJOP" so they can "identify targets ... for checks and control."[41] Our current research into the IJOP app suggests the IJOP system is pulling location information from these sensory systems to chart the movement or "trajectories" of people.

We also know—through reverse engineering the IJOP app and examining its source code—that the IJOP central system seems to draw on detailed information collected by the Xinjiang authorities about package delivery.[42] Presumably, there is a system tracking such information and feeding it to the IJOP system, which draws on some of that data in populating the app.

We know that there are at least two other apps that Xinjiang government officials use to gather personal data from residents: an app for Xinjiang officials when they conduct intrusive home visits ("新疆入户走访"[43]), and another app for collecting data on migrant workers ("基础工作小助手"[44]). While we have not had access to them, some local government reports state that the data collected via these other apps feed into the IJOP system.[45]

However, we do not know if—and how—the IJOP system is connected to other surveillance systems in China. For example, in the IJOP app screenshot tracking people who have "gone off-grid" (p. 39), the drop-down menu available for government officials includes an option to note that the person in question "has left Xinjiang." Presumably, if the IJOP system is connected to its counterparts elsewhere in China, it would have "known" that, and thus there would be no need to flag or investigate that person.

While the IJOP central system—and much of Xinjiang's mass surveillance systems—are managed by the Public Security Bureau, police officers are not the only Chinese government officials tasked with mass surveillance. Since 2014, Xinjiang authorities have sent 200,000 cadres from government agencies, state-owned enterprises, and public institutions to regularly visit and surveil people. Authorities call this initiative "*fanghuiju*" (访惠聚). [46] In October 2016, authorities initiated a related effort, called the "Becoming Family" (结对认亲) campaign, which involves requiring officials to stay in Turkic Muslims' homes regularly. [47] There is no evidence to suggest that families can refuse such visits. During these intrusive home visits, the cadres perform several functions, including surveillance and inputting the data of families into apps such as the IJOP.[48]

The IJOP system requires officials to respond to many perceived abnormalities in people's lives, a grueling task for government officials. One official lamented that many colleagues have "worked so hard" to meet the IJOP's appetite that "their eyes are so tired and reddened."[49] These officials are under tremendous pressure to carry out the Strike Hard Campaign. Failure to fulfill its requirements can be dangerous, especially for cadres from ethnic minorities, because the Strike Hard Campaign also targets and detains officials thought to be disloyal.[50] It is unclear how long Xinjiang authorities can sustain this high volume of labor-intensive investigations, though presumably authorities may be able to collect some of the personal information in a more automated manner in the future.

Currently, much of the IJOP system appears to function as simple conditional statements—if a, then b (for example, if the person who drives the car is not the same as the person to whom the car is registered, then investigate this person)—and the app suggests the IJOP system may not be as sophisticated as authorities have publicly advertised.[51] To what extent the IJOP central system is currently using big data algorithms in analyzing the collected personal data is unclear.

The IJOP system is generating a massive dataset of personal information, and of police behavior and movements in Xinjiang. Yet it is not known how the authorities plan to use such data. In 2017, the state-owned company that built the IJOP, CETC, established a new big data national laboratory for "social security risk awareness, prevention, and control"[52] in Urumqi, together with the Xinjiang police "special investigative unit" and Ministry of Public Security big data researchers. The lab dispensed grants for the first time in July 2017 to 16 grantees; one of the co-chairs of the panel evaluating the grantees was the vice-chief of Xinjiang's police.[53] An examination of the list of research topics suggests Chinese police are developing capabilities for "reality mining"[54] that go beyond existing forms of surveillance. By studying how people interact, using data gathered by machines such as their mobile phones or checkpoints—an approach considered more accurate than existing subjective sources for analyzing such interactions—the authorities seemingly hope to be able to understand in a more fine-grained way how people lead their lives: whom they talk to, where they go, and what they do. The goal is apparently to identify patterns of, and predict, the everyday life and resistance of its population, and, ultimately, to engineer and control reality.[55]

II. How the IJOP App Works: An Overview

> Party Secretary Ding Jian explained the IJOP system in detail.... He randomly chose one of the households [in the village], and the technician immediately pulled out the...positioning coordinates as well as relevant information about the family.... [The party secretary] randomly chose a vehicle number and asked the operator to pull up the vehicle's location.
> —Village-based work team report, describing the village CCP secretary in Tekes County demonstrating to his superior how the IJOP system and app works, February 2018

The IJOP app is a multi-functional tool. Beyond its three broad, main functions[56]—data collection, filing of reports, and prompting "investigative missions" by police—the app has a range of other functions, including:

- Communication function: The IJOP app relies on AcroPhone (AcroUC), a "unified communication system," for officials to communicate across platforms (such as voice messages, emails, telephone calls).

- Geolocation and map functions: The IJOP app logs the police officer's GPS locations and other identifying information when they submit information to the IJOP app. The IJOP app uses a map functionality by Baidu, a major Chinese technology company, for purposes including planning the shortest route for police vehicle and officers on foot, according to the app's source code.

- Search function: The IJOP app allows officials to search for information about people using their name, ID number, household number used to access public utilities (户号), and building address (see Appendix III). In addition, officials can access, upon approval of their superiors, the "full profile" of a given individual.

- Facial recognition function: The IJOP app uses a facial recognition functionality by Face++—a well-known facial recognition company in China. It is used to check whether the photo on the ID matches the person's face or for cross-checking pictures on two different documents.[57]

- Wifi detecting: The IJOP app appears to collect data about wireless networks in range of the device. The collected data includes SSID (the service set identifier, or the name of a Wi-Fi network), encryption method, and GPS locations. Our technical investigation suggests that this possibly serves the purpose of creating a map of the existing wireless networks in the region, also known as "War Driving."[58] This function could also potentially be used to identify and target weakly secured wireless networks and to join them for the purpose of surveillance and infiltration. It can also be used to understand the population density, connectivity, and the produced data volume of a given area. However, it is unclear how this functionality—or the data it gathers—is used.

Data Collection

The IJOP app prompts government officials to collect detailed personal data from people in Xinjiang.

April 23, 2019 | Video

Screen 1

Screen 1

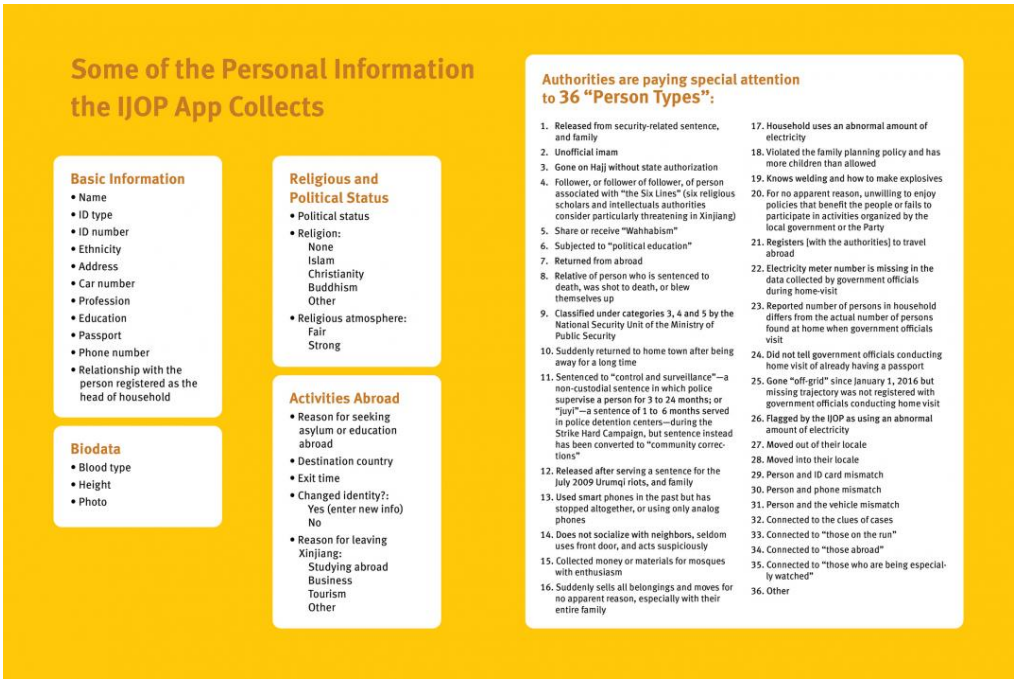
In screen 1, officials are prompted to choose the circumstances under which information is being collected by using a drop-down menu. The five choices are:

- "during home visits,"
- "on the streets,"
- in "political education camps,"
- "during registration for those who travel abroad," and
- "when collecting information from whose 'hukou' (or registered residency) is in Xinjiang but living in the mainland."[59]

Although not shown on the screenshot, officials with "administrative rights"[60] —likely higher-level officials—are also presented with a sixth choice: "when collecting information from foreign nationals who have entered [Xinjiang]."

Officials are then prompted to log and submit to the IJOP central system a range of information about the person, from the person's height, to their blood type, to their political affiliation.

There is a second main page that belongs to this set of data collection tasks, but we were unable to generate it when reverse-engineering the app. We examined the source code and found that this second page is prompting officials to collect even more information from people, including their religious and political status and activities abroad. This page also reveals that there are 36 "person types" to whom the authorities are paying special attention.



On this page, the IJOP app requests different types of data depending on the type of situation in which information is being collected. For example, when officials are collecting information from people "on the street," "in political education camps," or "during registration for those who have gone abroad," the app further prompts them to choose from a drop-down menu whether the person in question belongs to one of 36 types of problematic "person types."

Filing Reports

The app allows officers to file reports about people, vehicles, objects, and events they find suspicious. Human Rights Watch was able to replicate most of the pages in this set of tasks, and we have included some of them in Appendix IV. They are structured similarly to each other, in that they ask officers to log a written description of the suspicious person, vehicle, or event, log its location and identifying information (for example, license plate number, or ID card number), and add any relevant photos or audio recordings.

Investigative Missions

The most interesting—and revealing—part of the app is the group of tasks called "investigative missions" (调查任务). Mission instructions are sent directly via the IJOP central system to officers, requiring them to investigate certain individuals, vehicles, or events and provide feedback.

The IJOP app source code contains two simple mock examples. One states the person's problem:

Suspicious person Zhang San, whose address is Xinjiang Urumqi, ID number 653222198502043265, phone number 18965983265. That person has repeatedly appeared in inappropriate locations, and he displays [or his clothing shows] strong religiousness.[1]

Another contains a mock mission:

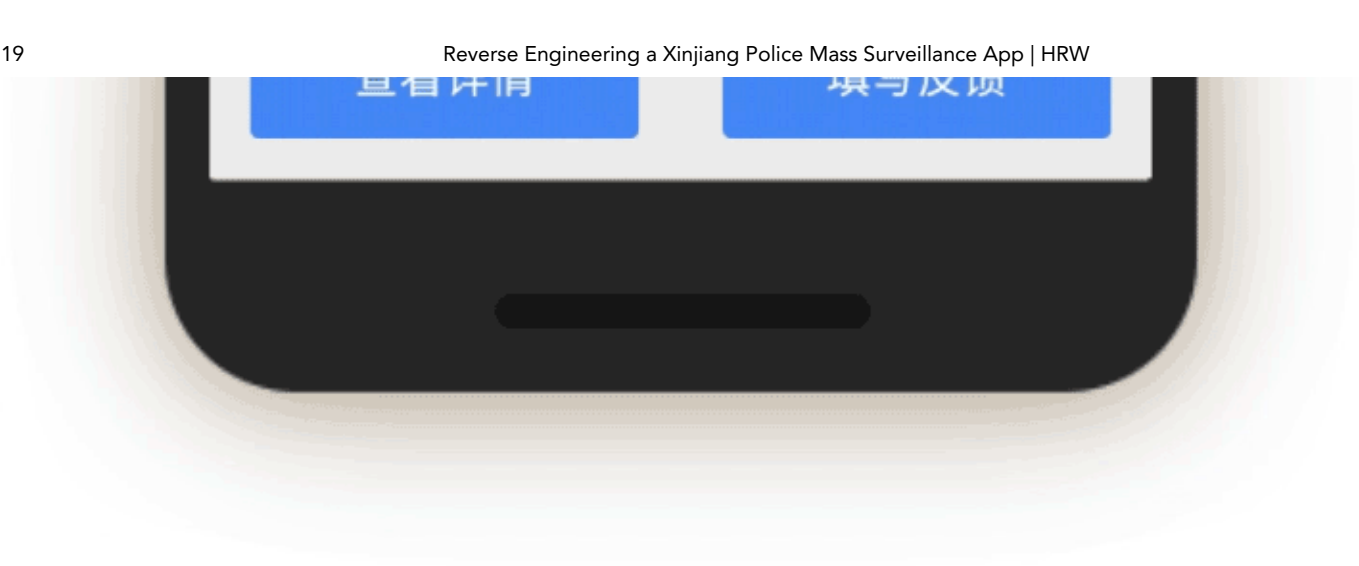
Reporter name: Zhang Sanfeng

Report text: Suspicious person Maimaiti Muhemuti, who originally lives in Xinjiang's Urumqi, ID number 653222198502043215, phone number 13803021458.

Report time: 2017-09-25 14:01:53

[Mission] text: Please carefully investigate whether he is still lives in Urumqi and investigate his family situation.


64% 15:07
事件详情
事件描述
调查对象姓名
调查地址
调查对象电话
未知
核查要求
未知
任务开始时间
工作状态



Screen 2

In screen 2, the official receives a description of the mission. The official can then view the details of the mission, conduct their investigation, and then fill out the feedback form. The missions can entail collecting extensive personal information from the individual.

In screen 3, officials are prompted to collect further identifying information about people's vehicles by opening related screens with information about the vehicle, including color and type, as well as the license plate number and a picture of the vehicle. Entering such information presumably enables cameras equipped with artificial intelligence capabilities to recognize and keep track of the vehicle as it travels and passes through vehicle checkpoints.

April 23, 2019 | Video

Screen 3

Screen 3

Officials are also prompted to log whether the people in question use a list of 51 "suspicious" internet tools, and if so, their account number.[61] Most of these tools are foreign messaging tools, such as Viber, WhatsApp, and Telegram, but also include Virtual Private Networks (VPNs).

Officials are also prompted, through related screens, to log individuals':

- Bank information (which bank they use and the bank account number),
- Family members (name, ID number, relationship, phone number), and
- "Suspiciousness," and, if so, explain whether they require further investigation.

III. Categories of People Authorities Find Suspicious

The investigative missions reveal the categories of people the authorities are focused on:

- People who move into or out of their registered residency (or "*hukou*") area:
  - **Internal migrants**;
  - People who have go abroad "for too long" **("overdue" persons**); and
  - People returning **from abroad**
- People who have "problematic" relationships:
  - People targeted in **"Operation 913"**;
  - Embassy Alert; and
  - **"Four associations"** ;
- People who use an **"unusual" amount of electricity**;
- **People who have gone "off-grid"** ;
- People with **mismatched identities**;

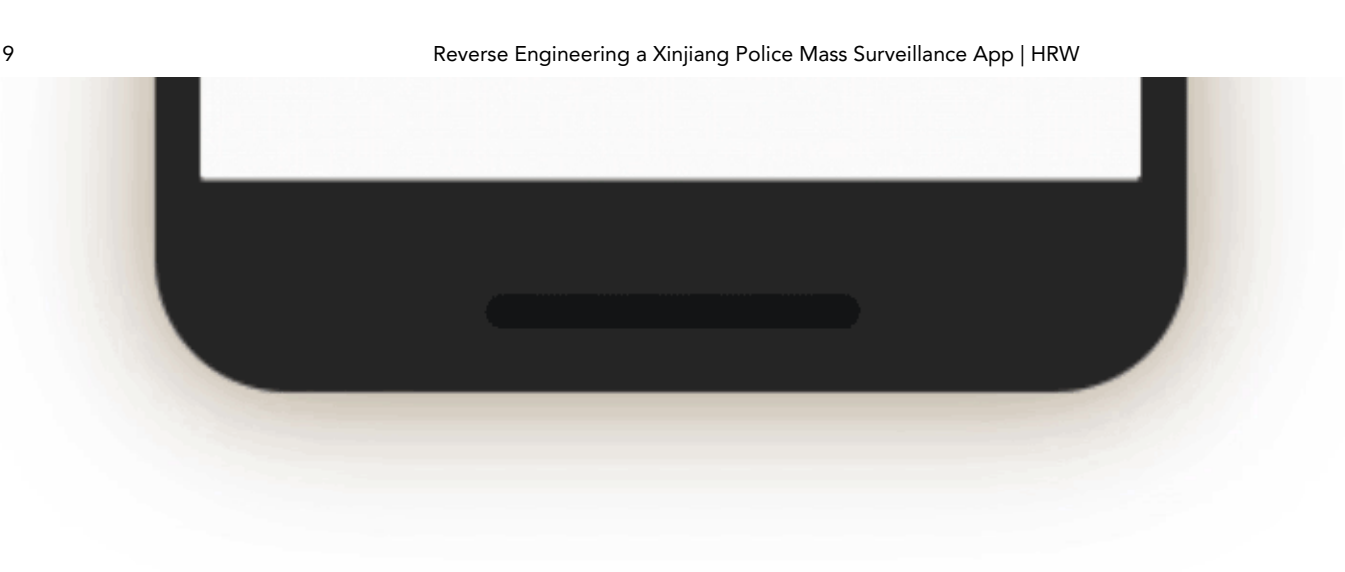
- **"Problematic" individuals** ;
- "**Problematic" vehicles** ;
- "Matched" **persons** ; and
- "Matched" **vehicles**

People Who Move into or out of Registered Residency Area

Internal Migrants

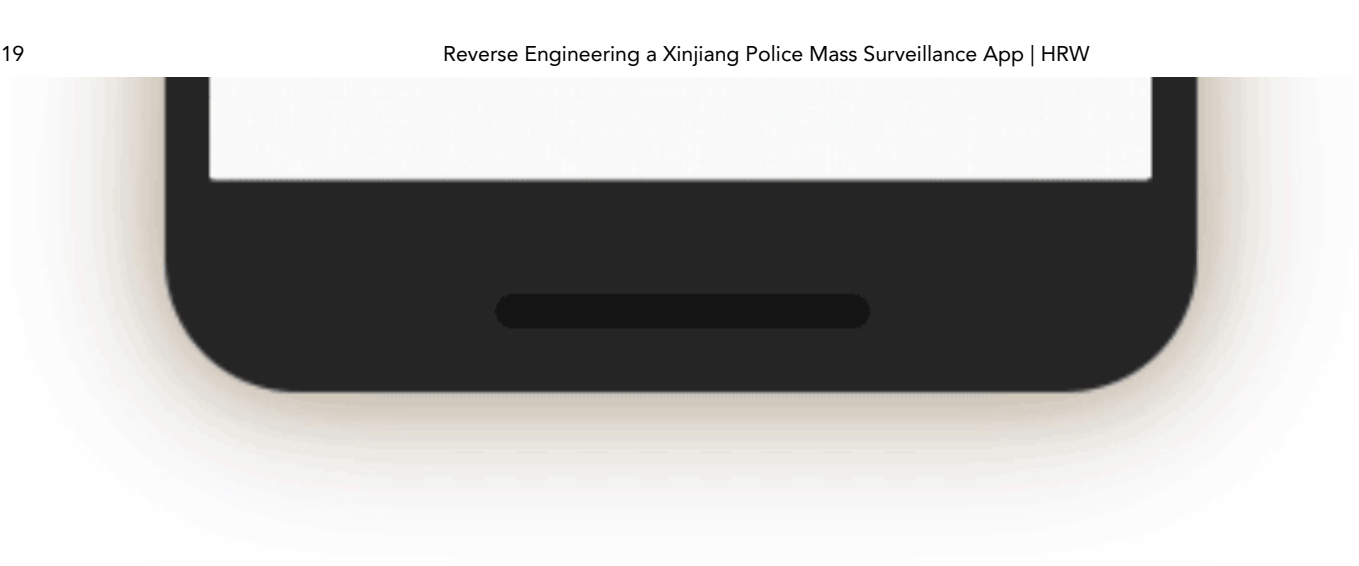
Analysis of the IJOP app suggests that Xinjiang authorities target internal migrants—those who are found outside their hukou area—for heightened monitoring and surveillance.[62] The IJOP system sends officers alerts with the "trajectory" information of a person who has moved into, or out of, their registered locale. Screens 4 and 5 are nearly identical except screen 4 is for people who have moved into a particular locale and screen 5 is for those who have moved out of that locale.


76% 16:05
人员流入地
姓名：
姓名
身份证号：
身份证号
手机号码：
手机号码
性别：
性别
居住地址：
居住地址
轨迹信息：
轨迹信息



Screen 4


68% 15:26
人员流出地详情
事件描述
流口信息
姓名
身份证号
手机号码
性别
居住地址
轨迹信息

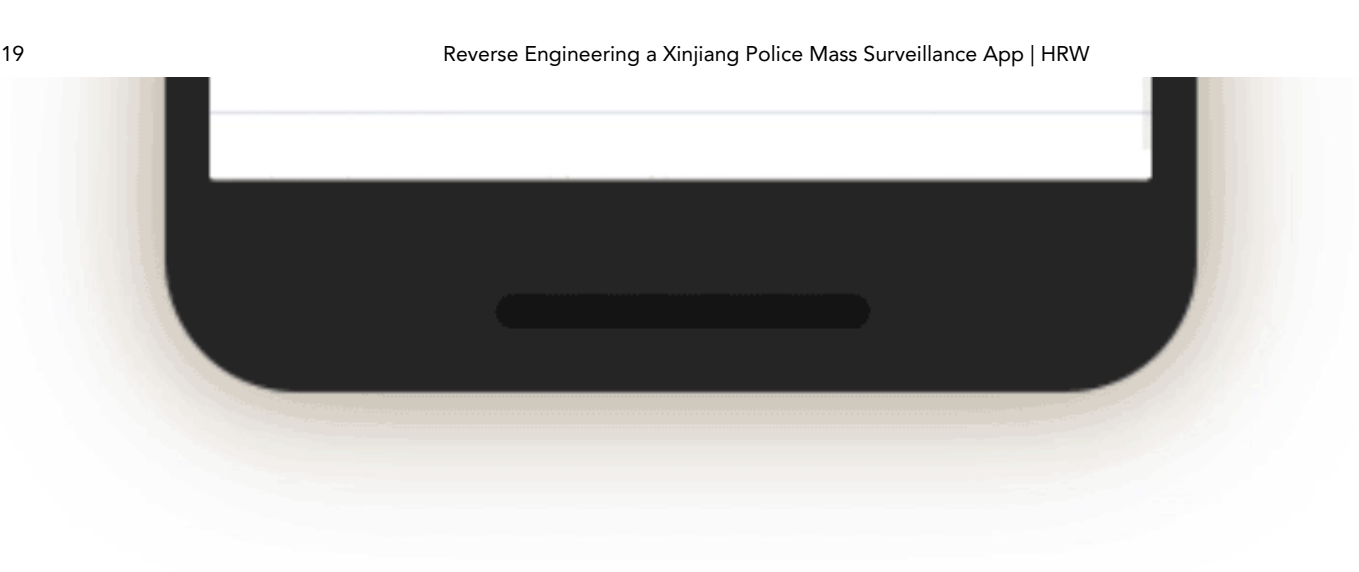


Screen 5

Officials—likely those who are in the locale to which the migrants have moved, judging from the context—are dispatched to visit the internal migrants who have been thus flagged, or people associated with them. Screen 6 suggests that officials are instructed to find out when the migrants move in, reasons for the move, their temporary address, and the personal particulars of people related to this person. Then, on a subsequent screen, officials are prompted to add the name, ID number, and phone number of each related person, and whether this migrant is suspicious.

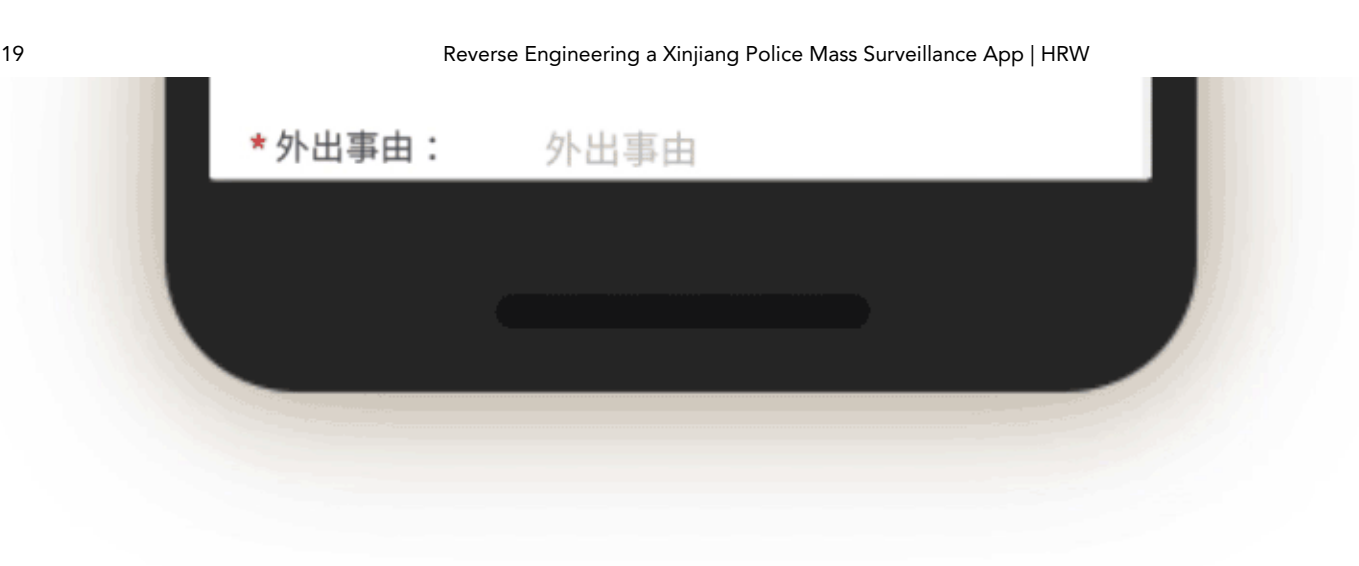
Similarly, officials are dispatched to investigate cases of people who have left their locale. The list of questions that officers are prompted to ask is similar (see screen 7). Again, the purpose is to track where people have gone, their relationships, and who they are travelling or spending time with.


76% 16:05
人员流入地
事件描述
走访对象
姓名：
姓名
身份证号：
身份证号
手机号：
手机号
性别：
未知
地址：
地址
新增走访对象
* 流入人员与走访对象关系：
未选择



Screen 6

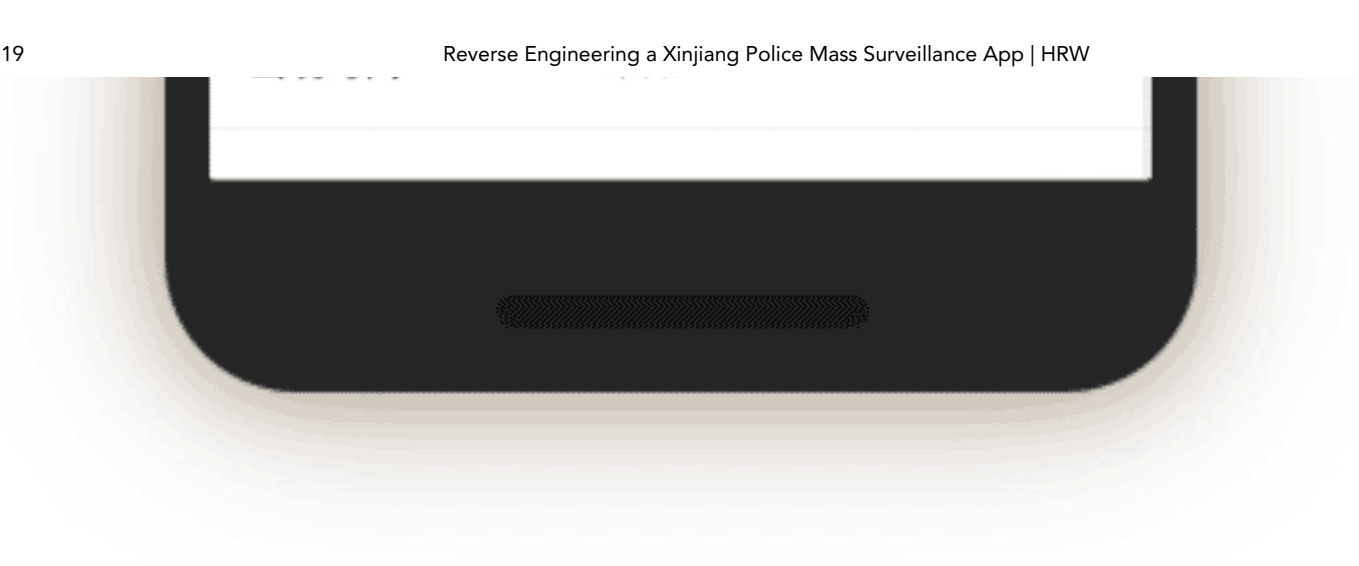

76% 16:05
人员流出地
事件描述
走访对象
姓名：
姓名
身份证号：
身份证号
手机号：
手机号
地址：
地址
照片
新增走访对象
* 关系：
未选择



Screen 7

People Who Go Abroad “For Too Long”


76% 16:05
逾期未归详情
人员详情
姓名 未知
性别 未知
国籍 未知
手机 未知
户籍地址 未知
身份证号 未知
证件类型 未知
证件号码 未知
出境口岸 未知
出境时间 未知

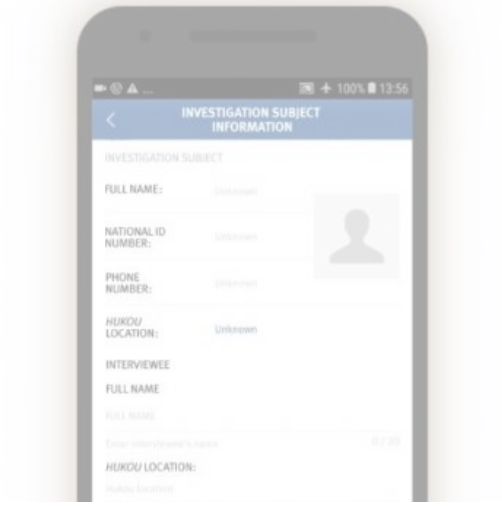


Screen 8

“Investigative mission” instructions are also sent to officers to look into people who went abroad or have been abroad “for too long” (逾期未归, or “overdue” persons). Screen 8 gives officials detailed information about such individuals, including which country they went to, reason for leaving, and their last recorded movement or “trajectory” in the country.

Officials are prompted to investigate such cases by interrogating the person in question or their family members and other social relations. The app prompts the official to investigate whether this person has gone abroad, and if so, which country they went to and the reasons for the trip (see screen 9).[63]

The app then prompts officials to add the person’s contacts abroad by opening a related page. Finally, the app asks officials to note if they think this person’s activities abroad are suspicious, and to describe the reasons for their suspicion.



April 23, 2019 | Video

Screen 9

Screen 9

If the officer is interrogating an "overdue person," the app also prompts the officer to check the person's phone. Officials are prompted to check and log, via a drop-down menu, whether the person's phone contains "suspicious content," including a VPN, "unusual software (or software that few people use)," "harmful URLs [or webpages]," or "violent terrorism audio-visuals."

People Returning from Abroad

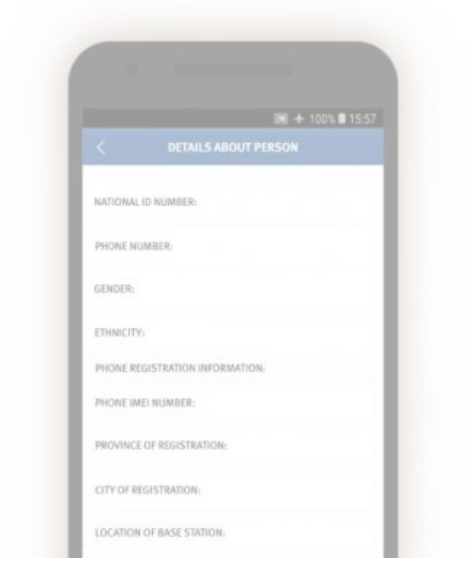
Another apparent function of the "investigative mission" feature of the IJOP app is the "prevention of people from returning from abroad."[64] This is an objective that is repeatedly referenced in official documents of Xinjiang's Strike Hard Campaign, one which appears to stem from concerns about returning "jihadists."[65] In practice, it means heightened restrictions on border crossings.[66]

The details of this task are not clear because we were unable to generate the relevant pages through reverse engineering. The source code suggests that this mission flags irregularities concerning a person's passport and immigration status, and that it allows those with administrative rights to designate responsibility for handling a person flagged in this category to another official.[67]

People Who Have Problematic Relationships

People Targeted in Operation "913"

The IJOP app reveals that officials are prompted to investigate people identified as targets in a crackdown with the code name "913."[68] Evidence contained in the IJOP app suggests the "913" crackdown focuses on individuals with "problematic" content and software on their mobile phones.[69] In screen 10, the IJOP system sends an alert to officials about such a target, giving extensive, identifying details about the target's phone, including the phone's unique identifier (IMEI number), base station information that can be used to track the movement of the phone user[70], where this person can generally be found, and whether the person has removed "unlawful software" from the phone.

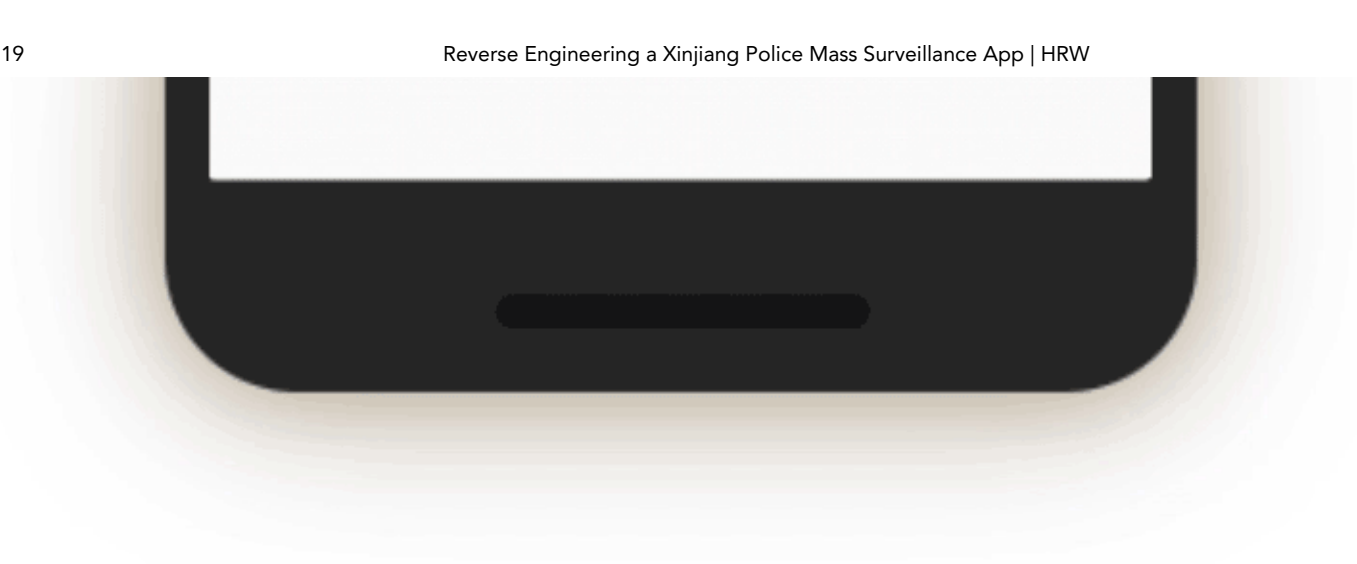


April 23, 2019 | Video

Screen 10

Screen 10


73% 15:50
境外联系人
保存
姓名 *
姓名
请输入姓名
0 / 20
人员信息 *
人员信息
人员关系
未选择
备注
备注
选择软件 *
未选择
选择软件 *
使用账户



Screen 11

Although we were unable to generate the screenshot for what appears to be the corresponding feedback page, entitled "feedback [form] on mobile phone investigation"[71] (手机调查反馈), that page's source code shows that the official is prompted to probe the "913" target or their relations by asking them about their phone and software use, such as why they use the "problematic" software. This feedback form appears to be the only page in the app that uses the term "terrorism," and we found no additional references to it in the source code.[72] Given the context, it might be that the official is prompted to note if the mobile phone or software use involves terrorism. The officials then note whether the person they are talking to seems suspicious and requires further police investigation.

The feedback page leads to subsequent screens for the officials to log information, which we were able to generate. In screen 11, the official can log people's foreign links and software they use to contact people outside China. A drop-down menu lists eight foreign communication and VPN tools: Hotspot VPN, IPSEC, L2TP, line, Viber, VPN dialogs, WhatsApp, and Payeco (a Chinese e-payment tool, 易联). The individual's account name for each tool or app is also logged.

Former Xinjiang residents told Human Rights Watch government officials and police routinely ask them for their phones and check their content without an explanation or warrant. According to Nurmuhemmet, a Turkic Muslim from Xinjiang:

> I was driving when I was stopped by the traffic police…. Then a few SWAT police officers came and demanded that I give them my phone. I did, and they plugged the phone in…. There were different kinds of cables for different types of phones. They plugged in my iPhone, but I didn't see what they were searching for. They handed the phone back to me after five minutes, and I was allowed to leave. Then a few days later when I was at the gas station, my wife also had her phone checked while waiting for me. Earlier, the neighborhood office told residents that they can go to the police to get their phones checked "for free" to see if there's anything "problematic." [73]

Nurmuhemmet said people were scared because it is unclear to them what exactly was being banned:

> People didn't know if what they have on their phones – apps, website content – is considered "unlawful" or "terrorist." I don't know what the unlawful content is either – I've heard about it, but I haven't never seen it.[74]

The fact that people are left guessing what content may irk the authorities reflects the arbitrary nature of online and offline surveillance in the region. Many interviewees told Human Rights watch they refrain from saying anything substantial when communicating with their families or neighbors, or on social media.

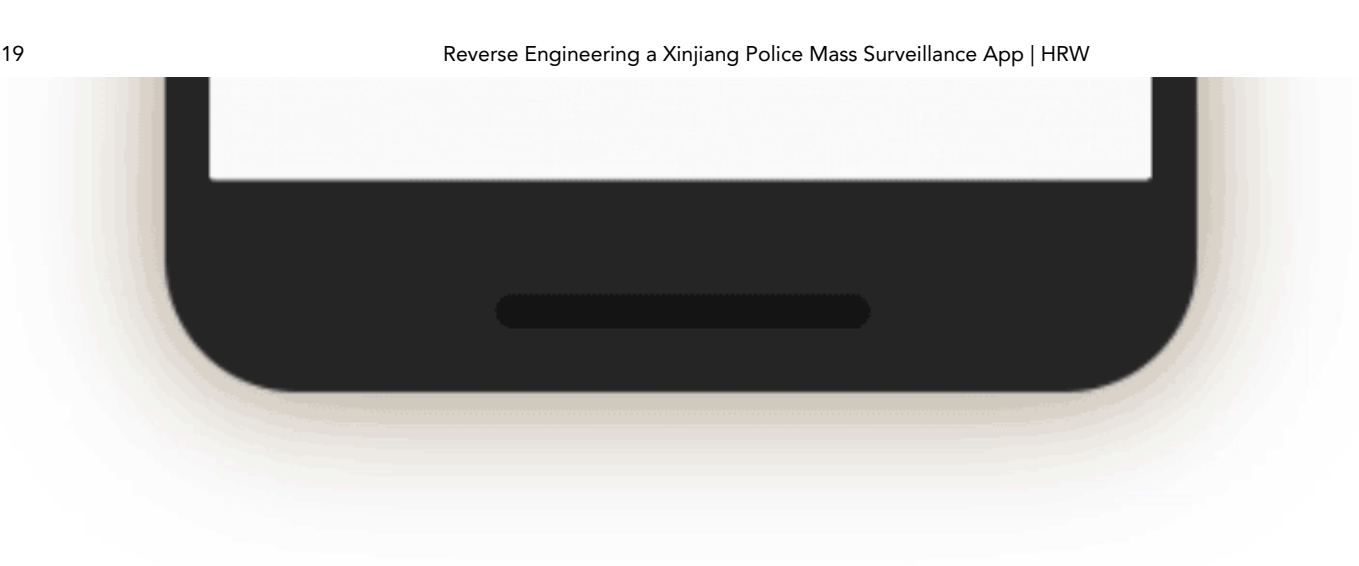
A number of interviewees said they or their family members have been detained for having foreign software such as WhatsApp or a VPN on their phones during these checks. Inzhu, who resides outside China but whose husband travels regularly back to Xinjiang, said:

> [M]y husband…told me that they took his phone and they found WhatsApp on it, and they handed the phone back. He told them in [the foreign country he lives in], a new phone comes with WhatsApp already installed. So, they asked for a receipt, and I sent my husband a receipt for the phone.[75]

Shortly after, the authorities took Inzhu's husband away to a political education camp, where, as best we can ascertain, he remains in detention.

Embassy Alert


73% 15:52
领馆预警
姓名：
身份证号：
身份证照片
相似度
采集照片
采集位置：
身份标签：
户籍地址：
处置措施：
确认核查

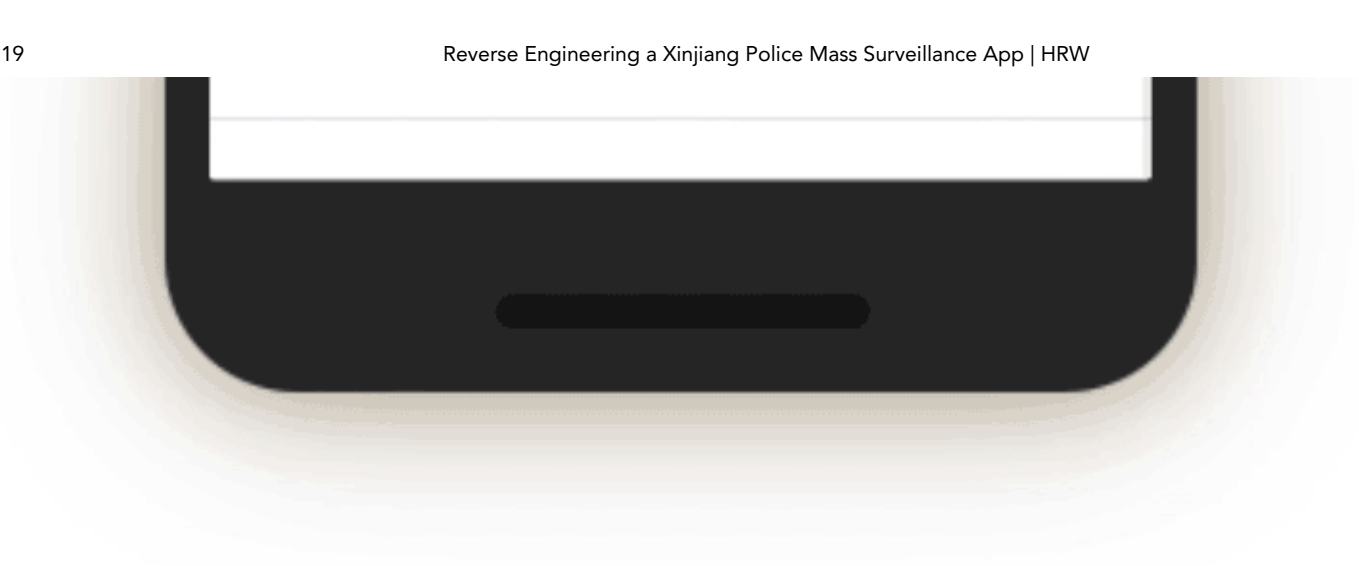


Screen 12

The IJOP app seems to send officials what it calls “embassy alert.” Screen 12 displays the person’s ID number, hukou address, and “disposal measures.” There is also a facial recognition component, as the screen shows the extent to which the person’s ID photo matches the photo of that person. At the bottom of the screen, the officer can click on the blue bottom, which says “confirm [and] check.” The purpose of this page is not entirely clear, but this page may be identifying people associated with embassies—either embassy staff or foreign nationals—and ordering officials to check them or to take certain measures against them as specified by the IJOP system.

“Four Associations”


76% 16:05
四关联
事件描述
走访对象
姓名：
姓名
身份证号：
身份证号
手机号：
手机号
地址：
地址
新增走访对象
* 与“四关联”人员关系：
未选择
现使用手机号：
现使用手机号



Screen 13

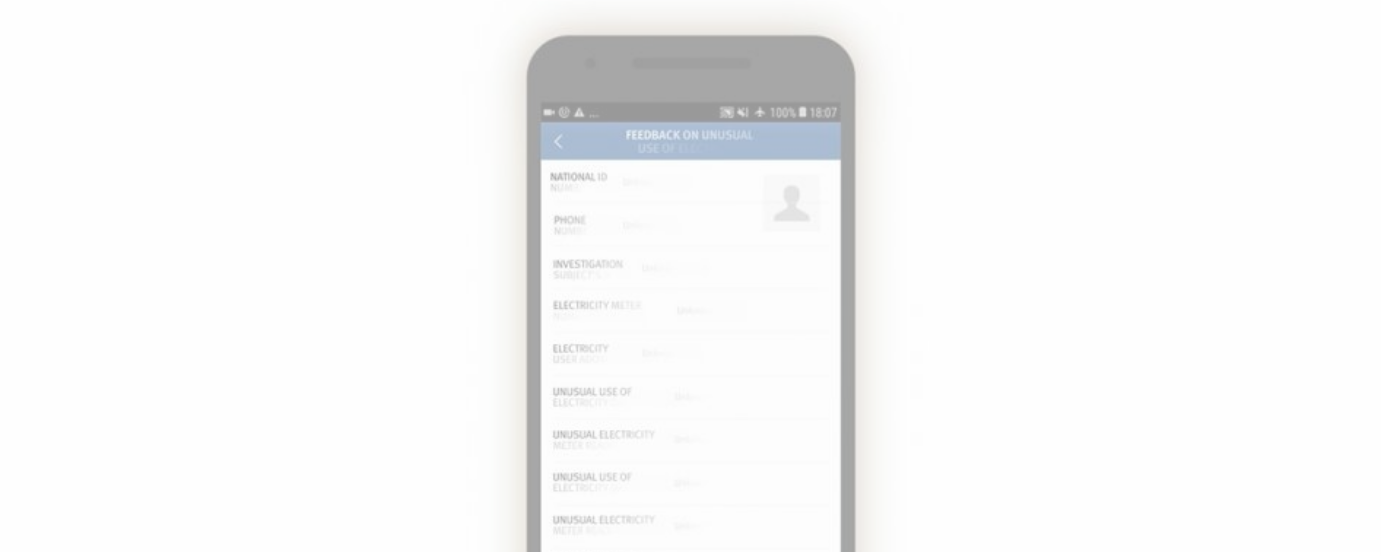
The IJOP app suggests Xinjiang authorities track people's personal relationships and consider broad categories of relationship problematic. One category of problematic relationships is called "Four Associations" (四关联), which the source code suggests refers to people who are "linked to the clues of cases" (关联案件线索), people "linked to those on the run" (关联在逃人员), people "linked to those abroad" (关联境外人员), and people "linked to those who are being especially watched" (关联关注人员).

The IJOP app suggests the IJOP center sends alerts to officials about people with these problematic relationships, and prompts officials to further investigate and provide feedback on these relationships along with details about the person (see screen 13). The officer is also prompted to note the person's behavior, and whether the person seems suspicious and needs to be investigated further.

Unusual Electricity Use

The IJOP app appears to draw from a database of people's electricity usage and send officers to investigate and provide feedback on those determined to have used an "unusual" amount of electricity, indicating that the authorities are surveilling electricity usage across Xinjiang's population.[76]

In screen 14, the officer is presented with an alert detailing the person's electricity usage, including the dates when unusual power consumption was recorded, and the relevant meter reading.



April 23, 2019 | Video

Screen 14

Screen 14

The official is prompted to investigate the reasons for unusual electricity consumption. The official can choose from a drop-down menu that allows them to note if the person:

- Had purchased “new electronics for domestic use”;
- Was doing “renovation”;
- Is a “farmer”;
- Possess “cutting or wielding tools or other electronics that have no reasonable domestic use”;
- Is suspicious because there is “no explanation”; and
- Other.

It also prompts the officer to decide whether this requires an “in-depth investigation” by the police, and, if so, why.

Mobile Phones, ID Cards, and Vehicles that Have Gone “Off-Grid”

The IJOP center also sends officials to investigate cases when an individual’s phone, ID card, or vehicle has gone “off-grid.” Screen 15 displays the prompt sent to officials requesting them to investigate a phone number that the system has lost track of. The officer is prompted to probe, using a drop-down menu, why the phone went off-grid. The officer

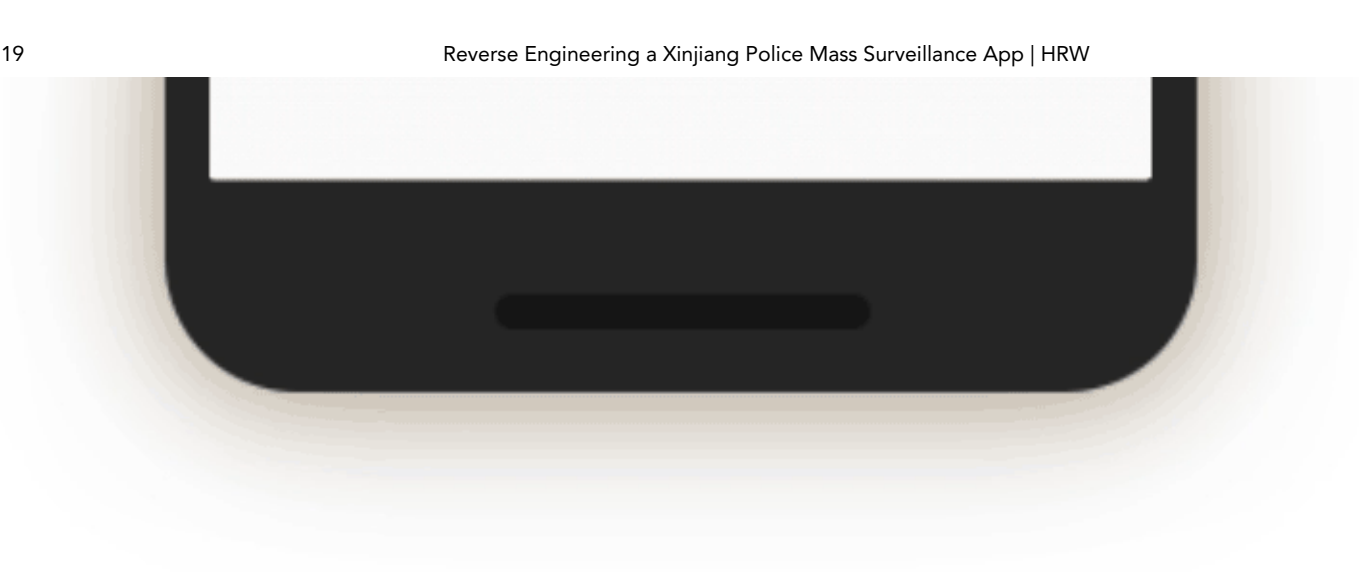
is then asked to note whether the person questioned seems suspicious and whether the case needs further investigation.

April 23, 2019 | Video

Screen 15

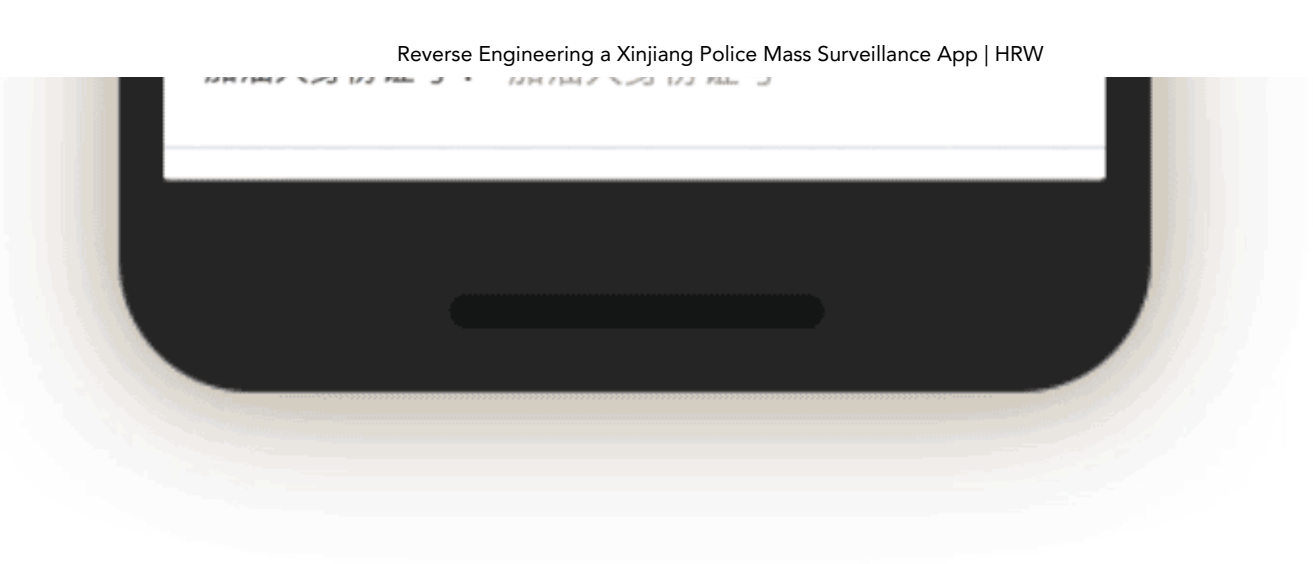
Screen 15


76% 16:05
详情
事件详情
车主姓名
车牌号码
身份证号
手机号码
户籍地址
轨迹消失日期



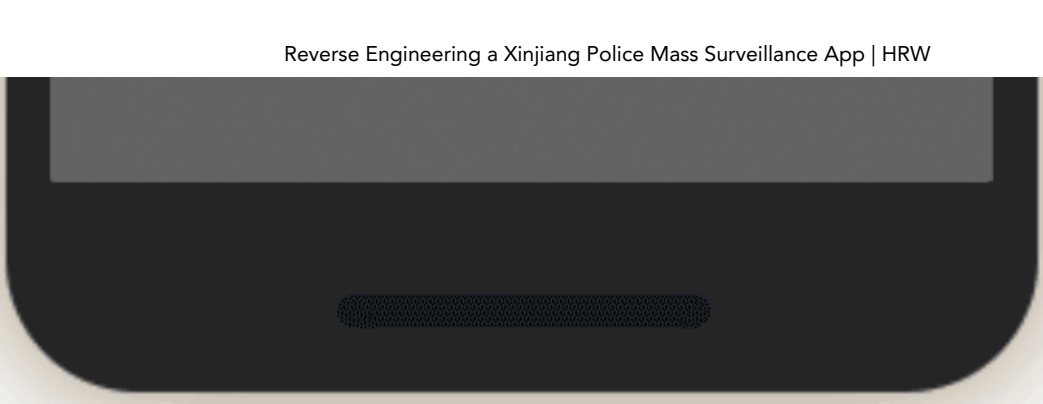
Screen 16


76% 16:05
人车不符
车牌号：
车牌号
车主姓名：
车主姓名
车主身份证号：
车主身份证号
车主手机号：
车主手机号
车主地址：
车主地址
加油人姓名：
加油人姓名
加油人性别：
加油人性别
加油人民族：
加油人民族
加油人身份证号：
加油人身份证号



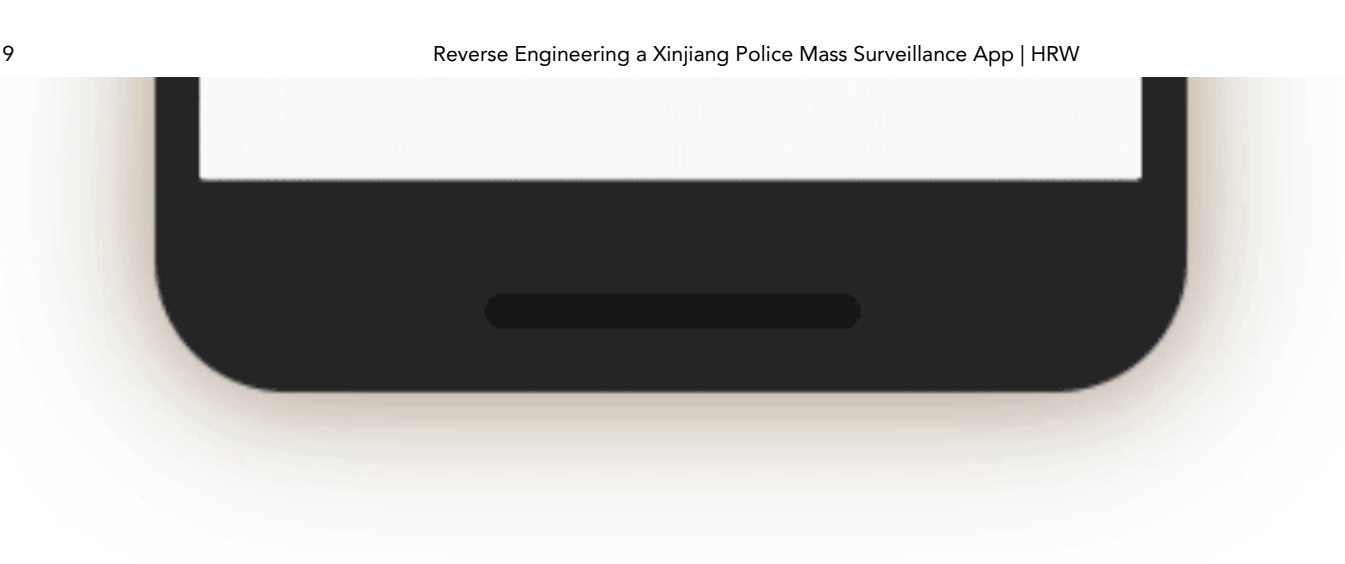
Screen 17


77% 16:09
人证不符
事件描述：
事件描述
姓名：
姓名
身份证号：
身份证号
手机号：
手机号
正在加载.....
轨迹信息：
轨迹信息



Screen 18


77% 16:10
人机不符详情
事件详情
开户人姓名
身份证号
手机号码
户籍地址
业务日期



Screen 19

Similarly, the IJOP center sends officers alerts about vehicles that have gone "off-grid," telling the officer the location in which the vehicle was last noted in the computer system (see screen 16).

We were unable to generate the screenshot for the corresponding feedback form, but an examination of the source code suggests that officers are prompted to investigate the case and provide feedback in a similar manner. Here the drop-down menu of reasons includes:

- Not selected;
- The vehicle has gone out of Xinjiang;
- The vehicle has been left unused;
- The vehicle is being repaired;
- The vehicle can no longer be used;
- The vehicle has been lent to someone else;
- The vehicle has been sold but the car registration has not been transferred;
- The vehicle has been sold but the car registration has been transferred;
- and Other.

In a similar manner, the IJOP system alerts officers when ID cards have gone "off-grid." Here is a list of options for officials to choose from in investigating the reasons:

- Gone to seek work elsewhere;
- Gone to school;

- Gone on a tour;
- In hospital;
- Moved hukou;
- Left the country;
- Left Xinjiang;
- Subjected to criminal detention;
- Subjected to political education;
- Whereabouts unclear;
- and Other.

Mismatched Identities

The IJOP system alerts officials to instances when people are using cars, phones, or ID cards that are not registered to them.

Screen 17 suggests the IJOP system alerts officers to cases in which there is a "mismatch between the person and the vehicle (人车不符)." The system spots such mismatches by monitoring whether the registered owner of the car is the same as the person who gets gasoline for the car at gas stations. The screenshot below also shows that the IJOP monitors the time and frequency of gas station visits.

Since July 1, 2016, Xinjiang authorities have implemented a "real name" registration system for gas stations, in which gas station entrances are equipped with systems that recognize vehicles' number plates and collect the identity of drivers, and require the drivers to swipe their ID cards before they can get gas.[77] The app suggests the IJOP system receives information from this "real name" registration system.

The corresponding feedback form requires officials to investigate. While we were unable to generate a screenshot of the form, the source code suggests officials are required to investigate mismatches, choosing the reasons from a drop-down menu, and deciding whether the incident is suspicious and requires further investigation.[78]

Similarly, the IJOP app sends officials alerts about people who are not using ID cards registered to them, presumably when going through checkpoints dotted throughout the region, or in other circumstances where IDs are required. Although the screenshot did not generate properly, the form asks for a description of the issue, followed by personal particulars such as ID card number, as well as the person's "trajectory information" (see screen 18). The IJOP app then prompts officials to find out the reasons for the mismatch.[79]

The IJOP system also alerts officials when people are using phones that do not belong to them, giving the officials information about the case and the personal particulars of the person who is registered to the phone account, such as their ID number (see screen 19). It is unclear how the system "knows" that a person is using a phone that does not belong to them.[80] Officials are again required to log the reasons for the mismatch and decide if the person is suspicious.[81]

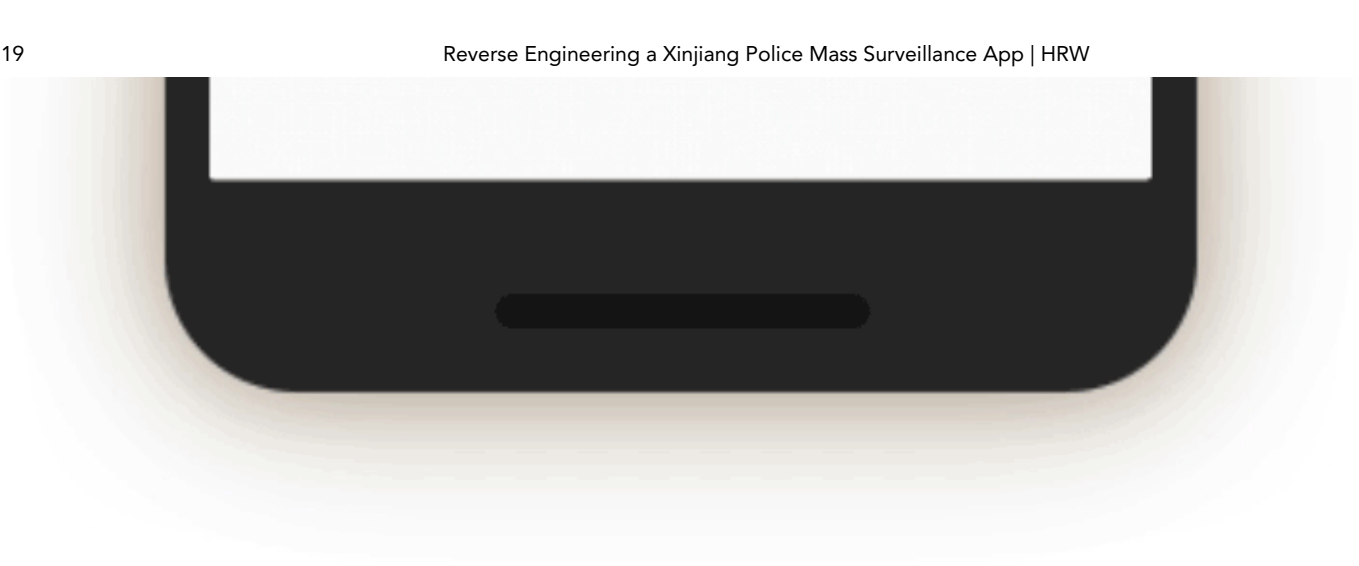
The data fields included in the IJOP system may help explain some of the bizarre interactions former Xinjiang residents described to Human Rights Watch, in which Xinjiang officials demanded specific and detailed personal information about them or their family members living abroad. Aylin, a woman in her early 20s, said:

> The official called my mom and asked her how many years she has had this phone number.... She said, "11," and the police said, "You're lying, it's 7!" She got frightened and then accidentally cut off the phone call.[82]

Aylin said her mother then went to get a new SIM card using her son's ID card. Two days later, the authorities detained the mother and son for purchasing and using this SIM card to call Aylin.

"Problematic" Individuals


77% 16:11
人员调查详情
问题类型
事件详情
姓名
身份证号
户籍地址
护照号码
手机号码



Screen 20

The app suggests officers are prompted to investigate certain individuals deemed “problematic.” Screen 20 shows such an alert detailing the “problem,” along with personal particulars of the individual.

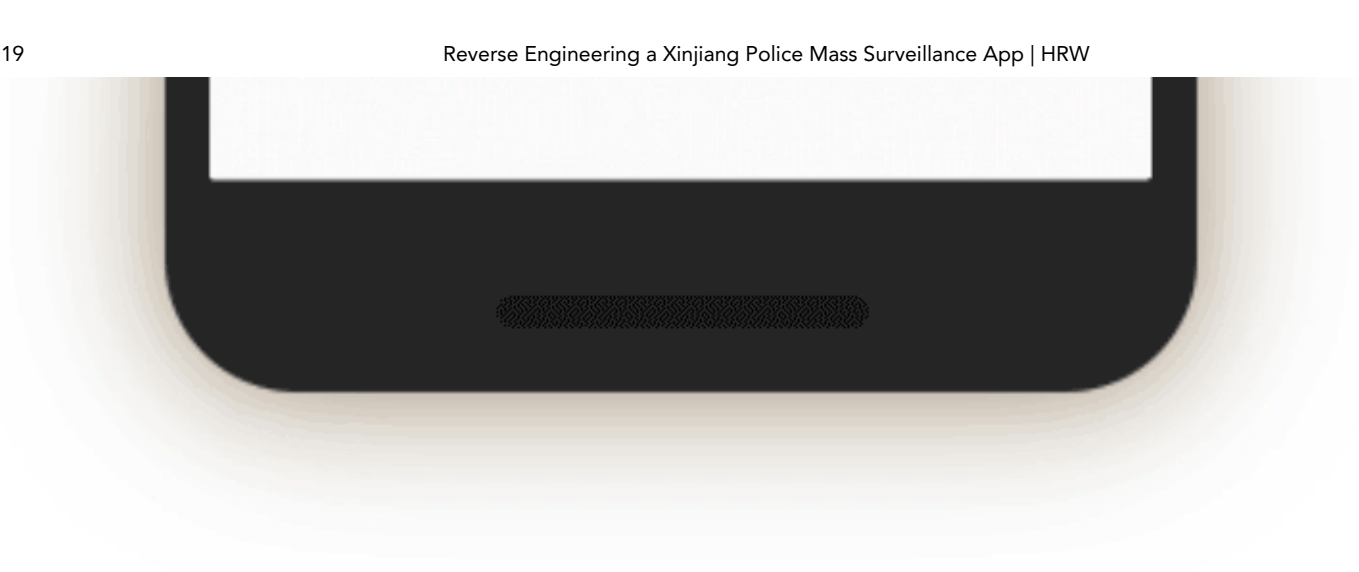
An examination of the source code suggests that the following categories of people are considered “problematic”:

- People related to those whose whereabouts are unclear;
- People related to internal migrants;
- People related to those who are monitored by the IJOP;
- People related to those who cannot be contacted;
- People related to those who use the identification documents of dead people;
- People related to those whose phone number and identity is mismatched;
- People related to those who have left the country three days ago;
- People related to those who have not returned after leaving the country 30 or more days ago;
- People related to those who have not returned after leaving the country [for over a] half year;
- People related to those who have not returned after leaving the country [for over] one year;
- People related to those [newly] held in detention centers for endangering security;
- People related to those who have started a new phone number account;
- and Others.

Officials are then prompted to investigate these people and fill in a feedback form, which asks the officer to obtain a wide range of personal data about the individual, such as their means of transport, internet tools, bank information, and family members (the form is nearly identical to screen 3).

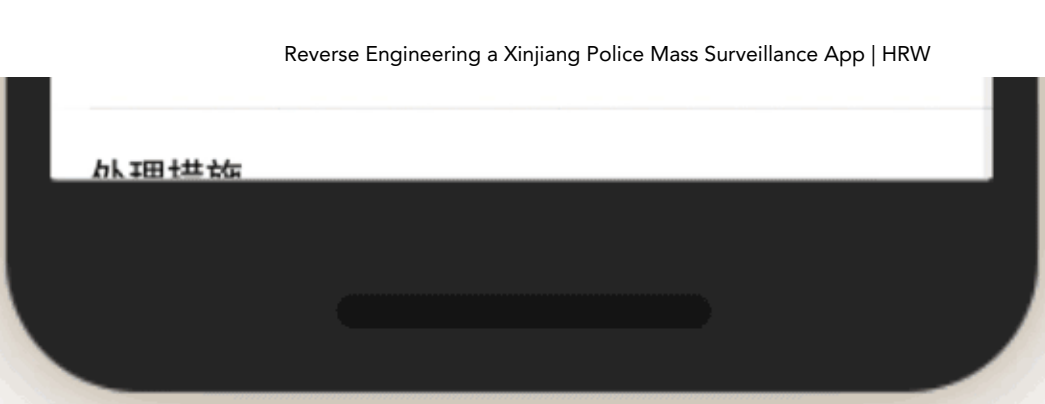
For each category of personal information, officials are prompted to add details such as the person's means of transport. Officials can then log the license plate number of their vehicle, if any, the vehicle color and the vehicle type by opening a related screen. Similarly, there are pages for officials to input information about the person's social media account tools and number, bank account information, and information about their family members.


76% 16:05
车辆报备
姓名
身份证号
手机号码
车牌号码
地址
推送时间
事件描述
备注

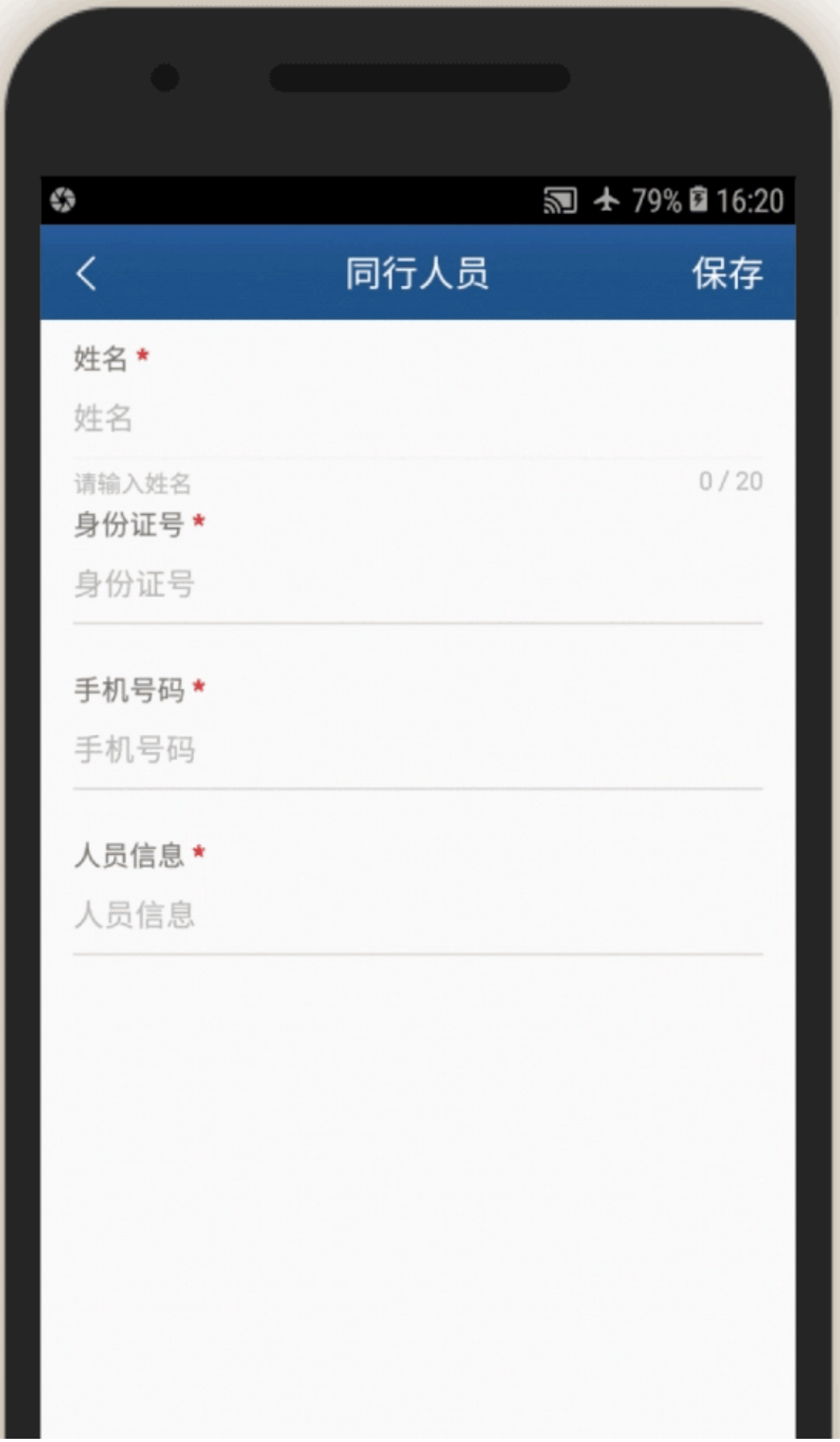


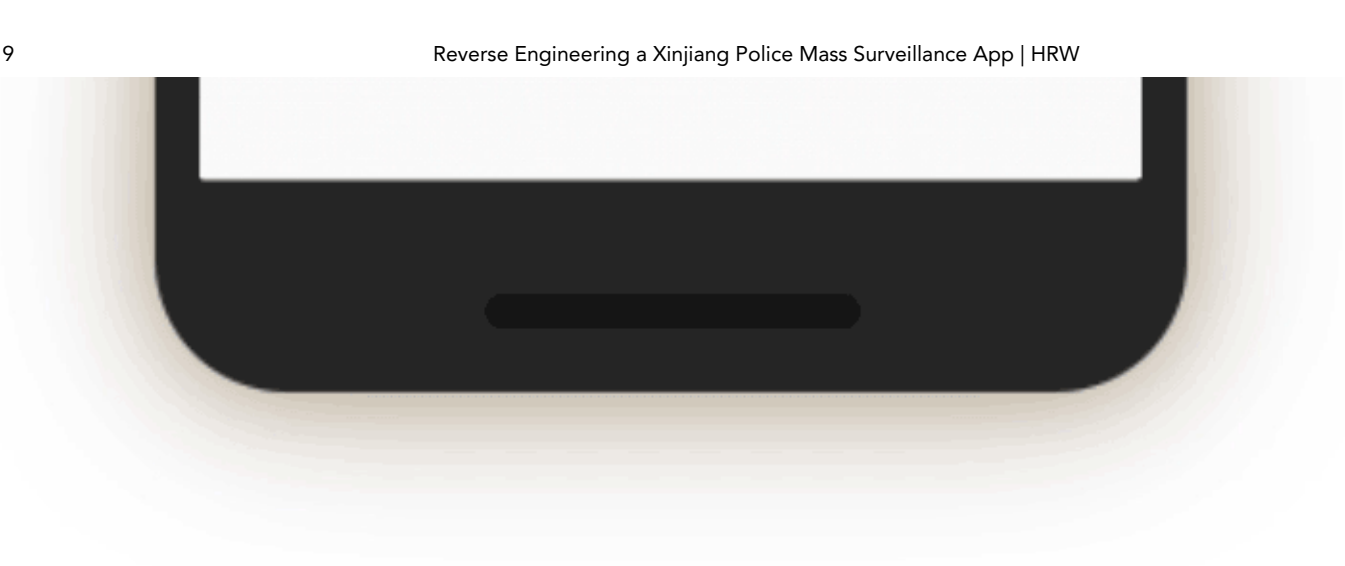
Screen 21


76% 16:05
比中人员详情
基本信息
类型
姓名
身份证号
身份证照片
相似度
采集照片
采集设备位置
数据门设备码
数据门位置ID
采集时间
身份证标签



Screen 22


79% 16:20
同行人员
保存
姓名 *
姓名
请输入姓名
0 / 20
身份证号 *
身份证号
手机号码 *
手机号码
人员信息 *
人员信息



Screen 23

Officers are also prompted to gather more information about specific "problems" concerning the individual or their relations. The app gives officers "hints," depending on the "problem" type, suggesting they ask the person about:

- The whereabouts of the person who has gone missing;
- Why they had come to this county;
- Why their relative travels and stays with "nine types of monitored individuals";
- Why their relative's phone number cannot be contacted;
- Why their relative uses the identification documents of dead people;
- Who is using the mobile phone number registered with their identity;
- Why their relative left China, whether have they been in contact with the relative, and when [the relative] crossed the border;
- Recent activities that involve their relative and people who endanger security, and why their relation travels and lives with detained individuals;
- and Why their relative has obtained a new phone number account.

Finally, the officers are required to report back to the IJOP center whether these individuals require further police investigation.

"Problematic" Vehicles

Officials are also alerted to certain vehicles and prompted to investigate (see screen 21).

An examination of the feedback form's source code shows it prompts officers to investigate the relationship between the driver and the owner of the vehicle, and logs the owner's particulars (e.g., name, phone, ID card number), presumably because the system detected a mismatch between the two identities or detected that the information was missing.

"Matched" Persons

The IJOP system sends alerts sent to officers, that contain information concerning when an individual passed through a checkpoint location and their ID, suggesting that the IJOP system picks out people as they go through Xinjiang's checkpoints (see screen 22). People are "picked out" or "matched" by the system through their ID cards, mobile phone MAC addresses, IMEI number, or facial recognition. This finding suggests some of Xinjiang's checkpoints are not merely recognizing people through their ID cards or facial recognition—identification procedures that people know they are undergoing at these checkpoints.

Instead, the equipment at some of the checkpoints—called "three-dimensional portrait and integrated data doors" (三维人像综合数据门)—are vacuuming up people's identifying information from their electronic devices.[83] Unbeknownst to the person going through the checkpoints, these "data doors" are detecting and collecting MAC addresses and IMEI numbers of the person's phones, and logging such data for identification and tracking purposes.

In addition, the screenshot below suggests that officers are told to take certain actions regarding these "matched" individuals (处理措施). The source code suggests three forms of action: subject them to information collection (信息采集), keep them for interrogation (滞留审查), or arrest them immediately (立即抓捕).

For "matched" individuals, officers are prompted to find out and log, among other things:

- Whether the person's phone has "suspicious" content;
- Whether the person had "applied to go on leave" from their hukou region;
- Whether they have left their hukou area in the past year;
- What reasons the person has for leaving (the options in the drop-down menu are: "doing business," "going to school," "no reasonable explanation," or "other").

The official is also required to log the personal particulars of people found together with the "matched" persons (see screen 23).

Ehmet, a Turkic Muslim released from a political education camp in Xinjiang in 2017, found his movements were still being restricted after his release. He told Human Rights Watch:

> When I tried going out of the region, my ID would [make a sound] at police checkpoints.... The police told me I could not go out of [the hukou] region, because I was blacklisted. So, I went to the police in my village, and said, “I have kids and I need authorization to go....” But the police wouldn't give the authorization, so I couldn't leave the region. I got very angry and said, "You either kill me, or you put me in prison, or I’ll kill myself."[84]

Eventually, Ehmet was allowed to leave the region. A number of people who left Xinjiang in recent years told Human Rights Watch of similar experiences: that they or their family members had experienced similar movement restrictions.

Alim said he was released after spending several weeks in a police detention center for “disturbing social order”:

> Everywhere in Xinjiang there were checkpoints. For the first week [after I was released], I was able to go everywhere. But then, I was entering a mall, and an orange alarm went off... the police already arrived, and they escorted me to the police station. I said to them, “I was in detention center and you guys released me because I was innocent....” The police [at the police station] told me, “Just don’t go to any public places.” I said, “It was fine for the first week and I was able to go places.” The police said, “They update the list every day.” I said, “What do I do now? Just stay home?” He said, “Yes, that’s better than this, right?”[85]

In many of the cases described to Human Rights Watch, the authorities made decisions about restricting people’s movement without any notification or avenues for redress. Alim recalled another incident:

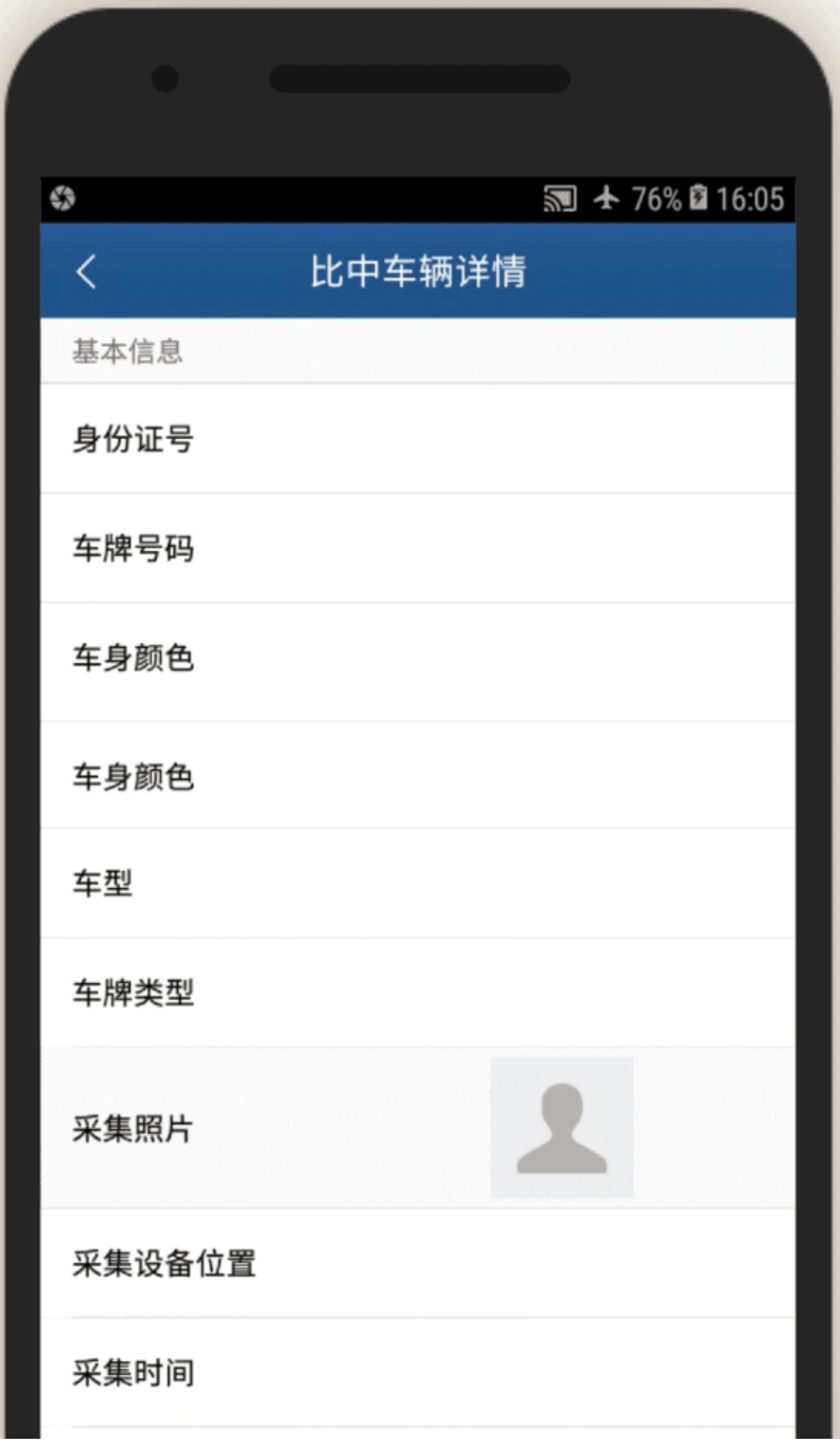
> We went to this waterpark right next to a lake, in a county that belongs to the city where I live. We went there, and on the way back, we had to go through a checkpoint...the orange alarm went off...they questioned me. I asked them, “What happened?” They said, “You’re supposed to get permission if you go out of [the city].” I said, “I didn’t know.”

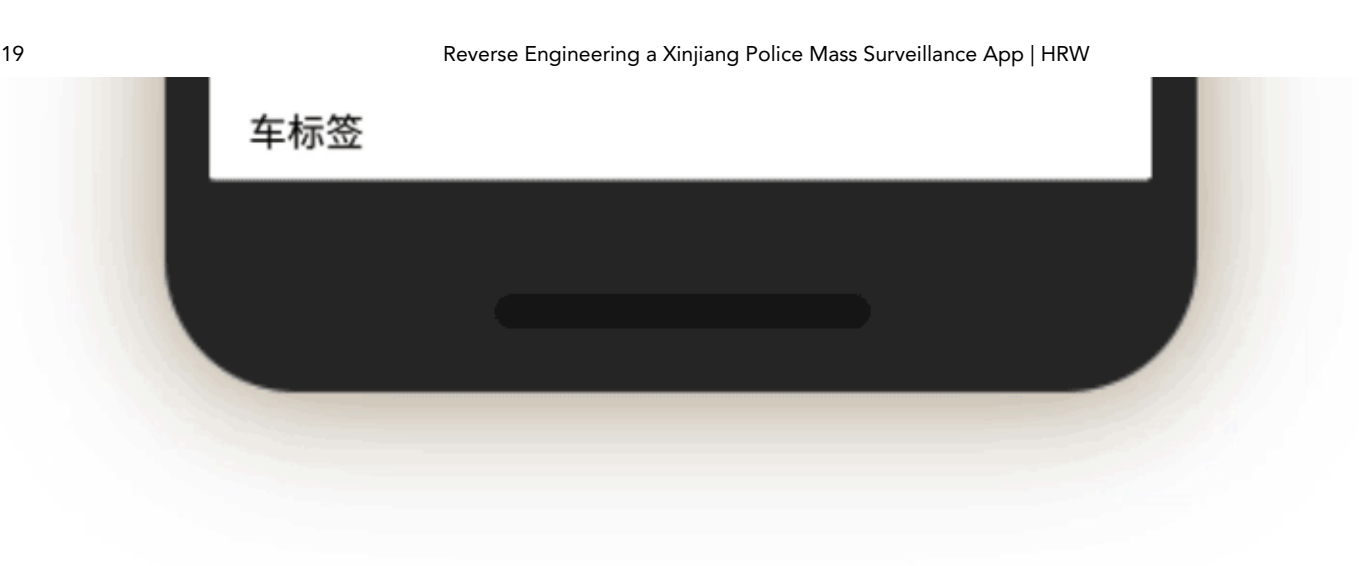
Alim then spent the next weeks at home and did not go anywhere: “My friend and I would go to the internet cafes to play video games, but I didn’t want to go, to go to the police station again.”[86]

People also told Human Rights Watch their movement had been restricted simply for being connected to those the IJOP system considers problematic. According to Nur:

> When my family and I were entering Urumqi after I was released.... the machines went “du du du” when our IDs were swiped. They called me into the office and asked us what crimes we had committed and why we were flagged, and they called our police station; our police explained that I and my family were blacklisted because I was a [foreign] national and because I was detained. [My family] said their ID cards have been making noise when going through the checkpoints ever since I was taken away.[87]

“Matched” Vehicles


76% 16:05
比中车辆详情
基本信息
身份证号
车牌号码
车身颜色
车身颜色
车型
车牌类型
采集照片
采集设备位置
采集时间



Screen 24

The IJOP system sends officials an alert about certain vehicles, flagging two types: second-hand vehicles and vehicles that belong to people on a "watch list" (布控对象车辆预警). The source code does not give a precise definition of the latter and we are not aware of any Chinese law or policy defining the term or detailing a process by which a person's vehicle is put on a police watch list or how to appeal such a designation.

Screen 24 shows the alert page, which gives details about the vehicle's license plate as well as the car's physical characteristics. It also gives the location and time that the "data collection devices" captured the information—likely to include the region's vehicle checkpoints—and the action required.

A corresponding feedback form, which we were unable to generate but which was indicated in the source code, says officials are required to log the driver's ID and phone numbers, and note whether the driver is the same person as the registrant of the car. If not, the official is prompted to investigate the reasons for the difference and log them using a drop-down menu:

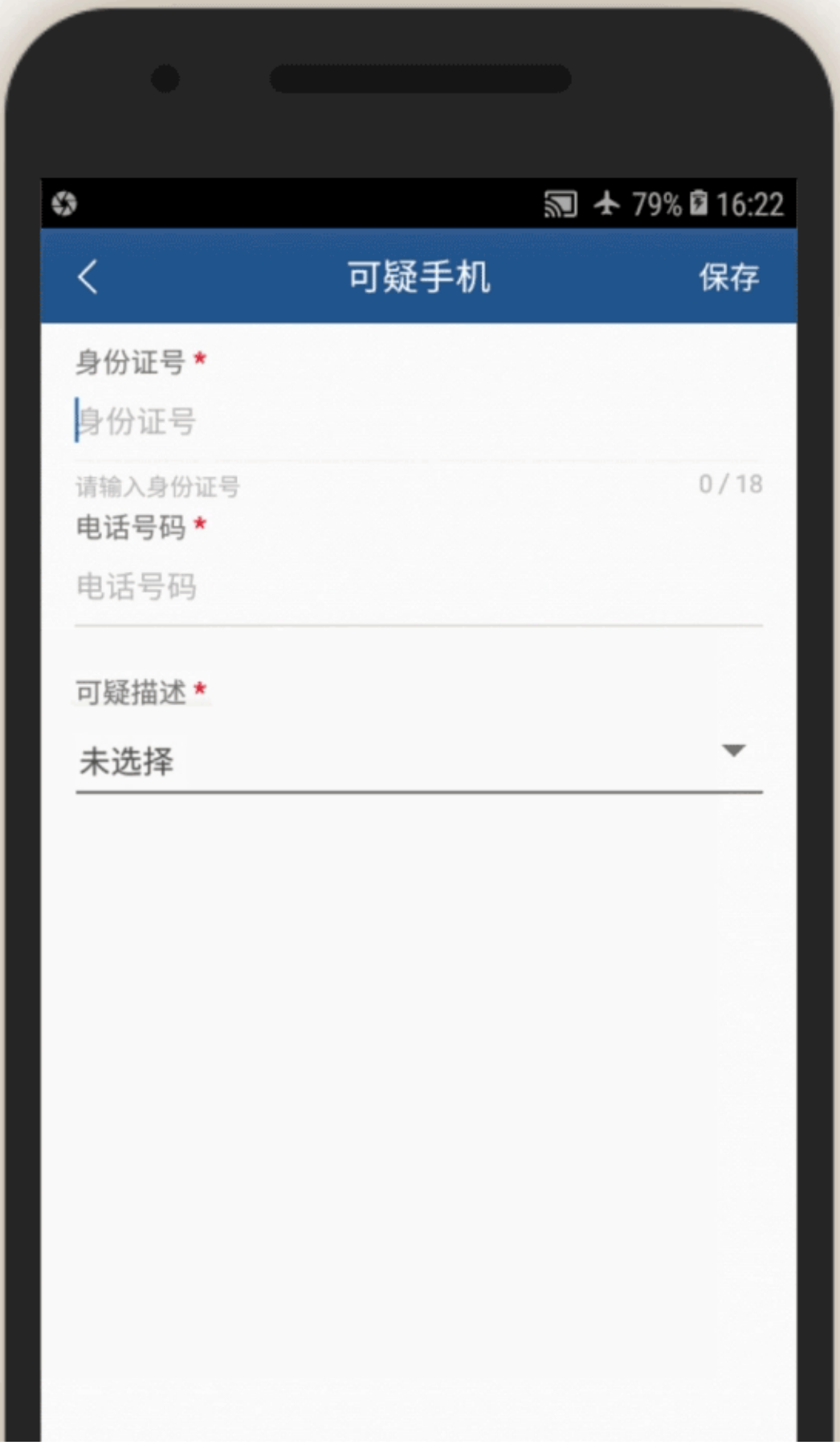
- Not selected;
- Borrowing the vehicle from friends and family;
- Vehicle used for business;
- The vehicle has not finished the process of transferring ownership;
- and Other.

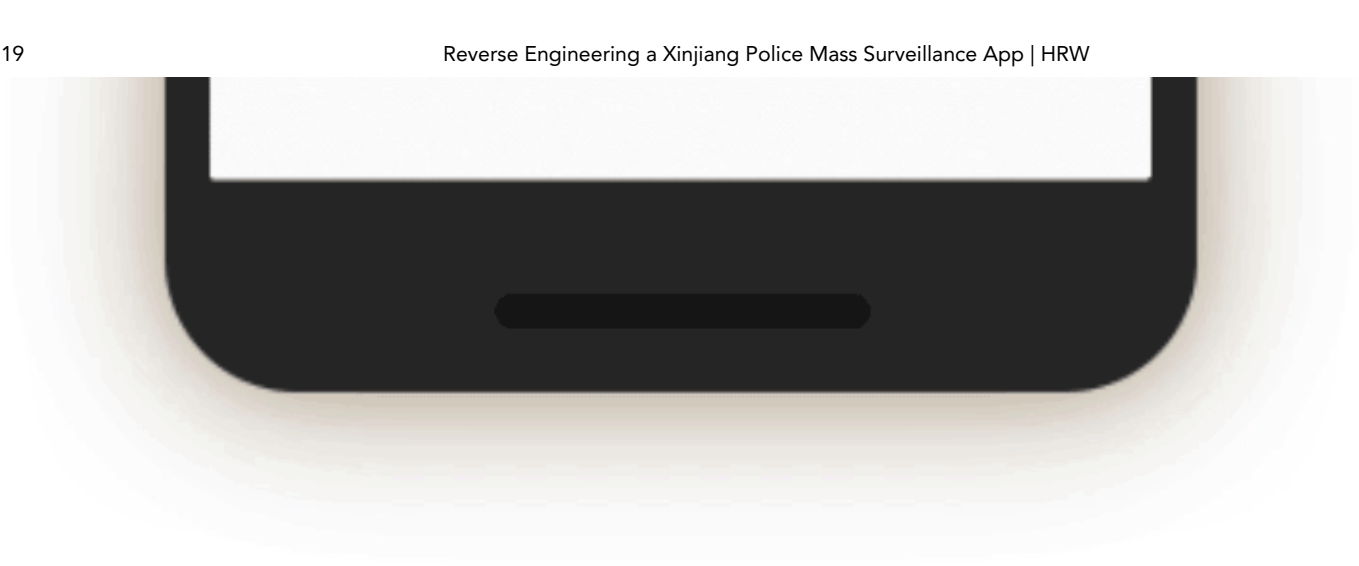
The form also asks officials to search the vehicle for contraband or forbidden items.[88] It then asks officials to determine whether the vehicle needs another round of checks and, if not, to select from a drop-down menu the reason further checks are not needed:

- Not selected;

- Borrowing the vehicle from a family member;
- Borrowing the vehicle from an acquaintance;
- Is in the process of transferring the ownership of the vehicle;
- Rental car;
- Vehicle belongs to employer [or business];
- and Other.

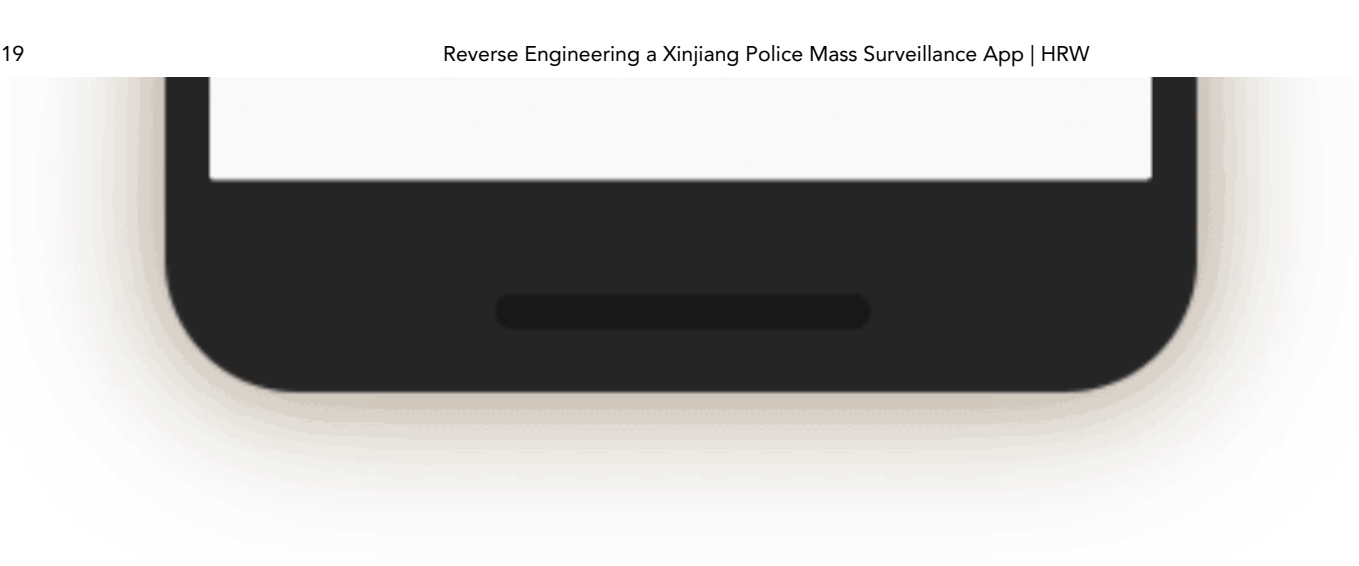
The form also prompts officials to see if the phones—presumably of the driver, but perhaps also of all the passengers—contain "suspicious" software (see screen 25). The person's ID and phone number are logged, along with a drop-down menu that allows officials to log whether the suspicious phone content concerns VPN, unusual software, suspicious websites, or others. The system also prompts the officer to log the identity and phone and ID numbers of the person travelling in the "matched" vehicle see screen 26).


79% 16:22
可疑手机
保存
身份证号 *
身份证号
请输入身份证号
0 / 18
电话号码 *
电话号码
可疑描述 *
未选择



Screen 25


80% 16:24
乘客信息
保存
身份证号 *
身份证号
请输入身份证号
0 / 18
电话号码 *
电话号码
人证核验结果 * 一致
不一致



Screen 26

IV. Applicable Legal Standards

International and Domestic Law

The International Covenant on Civil and Political Rights, which China signed in 1998 but has not ratified, provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, and that everyone has the right to the protection of the law against such interference.[89] Any interference with the right to privacy, including the collection, retention, and use of an individual's personal data, must be necessary and proportionate for a legitimate aim, and subject to a clear and public legal framework. Such a framework must ensure that the collection, retention, and use of personal data is:

> a) necessary to the achievement of a legitimate aim such as public safety, and in the sense that less intrusive measures are unavailable;
>
> b) appropriately restricted to ensure the action is proportionate to the legitimate aim; and
>
> c) subject to authorization and oversight by an independent body, as well as other safeguards that are sufficient to prevent and address abuses.[90]

The right to privacy is also a gateway to the enjoyment of other rights, particularly the right to freedom of opinion and expression.[91]

Current Chinese laws do not meet these international privacy standards and do not provide meaningful protections against unlawful or abusive government surveillance. Article 40 of the Chinese Constitution guarantees people's "privacy of correspondence,"[92] but China does not have a unified privacy or data protection law.[93] Although the government shows growing interest to regulate private companies' collection of consumer data, such regulations are limited to the commercial sphere.[94]

There are Chinese laws, regulations, directives, and rules that empower various government entities to collect and use miscellaneous personal data, and some give authorities wide powers in data collection. For example, state security-related legislation, such as the State Security Law, invests police and other state security agents with the broad power "to collect intelligence involving state security." Such laws that grant unfettered discretion to the bodies ordering or carrying out surveillance violate international privacy rights norms that require that surveillance, even if it is for a legitimate aim, must be proportionate and necessary.[95]

But even given these powers, the Chinese authorities' collection and use of personal data—particularly with respect to mass surveillance—have little legal basis.[96] In Xinjiang, the regional Implementation Methods of the Counter-Terrorism Law requires that delivery, telecommunications, internet, finance, hostel, long-distance bus, and rental car companies implement the real-name registration system.[97] But apart from this requirement, many mass surveillance practices described in this report do not appear to be authorized by Chinese law and on their face appear to violate it.

For example, Chinese law does not generally empower government employees to search the phones or collect the DNA samples of members of the public. Only crime investigators, such as the police can do so during the investigation of a specific criminal case.[98] Even if people are being investigated for a crime, the police must present "a search warrant…to the person to be searched."[99] There is no sign, based on interviews with former Xinjiang residents that Human Rights Watch conducted in 2018, that Xinjiang government officials or the police produce any search warrant prior to demanding to look through people's phones.[100]

In addition, many of the behaviors and relationships that set off red flags with the IJOP system are not crimes according to Chinese law. For example, no Chinese law or regulations define an "overdue" person, specify the length of time people are allowed to stay abroad, or prohibit extended stays. Chinese law also does not make it a criminal offense for individuals to use WhatsApp, Telegram, or any of the foreign communication tools or VPNs.[101] The broad "watch lists" or the flagging of people by the IJOP system described in this report have no legal basis: Chinese law only empowers the police to track people if they are suspected of crimes in specific criminal investigations.[102]

There is very little information available about how, and how securely, the data collected by IJOP system is stored, who can receive or share the data, and under what circumstances, if ever, the data is deleted.[103] There is no formal system for people to find out what information is held about them in the IJOP system, and no way to obtain redress for abuses associated with the collection, dissemination, and use of their data.

Businesses and Human Rights

While the Chinese government has the primary obligation to respect, protect, and fulfill human rights under international human rights law, businesses—including Chinese and international companies operating in Xinjiang—also have human rights responsibilities.[104] The "Protect, Respect, and Remedy" framework, articulated most notably in the United Nations Guiding Principles on Business and Human Rights, reflect the expectation that businesses should respect human rights, avoid complicity in abuses, and adequately remedy them when they occur. The Guiding Principles urge businesses to exercise due diligence to identify, prevent, mitigate, and account for the impact of their activities on human rights.[105]

Recommendations

To the Government of the People's Republic of China:

- Shut down the Integrated Joint Operations Platform (IJOP) in Xinjiang and delete all data it has collected;
- Suspend the collection and use of biometrics in Xinjiang until there is a comprehensive national law that protects people's privacy;
- Cease immediately the "Strike Hard Campaign against Violent Terrorism" (Strike Hard Campaign) in Xinjiang, including all compulsory programs aimed at surveilling and controlling Turkic Muslims;
- Impartially investigate Party Secretary Chen Quanguo and other senior officials implicated in alleged abusive mass surveillance practices associated with the Strike Hard Campaign, and appropriately hold those responsible to account; and

- Grant access to Xinjiang, as requested by the UN high commissioner for human rights and several UN special procedures.

To the National People's Congress Standing Committee:

- Draft and adopt legislation relevant to biometric and personal data to ensure its collection is compliant with international human rights standards:
    - The standards set forth in such legislation should be part of a larger legal framework ensuring that any collection, use, access, dissemination, and retention of such data is necessary; that less intrusive measures are not available; and that collection and use of such data are narrowly tailored and proportionate to a legitimate purpose, such as public safety.

    - To ensure these standards are enforced, any biometric data program should include: independent authorization for collection and use of the data, public notification that authorities are collecting the data, means of independent oversight of the program, and avenues for people to challenge abuses and obtain remedies.

    - The standing committee should also ensure relevant authorities publish information about the collection and use of biometric-based recognition technology, including about databases that have been created and how they are being used.

To Concerned Governments:

- Impose targeted sanctions, such as the US Global Magnitsky Act and other protocols, including visa-ban and freezing assets, against Party Secretary Chen Quanguo and other senior officials linked to abuses in the Strike Hard Campaign;

- Impose appropriate export control mechanisms to deny the Chinese government—and Chinese companies enabling government abuses—access to technologies used to violate basic rights, including by adding CETC and others named in this report to existing export control lists;

- Ensure that state-run institutions, including universities, do not engage with the Xinjiang police and Chinese technology companies that are linked to human rights abuses against Turkic Muslims in Xinjiang; and

- Push for an international fact-finding mission to assess the situation in Xinjiang and report to the UN Human Rights Council.

To the United Nations:

- UN Secretary-General Antonio Guterres and other senior UN officials should raise concerns publicly and privately with the Chinese government about human rights violations arising from the Strike Hard Campaign;

- Senior UN officials should act to ensure civil society activists can safely report on Chinese government abuses in Xinjiang and elsewhere to UN human rights mechanisms; and

- Senior UN officials should support Chinese civil society groups by resisting attempts by the Chinese government at the UN Department of Economic and Social Affairs (DESA) to block accreditation of groups advocating for the rights of Turkic Muslims in Xinjiang.

To Chinese and International Companies Operating in Xinjiang, including CETC, HBFEC, Baidu, Face++, and Hikvision:

- Ensure business operations are not supporting the Strike Hard Campaign, in particular, the mass surveillance and biometric profiling systems run by the Xinjiang Bureau of Public Security;

- Ensure business arrangements with the Xinjiang police or other security forces do not contribute to abuses and promptly act to end such relationships when there is evidence that they do;

- Adopt explicit policies in support of human rights and establish procedures to ensure company operations do not result in, or contribute to, human rights abuses; and

- Analyze the human rights impacts of proposed investments or operations and implement strategies to prevent and mitigate adverse impacts. Such "human rights impact assessments" should be conducted in coordination with civil society groups and human rights experts.

Acknowledgments

This report was researched and written by Maya Wang, senior China researcher in the Asia Division at Human Rights Watch. The reverse engineering process was guided by information security director Seamus Tuohy. The report was edited by Sophie Richardson, China director. Dinah PoKempner, general counsel, and James Ross, legal and policy director, provided legal review. Joseph Saunders, deputy program director, provided program review. An associate in the Asia Division provided editing and production assistance. The report was prepared for publication by Fitzroy Hepkins, administrative manager.

We are grateful to Cure53 for their work in reverse engineering the IJOP app.

We are particularly indebted to Greg Walton, an independent expert on cyber security and mass surveillance in China, who volunteered countless hours throughout this report's research process, providing technical advice and invaluable insights. He also commented on an early version of the report.

We are grateful to another external reviewer who also commented on an early version of the report but who does not wish to be named.

We thank all the people from Xinjiang who shared their stories with us as part of the research for our September 2018 report.

Region / Country Asia, China and Tibet