Turquoise Roof Bulletin No. 3

February 2024

Weaponising Big Data:

Decoding China's digital surveillance in Tibet

TIBET WATCH
བོད་གནས་ལྟ་ཞིབ་

TURQUOISE
ROOF

Table of contents

Cover page background image by

Chungpo Tsering, Selfie, 2014. © The Shelley and Donald Rubin Private Collection.

Dedication

Chungpo Tsering
(1979-2024)

If Tibetans were controlled by arms and ammunitions of China in the last century, today, they are also controlled through the phones in their pockets and cameras outside homes, with their reality, unbeknownst to them, being calculated for more oppression in the CCP's Oracle [database]. In memory of the artist Chungpo Tsering (1979-2024) who grew up as an orphan but chose to remember this life by choosing his birthday as 10 March, the Tibetan National Uprising Day. May you be reborn in a free Tibet. TC

In an obituary, Tenzin Dorjee wrote: "Chungpo gave so much to this world, to his people, to his community of exiled artists and activists, and to his ever expanding circle of friends and students and loved ones. A talented artist, a lifelong activist, a brilliant storyteller, a powerful dreamer, he was a creative genius who transformed everything he touched into a work of art."

Chungpo Tsering spent his final days in the Czech Republic, where he was director of Tibet Open House in Prague, cradle of the Velvet Revolution and the home of Vaclav Havel, the playwright-turned-president who was one of the closest friends of His Holiness the Dalai Lama. In his memory, Tibet Open House is hosting an exhibition of his art. KS

Executive Summary

This report uncovers the Chinese government's escalated digital surveillance in Tibet, marked by the compulsory installation of the 'National Anti-Fraud Centre' app on smartphones. Initially presented as a fraud prevention tool, the app is in fact a crucial element of a larger surveillance network. This report, developed in collaboration with Tibet Watch, London, is based on accounts from a Tibetan refugee in Golog in eastern Tibet[1] (present day Qinghai province).

Our investigation conducted a dynamic analysis of the Android and Windows Desktop versions of this app, finding that data collected could extend beyond internet fraud detection, feeding into broader control mechanisms. This includes integration with databases managed by the Criminal Investigation Bureau, reflecting wider strategies of surveillance and oversight in the region.

The report also investigates the 'Tibet Underworld Criminal Integrated Intelligence Application Platform', a sophisticated big data policing platform. Analysis of government procurement notices revealed that this system amalgamates data from various existing Public Security Bureau systems in the Tibetan Autonomous Region (TAR) into a central Oracle database. This database system, developed on top of U.S. technology, is instrumental in a campaign that criminalises even moderate cultural, religious expressions, language rights advocacy, and social work in Tibet.

This investigation into the weaponisation of big data analytics in Tibet by the Chinese security state sheds new light on the reach of Party mechanisms into the personal sphere. This is not only changing the way people communicate, but having a society-wide 'chilling effect' on the way they think, feel and relate to each other, in many cases leading to a complete breakdown of contact.

The integration of a panoply of advanced technologies in Tibet - AI-driven systems fusing facial recognition with internet browsing and app-based monitoring, to DNA and genomic surveillance, and GIS tracking data - underlines the emergence of a terrifying approach to governance in the 21st century. It uses machine learning to power systems that prioritise state control and suppression over individual liberties and self-determination.

There are clear parallels in the deployment of spyware and Universal Forensic Extraction Devices (UFEDs) at police checkpoints in both Tibet and Xinjiang. Similarly, sophisticated big data analytics platforms are in operation in both regions, and although specific systems might differ, the same overarching strategy of control and suppression through intelligence-led policing is evident in both regions. Civilian AI-driven surveillance systems deployed in Tibet and Xinjiang find their origins in military Command and Control (C4ISR) systems-of-systems, and integrated PLA joint operations doctrine. Chinese software developers have acknowledged this evolution in which cities and towns where people live are treated like a battlefield.[2]

Key Takeaways

1. The weaponisation of big data policing analytics in Tibet by the Chinese security state extends the reach of Party mechanisms into the personal sphere. This surveillance is not only changing the way people communicate, but is having a society-wide ‘chilling effect’ on the way they think, feel and relate to each other, in many cases leading to a complete breakdown of digital contact.

2. Digital forensic analysis of an app that Tibetans are being forced to install at police checkpoints shows that the app has access to sensitive data and control over key device functionalities. This is being used for invasive surveillance, enabling the monitoring of personal information and activities, thus compromising user privacy and security. The broad scope of the app’s privacy-invasive permissions aligns with the extensive surveillance practices in the region, potentially aiding in the government’s efforts to control and monitor the populace.

3. This bulletin examines a new AI-driven big data policing platform in China. This platform is instrumental in implementing a policy that categorizes peaceful dissent and civil society activities, including support for the Dalai Lama’s autonomy proposal for Tibet, as ‘transnational organized crime’. It achieves this by integrating various existing police databases. This policy not only breaches international standards for cultural preservation and self-determination but also impedes effective global measures against real transnational organized crime.

Introduction

> *"If someone exists, there will be traces, and if there are connections, there will be information"*

Onscreen message in a demonstration of a surveillance system by China Electronics Technology Corporation, a state-run defence manufacturer[3]

A Tibet Watch report of 6 September, 2023 published for the first time testimony[4] of a Tibetan from Golog (མགོ་ལོག)[5] in eastern Tibet. The Tibetan, who is now in exile, described how on his way home from school, police at a checkpoint forced him to install an app on his smartphone that enables access to all private data and can track personal networks.

The Tibetan refugee said: "On our way home during school vacation, we have to go through numerous checkpoints. Our luggage and backpacks, other accessories, and even mobile phones are scanned and searched. [This time,] we were instructed to download and install a security application (国家反诈中心) which, if found deleted at the next checkpoint, we were forced to download and install again."

The account of the Tibetan refugee from Golog (Chinese: Guoluo) in Amdo (present-day Qinghai) is new evidence of forcible installations of a national Anti-Fraud Centre (Guó Jiā Fǎn Zhà Zhōng Xīn 国家反诈中心) app[6] in individuals' smartphones, demonstrating the increasingly intrusive digital reach of the Chinese Party state into Tibetan lives. While the app's purpose is described as combating 'fraud', in the Tibet context it is a significant element of a complex surveillance architecture focused on monitoring the movements, associations, and communications of Tibetans, especially those with contacts in the Tibetan exile and diaspora communities.

Working in partnership with London-based monitoring organisation Tibet Watch, for this bulletin Turquoise Roof performed a dynamic analysis of the 'National Anti-Fraud Centre' app (the Android and Windows Desktop versions), exploring how data collected by the app might connect beyond those of fraud investigation into wider systems that integrate a range of databases operated by the Criminal Investigation Bureau, aligning with broader strategies of control and oversight in the region.[7]

This bulletin also investigates another big data platform known as the 'Tibet Underworld Criminal Integrated Intelligence Application'. Involving analysis of government procurement notices, Turquoise Roof found that this tool integrates data from existing Public Security Bureau systems in the TAR into a centralised system powered by an Oracle database, a multi-model database management system produced by an American multinational information technology company headquartered in Austin, Texas. This is a tool enforcing a system in Tibet in which even moderate forms of cultural and religious expression, peaceful advocacy for language rights, or social groups working for the homeless or animal welfare in Tibet are criminalised by the Chinese state.

It is a strategy which frames peaceful advocacy, for instance, for language rights as a state security threat, which not only undermines the broader international principles of cultural preservation and self-determination, but also renders international law enforcement cooperation to combat genuine transnational organised crime more difficult.

This eye-opening investigation into the weaponisation of big data analytics in Tibet by the Chinese security state sheds new light on the reach of Party mechanisms into the personal sphere. This is not only changing the way people communicate, but having a society-wide 'chilling effect'[8] on the way they think, feel and relate to each other, in many cases leading to a complete breakdown of contact. One of the tech platforms analysed in this report is integral to Chinese Communist Party policy characterising the peaceful expression of views that may differ from those of the state or social activities such as a Tibetan language group as 'transnational organised crime'.

The effect that emerges from growing awareness of the surveillance apparatus among Tibetans, has particularly been felt on WeChat - the Chinese state-owned multipurpose messaging application - which was widely used by ordinary Tibetans in and outside Tibet ever since its inception a decade ago. However, the growing number of chat groups and their members inevitably came under state surveillance. This resulted in detention of Tibetans,[9] suspension of accounts,[10] and ban on keywords[11] deemed politically sensitive by the cyberspace authorities, due to which Tibetans on both sides have consciously learned to self-censor the keywords in both written and spoken languages, and instead use codewords[12] during their online communication. The consequence has been a growing sense of fear and isolation, separating many Tibetans inside Tibet and in exile from long time friends and close family.

Similar sophisticated big data analytics platforms are in operation in both Xinjiang and Tibet, and while specific systems might differ, the same overarching strategy of control and suppression through ethno-racial surveillance and data-driven policing is evident in both regions.

Linked to Tibet's intensive securitisation, Tibet Watch has also documented the imprisonment and torture of political prisoners, the increasing dominance of the Chinese language in Tibetan schools, surveillance in Tibetan Buddhist monasteries, and the rapid decline of the Tibetan nomad community through grazing bans, fencing of pastures, and displacement from their land, highlighting broader issues of dramatic environmental, cultural, and societal changes in occupied Tibet.

Findings of this bulletin were compared with a more comprehensive static analysis report by the Open Technology Fund's Red Team lab[13]. Turquoise Roof also reviewed central government procurement data related to public security and surveillance technologies in Tibet, internet-published reports by Chinese citizens about the app and extensive information from Tibetans now in exile obtained by Tibet Watch. Turquoise Roof is indebted to Tibet scholar Matthew Akester for obtaining technical details relating to the 'Tibet Underworld Criminal Integrated Intelligence Application Platform', and sharing them with us. This survey of the contemporary digital surveillance landscape in Tibet will be further developed in subsequent Turquoise Roof-Tibet Watch bulletins.

The National Anti-Fraud Centre app

The National Anti-Fraud Centre (Guó Jiā Fǎn Zhà Zhōng Xīn, 国家反诈中心) is a PRC government initiative focused on combating various forms of fraud, particularly those mediated through telecommunications and the internet. The centre reportedly operates as a hub for gathering and analysing threat intelligence related to fraudulent activities, coordinating with different central government departments, and law enforcement agencies. Its stated aims are to enhance public awareness of internet fraud, implement preventive measures, and effectively respond to fraudulent schemes. The establishment of this centre[14] is part of China's broader regulatory efforts to address the increasing societal challenges posed by rapid technological advancements in the realm of cyberspace.[15]

The National Anti-Fraud Centre app[16] is a multi-platform mobile application developed by the Telecommunications Network Fraud Investigation Division (电信网络诈骗犯罪侦查处) of the Criminal Investigation Bureau of the Ministry of Public Security (公安部刑事侦查局), and released in March, 2021 as part of the central government initiative to combat internet fraud.[17] The app serves as a platform for the public to report fraudulent activities, receive alerts about potential internet scams, and access information and resources to enhance awareness about various types of internet fraud. The app integrates functions for both prevention and reporting,[18] ostensibly aiming to reduce the incidence of internet fraud and to protect citizens from financial and personal security threats posed by fraudulent activities.

The National Anti-Fraud Centre app has raised serious concerns over privacy and digital rights among Chinese citizens. There are widespread claims that PRC citizens are compelled to install the app, which they allege demands extensive permissions and potentially violates their privacy. There are controversies surrounding its alleged use for monitoring online activities more broadly, particularly regarding users accessing overseas financial websites, triggering police interrogations and further scrutiny.[19]

The registration process for the app requires users to go through facial recognition capture while holding up their government identity card to the camera (see screenshot, figure 1), and allows the app to scan for other installed applications. These requirements in particular have raised concerns, as they could potentially enable extensive data collection and monitoring of individual internet user behaviour, tied to central government identity records. These requirements, taken with reports of mandatory installations enforced by local authorities particularly during the COVID19 pandemic, have led to public complaints published online, indicating growing concern among citizens about their privacy and digital autonomy in contemporary China.

Figure 1: National Anti-Fraud Centre app icon

One of the most contentious aspects of this app, certainly for urban middle class users, is its alleged tracking of users who visit foreign financial news websites, such as Bloomberg.[20] Users who access these sites are reportedly identified by the app and may subsequently face police interrogation. This level of surveillance suggests that the app is used not only for preventing fraud but also for monitoring citizens' online activities, particularly those related to overseas financial information data and international news consumption.

These practices point to a broader pattern of digital surveillance and control in China, where state security concerns often ride roughshod over individual privacy rights. The use of such an app as a tool for mass surveillance raises significant questions about the balance between national security, public interest in combating telecommunications fraud in China, and the protection of individual civil liberties and privacy. The extensive coverage and discussion of these issues by PRC citizens in Chinese language internet sources, aggregated and analysed by China Digital Times, highlight both a growing awareness among PRC citizens of individual privacy rights in the digital age, and increasing unease about mass surveillance.[21]

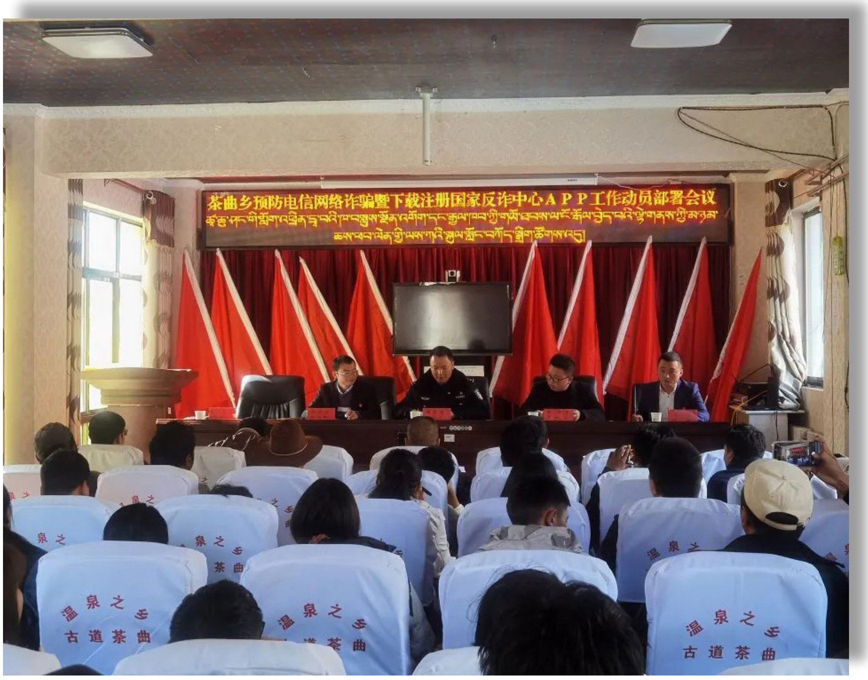

茶曲乡预防电信网络诈骗暨下载注册国家反诈中心APP工作动员部署会议
温泉之乡
古道茶曲

Figure 2: Meeting on telecommunications fraud prevention and the National Anti-Fraud Centre app download and registration in Tsachu Township where, in 2013, over hundreds of Tibetans led anti-mining protests, which was immediately suppressed with a series of mass arrests and 'patriotic education' campaigns.

Source: Driru County Public Security Bureau WeChat feed

Surveillance, the 'anti-fraud' app and Tibetan use of WeChat

Before the launch of the National Anti-Fraud Centre app in 2021, WeChat was a principal source of information used by researchers and journalists to monitor different emerging issues ranging from trending topics, blogs, and 'moments' to audio-visual contents and recordings of Buddhist teachings. For the first time, virtual chat groups directly accessible on smartphones allowed direct individual and group discussions[22] between Tibetans from different regions of Tibet and the exile.

However, the growing number of chat groups and their members inevitably came under state surveillance. This resulted in detention of Tibetans,[23] suspension of accounts,[24] and ban on keywords[25] deemed politically sensitive by the cyberspace authorities. As a result, Tibetans both in the PRC and in exile have consciously learned to self-censor the keywords in both written and spoken languages, and instead use codewords[26] during online communication with each other.

This has led to extreme psychological distress and pervasive fear, with many Tibetans, including close family or friends, completely ending their communication, often without explanation. Tibetans in exile, fearing harm for their compatriots in Tibet, often withdraw from contacts inside Tibet. Surveillance and self-censorship are particularly heightened on politically charged anniversaries or days of cultural significance such as 6 July, the Dalai Lama's birthday and 10 March, Tibetan National Uprising day in 1959 (and anniversary of the 2008 protests that swept across Tibet, leading to a crackdown of unprecedented scope and intensity).

The Party state's scrutiny over individuals can also intensify following external reporting on human rights violations in Tibet, as local authorities drill down on efforts to uncover sources of the news.[27]

A similar pattern has been observed in the seasonal incidence of targeted malware attacks on the Tibetan exile community over the past decade or longer.[28]

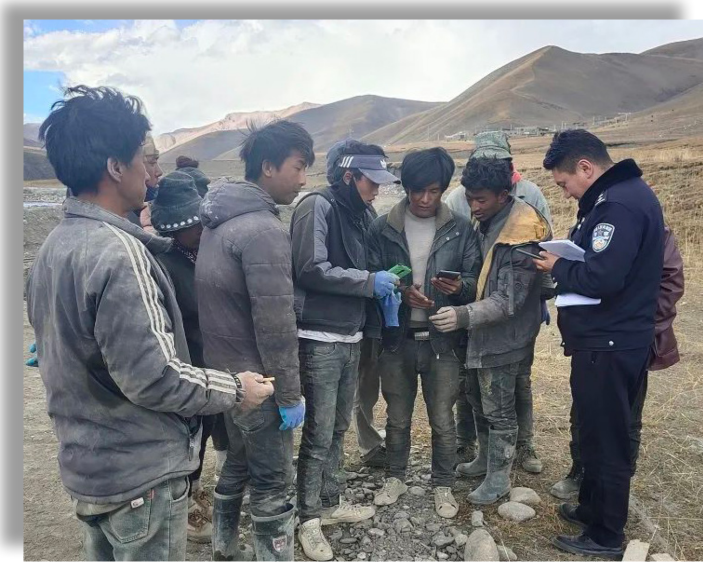


Figure 3: Outdoor campaign promoting National Anti-Fraud Centre app amongst labourers.

Source: Driru (Biru) County PSB, Nagchu Municipality (那曲市比如县公安局) (TAR) WeChat feed

The Tibetan Centre for Human Rights and Democracy notes in its 2020 report Surveillance and Censorship in Tibet: “An overwhelming number of interviewees agreed that since 2016, restrictions on local Tibetans and their phone and Internet connections have become noticeably severe. Jamyang, a teacher at a Tibetan religious institute in India, noticed unprecedented levels of surveillance and censorship since 2016 in his hometown of Mangra County in Tsolho (མཚོ་ལྷོ།)[29]. He had not experienced such restrictions during his two-month visit to Tibet in 2015. He added that local police were now quick to interrogate and charge anyone of ‘endangering state security’ for sharing news, articles, scriptures, and pictures of religious leaders that had originally been published outside of Tibet.”[30]

The same report detailed another testimony of a source in exile, who observed a marked rise in intrusive surveillance during his 2016 visit to hometown in Dola[31] in Tsojang[32] Tibetan Autonomous Prefecture, Qinghai, compared to his 2014 visit. The Tibetan added that he was given an iPhone to use by a branch office of the Party’s United Front Work Department, which undertakes a blend of intelligence, engagement and heavy-handed influence operations in order to promote PRC interests and ensure compliance with Party policy. The Tibetan later found that the phone had malware installed.[33]

The National ‘Anti-Fraud’ app was launched in 2021 in a context of an already intensifying digital surveillance on Tibetans via WeChat as well as other means.

In April 2021, apparently under suspicion of contacting exile Tibetans, several Tibetans were arrested in Driru County[34] in Tibet Autonomous Region (TAR), an area which in 2013 became a hub of resistance to harsh Chinese policies. A tough crackdown was imposed after Tibetans protested against mineral exploitation at mountains they regard as sacred, and objected to being forced to display the Chinese national flag.[35]

In one case, a Tibetan tour guide, Kunchok Jinpa, died following torture after he was accused of sharing information with Tibetan exiles via WeChat. Kunchok Jinpa, 51, died in hospital in Lhasa on 6 February 2021, less than three months after being transferred there from prison without his family’s knowledge. He had been serving a 21-year sentence for reporting protests in his native region, Driru.

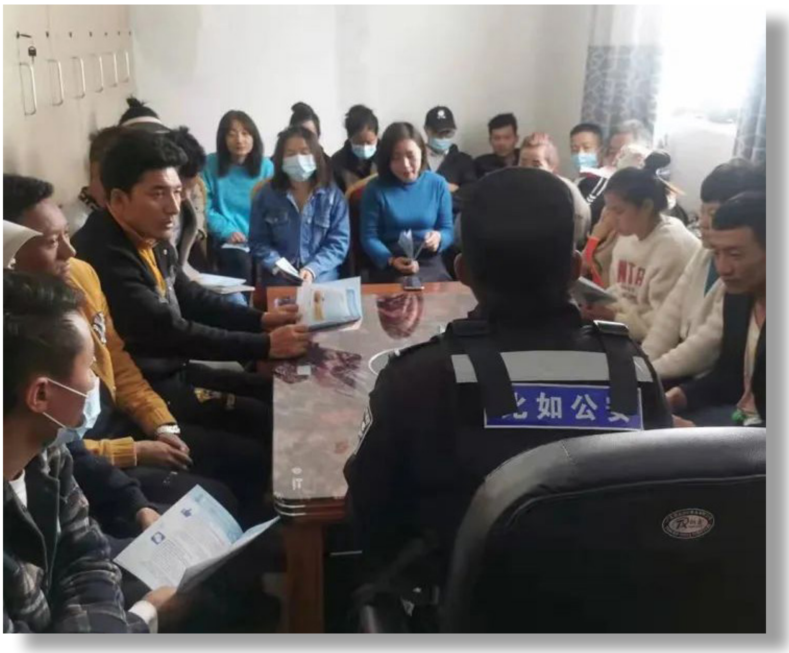


Figure 4: National Anti-Fraud Centre app Download and Registration campaign promotion being carried out amongst the public.

Source: Driru (Biru) County PSB, Nagchu Municipality (那曲市比如县公安局) WeChat feed

Little information about the identity of those arrested for attempting to send information about the protests outside Tibet is known. Only the identity of one of those detained is known - Gyajin, a father of three, arrested on suspicion of contacting Tibetans in exile through social media and by phone.[36] The arrest took place only after Kunchok Jinpa''s death, as well as other new details of the 2013 mass arrests and a 2015 self-immolation protest were reported by foreign media and research groups in the previous three months. Then, on 22 November 2021, the Driru County Propaganda Office posted on WeChat about its official promotional campaigns for the Anti-Fraud app, detailing how it approached "the masses", posted 400 posters of National Anti-Fraud Centre app, and taught the public how to scan the code to download the app, and "how to use the APP to conduct risk inquiries on payment accounts, websites, QQ, and WeChat".[37]

A year later, on 6 October 2022, amid the brutal, nationwide zero-COVID lockdown, Driru County PSB posted on WeChat about the app being promoted at COVID test checkpoints. The report begins with a quote on what is described as "Escort+Publicity" (护航+宣传): "Please keep one metre apart, line up, wear masks, and do not gather! After completing the nucleic acid test, please ask the police on duty to see if the 'National Anti-Fraud Centre' APP on your mobile phone is correctly installed and the early warning is turned on…"[38]

In 2023, Tibet Watch interviewed two newly arrived Tibetan refugees, who both shared experience of compulsory installation of the National Anti-Fraud Centre app. The young man from a nomadic family in Golog cited earlier in this report observed: "It looks like a surveillance app that tracks all our movements and places of stay." He said that other Tibetans told him that the app "tracks not only our movement but also has built-in automatic voice recording and photo-sharing functionalities. So every time I travel, I have to download, install this app, and uninstall it upon reaching my destination."[39]

The second refugee is a monk from Ngaba (Chinese: Aba) Tibetan and Qiang Autonomous Prefecture in Sichuan (the Tibetan area of Amdo), whose home county saw at least three fatal self-immolation protests in 2012. Describing the extreme caution he used to take in accessing foreign websites, he said: "My uncle told me that we would be punished severely if caught using VPN…On mobile, we have to install an application (国家反诈中心) that is said to be a surveillance app."[40]

Forensic analysis of the National Anti-Fraud Centre app

Turquoise Roof obtained a copy of the latest Android version and executed the app in a dynamic analysis tool. The tool is designed to detect and analyse potential behaviours by running files in an isolated environment, known as a ‘sandbox’, where the behaviour of the software can be observed without risking harm to the host system[41]. This tool is particularly useful for security professionals and researchers to identify, analyse, and understand potentially privacy-invasive software activities.

Dynamic analysis helps in identifying behaviours that may only be revealed during execution, such as the presence of malicious logic (‘malware’) or other malware-like, privacy invasive, or otherwise malicious activities. This could reveal, for example, how the app accesses and uses data, communicates over networks, and interacts with other applications or system components. By analysing these behaviours, researchers can identify potential surveillance activities. Situating these findings in the context of the wider digital surveillance ecosystem in Tibet then involves comparing the app’s activities with known surveillance practices and systems in the region, and in other frontier regions in the PRC, drawing connections to broader strategies of monitoring and control by the authorities. This analysis provided initial insights into the potential role of the Anti-Fraud app within the larger framework of digital surveillance in Tibet.

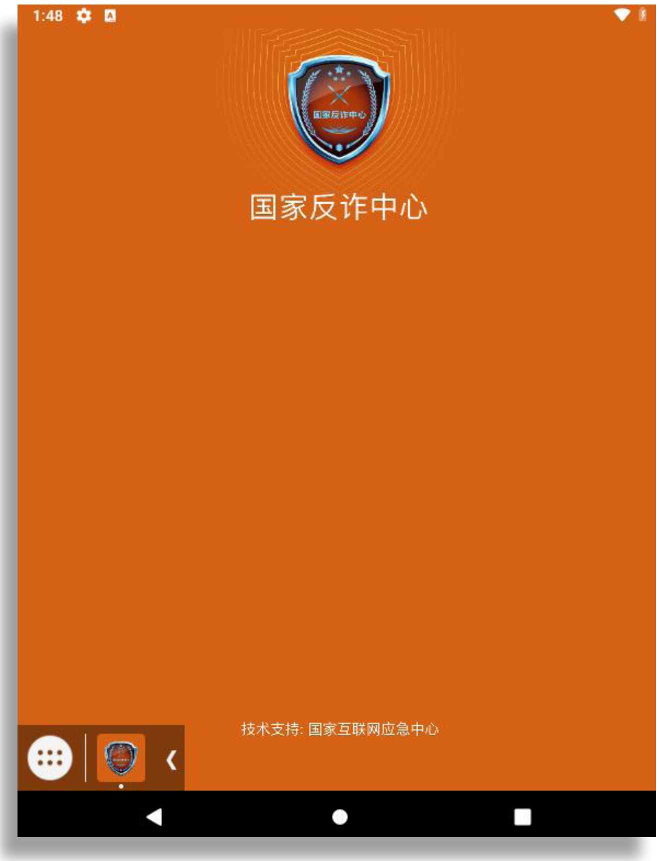


Figure 5: A screenshot of the National Anti-fraud app opening in the sandbox

Dynamic and contextual analysis of 2.0.12_Apkpure.apk (国家反诈中心)

SHA1: fe2e5d725e0ff558049656dbe548a89abf526608

App Permissions and other notable behaviours	Observations relating to privacy implications in Tibet
Has permission to receive SMS in the background, monitors incoming SMS	This can allow the app to access private messages without user awareness. This capability could be used to monitor personal communications and gather data that could be used for surveillance purposes, aligning with broader strategies of control and oversight in the region.
Has permission to read low-level log files	Potentially accesses sensitive user data, including personal information and activity logs. These logs can reveal extensive information about the device's operations, user behaviours, and app interactions, such as usage of VPNs or other prohibited apps. In a surveillance context, this could be used to track individual activities, preferences, and if ingested into a big data analytics platform, even identify patterns of behaviour at scale, contributing to broader monitoring and data collection efforts.
Detected TCP or UDP traffic on non-standard ports	Non-standard port traffic indicates that the app might be communicating with external servers in unconventional ways, which could be a privacy risk. This feature enhances the capability for covert surveillance, potentially bypassing standard network monitoring and security measures when communicating with police servers.
Has permission to draw over other applications or user interfaces	This could be used for more than just providing helpful overlays or user interface enhancements. This capability could be used to capture sensitive user inputs surreptitiously. It potentially allows the app to present false screens, capture user input (including passwords), or even trick users into interacting with seemingly benign pop-ups or notifications. This overlay capability, if misused, could conceivably be a tool for targeted surveillance and data collection.

App Permissions and other notable behaviours	Observations relating to privacy implications in Tibet
Obfuscates method names	Indicates efforts to hide the app's functionality, making it harder for users and researchers to understand what the app is doing. This may indicate an effort to conceal the app's internal workings and functionalities. This obfuscation could be a tactic to hinder analysis and understanding of the app's true capabilities or intentions. It raises transparency issues, making it challenging for users or external auditors to ascertain what the app is actually doing.
Has permission to read the SMS storage	This can allow the app to access private messages without user awareness. This access allows the app to read all stored text messages on a user's device, potentially including sensitive and private communications. In a region where monitoring and controlling information flow is paramount for the authorities, this feature could be used to track personal conversations, gather intelligence to ingest into public security analytics systems, in order to identify dissent or non-compliance with government directives. It represents a significant invasion of privacy and could contribute to the broader strategy of surveillance and control.
Has permission to mount or unmount file systems (removable storage)	Allows the app to access (and potentially modify) data on external storage devices connected to the phone. This could be used to read, alter, or delete data stored on these devices. Such access poses a significant privacy risk, as it could lead to unauthorised exposure or loss of personal data stored on external drives or memory cards to the app.
Has permission to read the phone's state (phone number, device IDs, active call etc.)	In Tibet's surveillance environment, this data could be ingested into a police analytics platform to facilitate the tracking of individuals' real-world identities (linking IMEI to biometric data) and their communication patterns. Such access not only compromises anonymity at an individual level, but also provides a means to closely monitor wider personal networks and interactions, aligning with broader state surveillance objectives.

App Permissions and other notable behaviours	Observations relating to privacy implications in Tibet
Has permission to read the call log	This feature allows the app to access detailed records of incoming and outgoing calls, including timestamps and contact information. In a region under tight surveillance, such access could be used to map social networks, monitor contacts, and potentially identify dissidents or track, at scale, interactions considered sensitive or subversive by the authorities.
Accesses Android OS build fields	The app's ability to access build fields means it can retrieve information about the specific version of the operating system, the phone's model, and other technical details of the device. In the Tibetan context, where state surveillance is extensive, such data could be used to identify specific devices, enumerate software vulnerabilities, and thereby potentially tailor targeted surveillance tactics to a registered individual's phone, should they subsequently uninstall the app.
Has permission to read the default browser history	This feature enables the app to track and analyse users' internet browsing patterns, including websites visited and the frequency of visits. In a region where information control is critical, such access could be used to monitor and potentially censor or penalise access to non-state-approved information sources. This capability also poses a risk to personal privacy, as it could reveal users' interests, beliefs, or affiliations based on their online activities.
Has permission to take photos	Beyond needing this permission for the portrait capture (with government issued ID card), linked to the face recognition capability, this feature could allow for unauthorised photo capture, potentially used to gather visual data on users and their surroundings. This permission raises privacy and security concerns in an already heavily surveilled region.

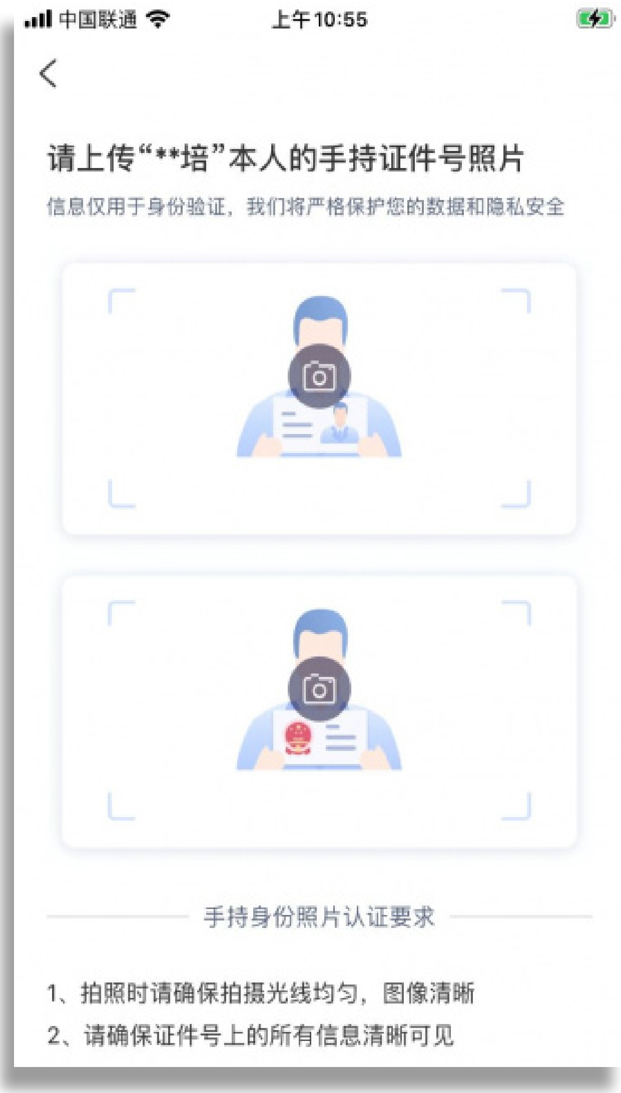
App Permissions and other notable behaviours	Observations relating to privacy implications in Tibet
Face recognition verification with government issued ID card	The face recognition verification feature in the Anti-Fraud app, which requires users to match their faces with government-issued ID cards, could be a powerful tool within Tibet's surveillance regime, if connected to a police analytics platform. This functionality not only verifies user identity but also potentially links wider digital activity to real-world identities, enhancing the state's ability to monitor individuals. Such biometric verification, when combined with what we know about the overall digital surveillance infrastructure, could significantly impact personal privacy and freedom. Face recognition data harvested at scale through this app could potentially be ingested into a big data analytics platform. In a comprehensive surveillance system like that in Tibet, this biometric data can be integrated with other data sources to enhance tracking and monitoring capabilities at population scale. The analytics system could analyse patterns, behaviours, and social connections, contributing to a detailed profiling of individuals. Such a process aligns with broader surveillance and control strategies, and would significantly impact personal privacy and freedom.
Has permission to query the list of currently running applications	The app's permission to query the list of currently running applications could be significant in the context of Tibet's surveillance system. This feature allows the app to identify and monitor other apps in use, potentially giving insights into users' habits, preferences, and even their political inclinations based on the types of apps they use. Notably this could be used to identify usage of proscribed VPNs, in a region where citizens have been jailed for using VPNs. This kind of monitoring can also contribute to broader data collection and surveillance efforts, potentially leading to more targeted and personalised surveillance strategies. A strategy of content filtering and surveillance at the edge of the network, on the user's device, rather than at international gateways, would be reminiscent of the proposed mandatory pre-installation of the now (largely forgotten) 'Green Dam Youth Escort' (绿坝·花季护航) software of 2009.

Decoding the 'maze of digital ethno-racial profiling'

The permissions detailed above grant the app's operators access to sensitive user data or control over key device functionalities. The broad scope of these permissions, allowing for highly invasive surveillance, along with mandatory installation aligns with what is known about the extensive surveillance practices in the region.

Given the extensive surveillance infrastructure in Tibet, and the increasing level of Public Security Bureau (PSB) database systems integration detailed in government procurement documents we have reviewed, our analysis suggests that data collected by the Anti-Fraud app could connect to PSB databases beyond those of the Telecommunications Network Fraud Investigation Division, and into wider systems operated by the Criminal Investigation Bureau. The mandatory installation of the app at police checkpoints in Tibet could serve as a platform for harvesting a dataset used for monitoring and controlling the population beyond the incidence of telecommunications fraud, particularly in suppressing dissent and cultural expression.

A similar point can be made about the reported forensic extraction of data at the checkpoint referred to in the interview transcript ("even mobile phones are scanned and searched")[42]. This checkpoint protocol - smartphone data extraction, in parallel with the mandatory installation of a police surveillance app - aligns with broader strategies of maintaining tight control over frontier region populations in China - not just in Tibetan areas, but also in Xinjiang - using digital platforms and mobile apps to reinforce the central government's surveillance and security objectives.



请上传“**培”本人的手持证件号照片

信息仅用于身份验证，我们将严格保护您的数据和隐私安全

手持身份照片认证要求

1、拍照时请确保拍摄光线均匀，图像清晰

2、请确保证件号上的所有信息清晰可见

Figure 6: The National Anti-fraud centre app directs users to upload handheld government ID cards during face recognition onboarding to the app

Universal Forensic Extraction Devices (UFED) are products originally manufactured by the Israeli company Cellebrite,[43] and while security personnel in Tibet have been reportedly using Cellebrite UFEDs at checkpoints[44] recent procurement data[45] also shows that a Chinese company, Meiya Pico,[46] is increasingly supplying police in Tibet and Xinjiang with UFEDs and digital forensics labs. Regardless of manufacturer, these portable UFED devices are typically used by PRC police for forensic data extraction from mobile devices.

In an article for Logic Magazine[47] anthropologist Darren Byler details the intensive surveillance practices now common in Xinjiang, particularly focusing on their impact on Uyghur communities. Byler describes how security checkpoints combined with advanced surveillance technologies have become commonplace forming “a maze of digital ethno-racial profiling” deeply impacting daily life. The article details the role and impact of such surveillance measures and the technology used, such as the ‘Clean Net Guard’ (Jìng Wǎng Wèi Shì, 净网卫士) app[48] and UFEDs for scanning smartphones:

“...at some checkpoints, officers asked Uyghur young people to give them the passwords to unlock their smartphones. The officers then looked at the spyware app Clean Net Guard, built by state contractor Landasoft, a company that describes itself as a Chinese version of Palantir, using open-source software from the U.S.-based company Oracle. This app automatically scans smartphones registered to Uyghurs, searching through WeChat, Weibo, Douyin, and other apps looking for thousands of flagged images and text associated with so-called extremist groups, Islam, and Uyghur political history...”

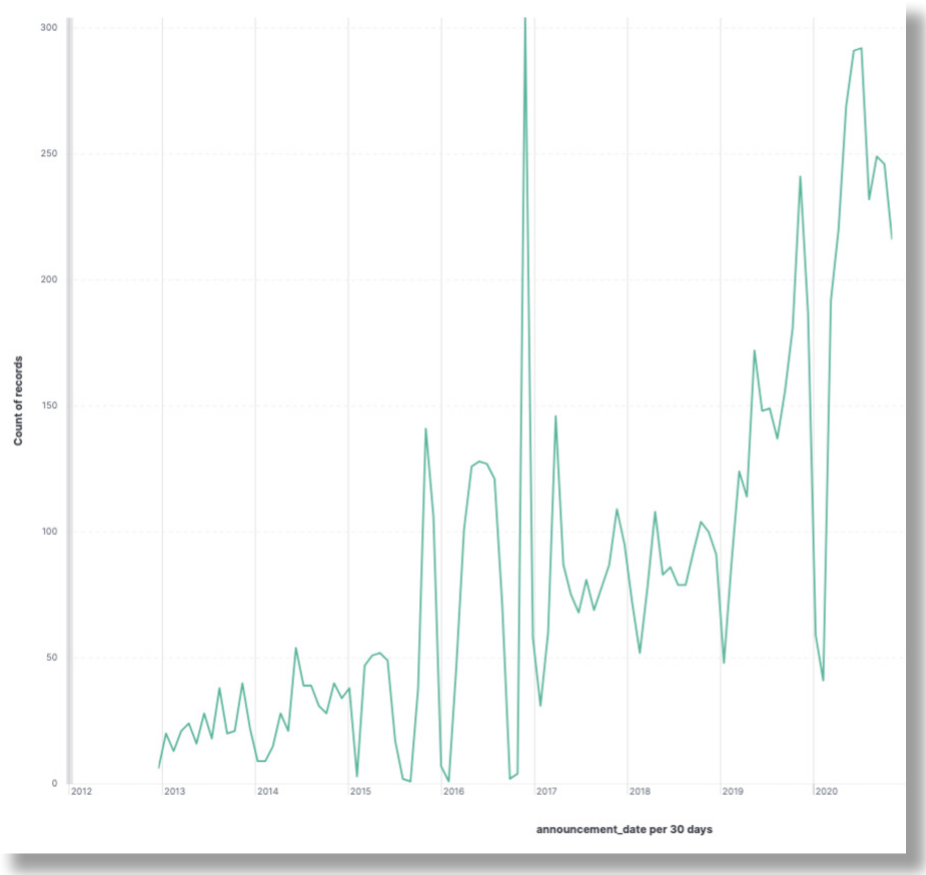


Figure 7: Incidences (8,338) of PRC central government procurement notices that relate to purchases in 西藏 (Tibet) (2013-20). Generated from data scraped from ccgp.gov.cn

Source: SecDev/Turquoise Roof

Maya Wang, Human Rights Watch's interim China director, has also researched the broader implications of these algorithmic surveillance practices on the lived experiences of the Uyghur population. In 2019, Wang reverse engineered a police app that fed into a big data analytics system known as IJOP, or the 'Integrated Joint Operations Platform'[49] (Yī tǐ huà lián hé zuò zhàn píng tái, 一体化联合作战平台) that tracks Turkic Muslim individuals in Xinjiang considered a potential threat by the authorities. The report's digital forensics, combined with in-field ethnography, illustrated the brutal logic of machine learning-driven state surveillance, including the mass collection of biometric data, monitoring of online activities, and the intense scrutiny of everyday behaviours to support 'predictive' or intelligence-led policing[50] (qíng bào zhǐ dǎo jǐng wù 情报指导警务) at population-scale.

The Human Rights Watch report's remarkable insights into the IJOP system were derived from a forensic examination of the mobile police app that connects directly to the IJOP platform, rather than the central (IJOP) system itself. Ethical, legal, and security considerations limited the scope of the reverse engineering engagement, so for example, no connections were made to external servers in the region. System-wide functionality was extrapolated based on code structures in the sub-system, the mobile app, triangulated with earlier HRW research into the central system,[51] and in-field interviews with Uyghur refugees describing interactions with the police. Wang's findings significantly enhance our understanding of the IJOP system and the wider context, yet leave several aspects of this 'black box' under explored or unknown.

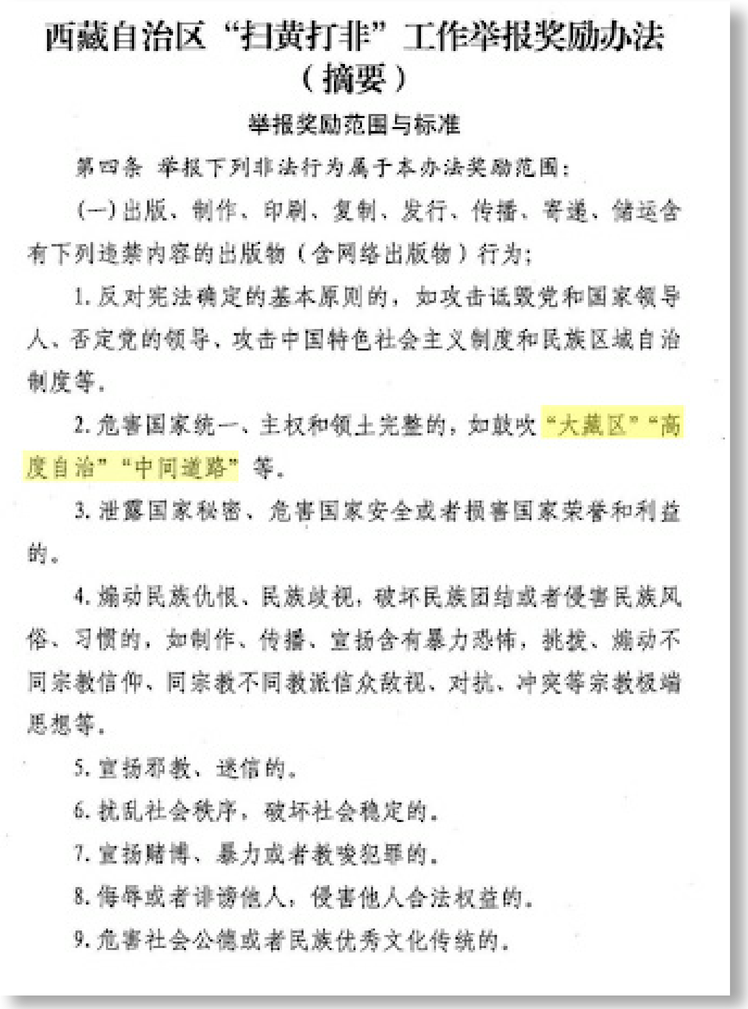
Comparing these reports from Xinjiang to the eyewitness account in Tibet Watch's bulletin, there are clear parallels in the deployment of UFEDs and spyware at police checkpoints. Similarly, sophisticated big data analytics platforms are in operation in both regions, and although specific systems might differ, the same overarching strategy of control and suppression through intelligence-led policing is evident in both regions. Key features of Xinjiang's extensive surveillance system were introduced under the tenure of then Party Secretary Chen Quanguo (陈全国), after he was transferred to that region from the Tibet Autonomous Region (TAR).[52]

This indicates a similar approach to ethno-racial surveillance and data-driven policing across the different frontier regions of the PRC, highlighting a broader pattern in the implementation of state security measures. IJOP, for example, finds a close counterpart in a big data policing system known as the 'Tibet Underworld Criminal Integrated Intelligence Application Platform' (xī cáng hēi è fàn zuì qíng bào zōng hé yīng yòng píng tai, 西藏黑恶犯罪情报综合应用平台).

The upgrade of this intelligence analytics platform commenced in November 2020, with a budget to improve the existing system of RMB 900,000 (at that time approximately USD 600,000).[53] The expansion of the capacity of this police intelligence system followed the announcement of a crackdown on traditional Tibetan cultural practices, in the name of fighting 'organised crime'.

According to Human Rights Watch, in February 2018, the PSB in the TAR issued a police notice that encouraged the public to inform on “underworld forces”[54] and declared a range of traditional or informal social activities among Tibetans to be illegal. These reportedly included grassroots initiatives for environmental protection, language preservation, and dispute mediation, some of which the notice claimed “secretly encourage support for the exiled Dalai Lama or for Tibetan independence”. The police notice also described any expression of support for the Dalai Lama’s proposal for increased autonomy in Tibet as a form of ‘organised crime’. According to HRW, this was the first time such activities and opinions have been officially listed as crimes by a provincial-level body in Tibet.[55]

While other provinces in China have focused their versions of the anti-organised crime drive on activities such as gun-running and human trafficking, authorities in the TAR have used the campaign to target suspected political dissidents and to suppress civil society initiatives.



西藏自治区“扫黄打非”工作举报奖励办法
（摘要）

举报奖励范围与标准

第四条 举报下列非法行为属于本办法奖励范围：

(一)出版、制作、印刷、复制、发行、传播、寄递、储运含有下列违禁内容的出版物（含网络出版物）行为；

1.反对宪法确定的基本原则的，如攻击诋毁党和国家领导人、否定党的领导、攻击中国特色社会主义制度和民族区域自治制度等。

2.危害国家统一、主权和领土完整的，如鼓吹“大藏区”“高度自治”“中间道路”等。

3.泄露国家秘密、危害国家安全或者损害国家荣誉和利益的。

4.煽动民族仇恨、民族歧视，破坏民族团结或者侵害民族风俗、习惯的，如制作、传播、宣扬含有暴力恐怖，挑拨、煽动不同宗教信仰、同宗教不同教派信众敌视、对抗、冲突等宗教极端思想等。

5.宣扬邪教、迷信的。

6.扰乱社会秩序，破坏社会稳定的。

7.宣扬赌博、暴力或者教唆犯罪的。

8.侮辱或者诽谤他人，侵害他人合法权益的。

9.危害社会公德或者民族优秀文化传统的。

Figure 8: First page of Measures for rewarding informants to ‘’eliminate pornography and illegal content’ which includes prohibited terms: “Greater Tibet”, “high degree of autonomy”, and the “Middle Way”.

Source: Tibet Watch

In one Tibetan area, being found with a photo of the Dalai Lama was even deemed by the authorities to be as serious an offence as keeping a gun. After local anti-gun campaigns were implemented in Kardze (Chinese: Ganzi) Tibetan Autonomous Prefecture in Sichuan,[56] local Tibetans in Dza Wonpo, Sershul county in Kardze, were warned, amid search operations following a death in custody of a 19-year-old monk, that those found with images of the Dalai Lama would face charges similar to those charged for keeping guns.[57] Underlining the absurdity of this official drive, across Tibet, Tibetans have often handed in their guns and knives in a community-driven effort with the unspoken intention of honouring the Dalai Lama's position of nonviolence.

The campaign continued into late 2023, in Tibet Autonomous Region, with The TAR Working Group office on the ''elimination of pornography and illegal content" publishing a notice on 16 November 2023, 'Measures for rewarding informants to ''eliminate pornography and illegal content.'[58]

The notice reveals the continuation of a keyword term previously enlisted in the 'underworld' campaign - "the Middle Way", policy of the exile Tibetan government, the Central Tibetan Administration (CTA), that seeks a genuine autonomy under the sovereignty of the PRC. It also includes two other keywords - ''high degree of autonomy'', referring to the Middle Way, and "greater Tibet''. The latter is a term which the first Sikyong (political leader) of CTA, Samdhong Rinpoché, described as having never been used by Tibetans themselves for Tibet, but instead the PRC uses to refer to all areas inhabited by Tibetans which are at present divided into Tibet Autonomous Region and Tibetan autonomous prefectures and counties outside TAR.[59]

Article Four lists contents (including online publications) related to these keywords as "illegal" with cash rewards (Article Seven) for any reports on their publishing, making, printing, reproducing, disseminating, transmitting, delivering, and storage of publications. Prohibited content also includes "other contents prohibited by laws, administrative regulations and state provisions, such as "the central government's strategy for the governance of Tibet and the party's policy on nationalities and religion".[60]

The definition of organised crime as outlined in the United Nations Convention against Transnational Organised Crime,[61] and subsequently adopted by the EU,[62] frames the activity as "a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit."

China's approach of equating non-violent preservation of Tibetan culture and language rights with organised crime significantly undermines human rights. This position by the Party state has acquired additional force since the unprecedented wave of protests[63] and self-immolations[64] from 2008 and 2009 onwards.

This approach renders international law enforcement cooperation to combat genuine transnational organised crime more difficult. It finds parallels in the abuse of Interpol's Red Notice system for the transnational persecution of China's political opponents, which similarly undermines the very foundations of international police cooperation.[65]

U.S. database Oracle integral to Tibet police work

The ‘Tibet Underworld Criminal Integrated Intelligence Application Platform’ is described in a document attached to procurement notices regarding its upgrade as a sophisticated policing tool that employs big data analytics to support intelligence-led policing strategies. It integrates data from various existing PSB systems in the TAR into a centralised Oracle database.[66] The platform is presented as being designed to enhance the efficiency and effectiveness of law enforcement in Tibet, “guiding criminal underworld investigation work, analysing, and studying criminal situations and organisations ... in order to directly investigate extremely serious criminal cases.”[67] The platform is described as being only accessible via the TAR PSB’s internal network, with no connection to the public internet.[68] The procurement notice indicates that due to the informatization localization project within the TAR PSB, the contractor should aim to replace the Oracle database with a Chinese equivalent.[69]

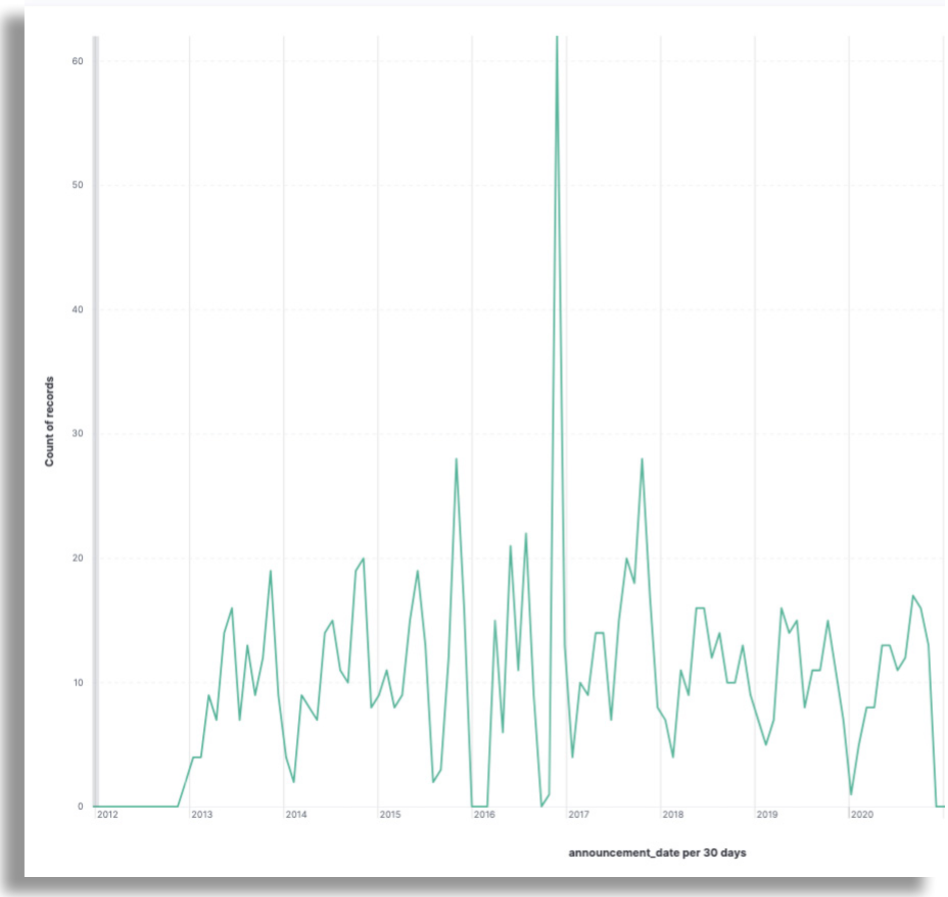


Figure 9: Incidences (1,096) of PRC central government procurement notices that mention Oracle database software (2013-20). Generated from data scraped from ccgp.gov.cn

Source: SecDev/Turquoise Roof

The Tibet Underworld Intelligence Platform "takes full advantage of the integrated affordances of 'big data' computing" in order to "achieve dynamic management and control of key personnel."[70] The term "key personnel" or "focus personnel" (zhòng diǎn rén yuán 重点人员) used here, refers to individuals or types of individuals arbitrarily deemed a potential threat to CCP-defined "regional stability" (increasingly determined through algorithmic scoring mechanisms, as in the PoliceGIS sub-system of Police Cloud, for example) and subject to special control measures by the authorities. According to Human Rights Watch, usage of the term to describe suspected political opposition or views even moderately critical of the Chinese Party state is far more prevalent in Tibet than in China as a whole.[71]

Keyword search from PSB terminals pushes automated summaries of key personnel dossiers that show "personnel relationship networks, activity 'trajectory'[72], dynamic management and control records, etc."[73] The entities stored in the platform's database are linked together semantically to form a knowledge graph. The system uses data mining and interactive visual display of the knowledge graph to analyse relationships and networks among individuals. The platform supports continuous discovery of related key personnel based on complex filtering conditions, including "kinship, social networks, and group affiliations".[74] It integrates various PSB databases, creating a "comprehensive view of personnel, cases, and locations".[75] These electronic profiles consolidate a wide range of sensitive personal information, such as residence, vehicle registration, phone, internet browsing data, and social connections, along with police records of surveillance activities, further enhancing the system's capability for tracking and monitoring.

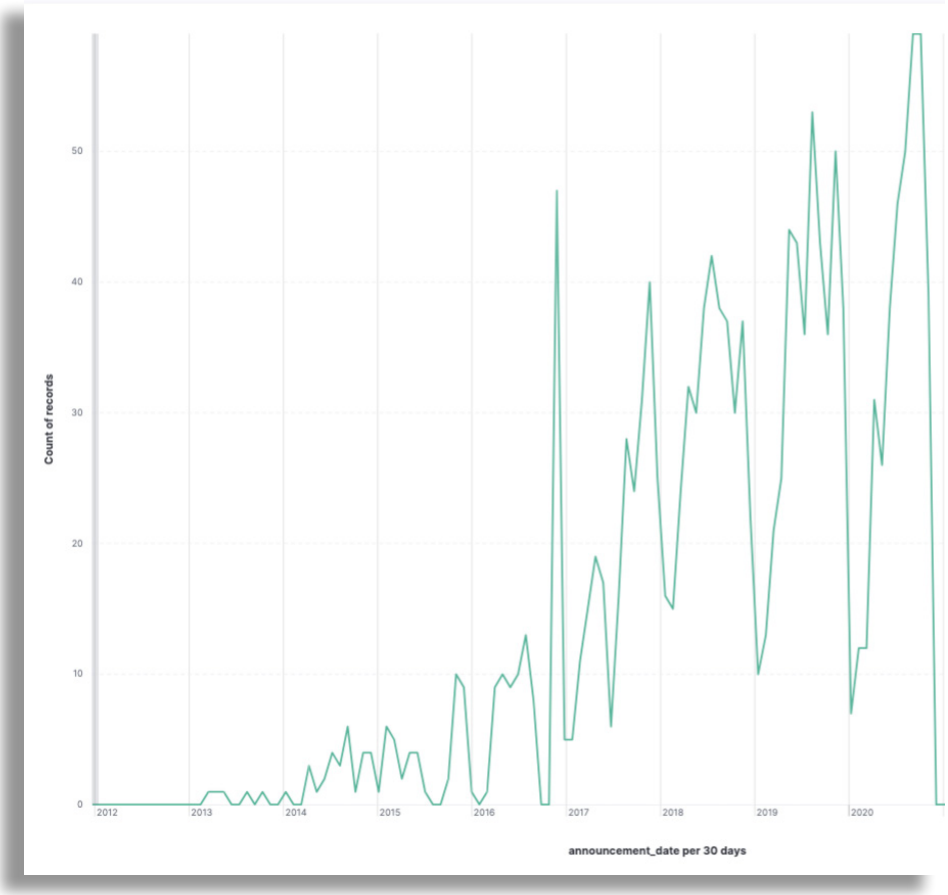


Figure 10: Incidences (1,580) of PRC central government procurement notices that mention "大数据" AND "监控" ("big data" AND "policing" systems (2013-20). Generated from data scraped from ccgp.gov.cn

Source: SecDev/Turquoise Roof

Data sources that are “classified and aggregated” by the Tibet Underworld Intelligence Platform through the PSB’s internal network, from other PSB criminal investigation databases are said to include: “police information data (sourced from the 110 police handling system)[76]; case data (sourced from the criminal comprehensive information system); police reporting system; police comprehensive platform; “key personnel” data (from the criminal information system); other databases”.[77] The system “...concatenates and integrates criminal case information resources, strengthens coordination and cooperation among various police departments”[78] extending beyond the TAR into any areas where there are Tibetans who might be suspected of engaging in “cross-regional gang criminality”.[79]

Cross-regional police cooperation on Tibetans who are under state surveillance is demonstrated by the case of prominent imprisoned writer Go Sherab Gyatso. Go Sherab is a Tibetan monk, passionate educator and outspoken public intellectual who is known to have been detained several times since he was 22 years old, on charges for instance of displaying a photograph of the Dalai Lama.[80] Go Sherab Gyatso studied at Kirti monastery in Ngaba, the eastern Tibetan area of Amdo, where a wave of self-immolation protests began when fellow Kirti monk Tapey set himself on fire in February 2009. Although Go Sherab Gyatso was detained[81] in the same province of his hometown, Sichuan, his arrest was carried out by Chinese State security officers from the TAR,[82] he was later tried in secret in Lhasa,[83] and is now serving a ten-year sentence in the TAR at Chushul prison, 20 kilometres southwest of Lhasa.[84]

Conclusion

It is reasonable to hypothesise that the dataset collected by the mandatory installation of the Anti-Fraud app, and the data extracted by UFEDs at checkpoints, also contribute data that feeds into databases that are integrated into the Tibet Underworld Intelligence Platform. Given the Anti-Fraud app's extensive access to a mass of sensitive personal information through intrusive permissions and forced installation, and given the Tibet Underworld Intelligence Platform's integration of numerous Criminal Investigation Bureau databases (the Telecommunications Network Fraud Investigation Division that analyses data from the anti-fraud app, being one of the CIB's units) it would be more remarkable if the dataset derived from the anti-fraud app and UFED extractions were not integrated in this manner. Such integration would align with the broader trend of increased data consolidation, integration, and network interconnectivity in the PRC's digital surveillance infrastructure, as described in recent (post-2020) procurement notices, patents, and academic research literature (notably in MSc dissertations in police college journals).

China's algorithmic surveillance ecosystem in Tibet and Xinjiang, involving the deployment of large-scale surveillance and AI analytics, has induced a society-wide 'chilling effect,' influencing individuals to alter their behaviours out of fear of repercussions. This constant monitoring can lead to self-censorship and a decline in cultural expression, as people become wary of engaging in activities that might be perceived as crossing the CCP's continually shifting red lines.

This atmosphere of dread profoundly impacts the social and cultural fabric of these regions, reinforcing control and conformity. The intense cultural trauma engendered by domestic surveillance in China's frontier regions including of WeChat, in parallel with the psychological impact of phishing and malware campaigns targeting exile networks over several decades, severs digital ties between the diaspora populations and their compatriots.

The surveillance landscape in Tibet demands continued international scrutiny and research that contributes to a broader dialogue around the appropriate balance between state security, personal privacy, and free expression. This bulletin offers a glimpse into a vast and opaque apparatus of repression that monitors the daily lives of the inhabitants of a region the size of western Europe, but consists of 'predictive', black box AI-driven systems, the inner workings of which we can know remarkably little about. Our initial findings clearly underscore the urgent need for greater global awareness and action to prevent the egregious abuses of state power being documented by Tibetan monitoring NGOs.

The Tibetan people face these challenges, but they should not do so alone. The international community must engage in robust discourse about the implications of such AI-driven surveillance practices on fundamental human rights, especially in countries still under occupation.

Recommendations

To international governments

- Adopt robust measures to ensure that national companies cannot provide resources to, or otherwise participate in, mass surveillance in Tibet.
- Urge the Chinese government to end its policy of mass surveillance in Tibet and the wider People's Republic of China.

To the government of the United States

- In addition to the above, conduct an inquiry into the role of US-based companies including Oracle, in providing police in Tibet and the People's Republic of China with products that may have facilitated police surveillance.
- Press for any ongoing supply of such products to be halted.

To international companies

- Conduct an internal review to assess whether company products and expertise are being provided to police in Tibet and the People's Republic of China for use in surveillance, and halt any direct or third-party supply of these goods.
- Evaluate and review environmental, social, and cultural rights violations of Chinese companies before establishing any partnership on technology and knowledge exchange

To the government of the People's Republic of China

- Introduce legislation to protect the right to privacy as a fundamental human right.
- Investigate claims that police have coerced Tibetans and Chinese nationals into installing the National Anti-Fraud Center app or other apps on their mobile devices.
- Abolish any government regulations requiring users to install the National Anti-Fraud Center app or other surveillance apps on their devices.
- Review the Cyber Security Law of the People's Republic of China and amend its provisions in line with international standards on freedom of expression and freedom to seek, receive and impart information and ideas.

Endnotes

1 The term ‘Tibet’ is used generally in this briefing to refer to areas within the PRC that are traditionally inhabited by Tibetans. The eastern areas of the plateau, Kham and Amdo, were incorporated into Chinese provinces, where they were designated ‘Tibetan autonomous’ prefectures and counties within the western provinces of Qinghai, Gansu, Sichuan, and Yunnan. The term TAR, a province-level administration established by China in 1965, describes the western and central parts of the Tibetan plateau traditionally known as ‘U-Tsang’. The PRC has a long and documented history of colonisation in Tibet since its invasion in the middle of the twentieth century. Over the past seven decades China has renamed thousands of Tibetan towns and landmarks, introduced territorial divisions, and imposed a slew of social and cultural restrictions. The geographical divisions that created the Tibet Autonomous Region (TAR) are a case in point.

2 Civilian AI-driven surveillance systems, such as those deployed in Tibet and Xinjiang, find their origins in military Command and Control (C4ISR) doctrine (see DeLanda, Manuel (1991). War in the Age of Intelligent Machines. New York: Zone Books. Paperback – ISBN 0-942299-75-2). Separately, Chinese software developers have acknowledged this evolution: “treating a city like a battlefield, the platform was designed to “apply the ideas of military cyber systems to civilian public security,” Wang Pengda, an engineer for the China Electronics Technology Group involved in developing big data policing platforms in Xinjiang, said in an official blog post. ‘Looking back, it truly was an idea ahead of its time.’” Original blogpost https://www.sohu.com/a/249485931_757363 archived at https://archive.is/AqTeH cited by Chris Buckley and Paul Mozer in New York Times, 22 May 2019, https://archive.is/DyybE

3 Cited by Chris Buckley and Paul Mozer in New York Times, 22 May 2019, https://archive.is/DyybE

4 ‘Forced to install phone app at security checkpoints’ (Tibet Watch, 6 September 2023) https://www.tibetwatch.org/news/2023/9/6/forced-to-install-phone-app-at-security-checkpoints

5 Golog Tibetan Autonomous Prefecture (果洛藏族自治州)

6 https://apps.apple.com/cn/app/%E5%9B%BD%E5%AE%B6%E5%8F%8D%E8%AF%88%E4%B8%AD%E5%BF%83/id1552823102

7 Including Android permissions - permissions on Android (Google for Developers) Retrieved 2024-01-09

https://developer.android.com/guide/topics/permissions/overview

8 Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, Amy Stevens, The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe, Journal of Human Rights Practice, 2023; https://academic.oup.com/jhrp/advance-article/doi/10.1093/jhuman/huad020/7234270

9 Tibetan man imprisoned for sharing books on Tibet, (Tibet Watch, November 18, 2019), https://www.tibetwatch.org/news/2019/11/18/tibetan-man-imprisoned-for-sharing-books-on-wechat ; Three Tibetans arrested for sharing photos of an official event on WeChat group, (Tibet Watch, August 10, 2021), https://www.tibetwatch.org/news/2021/8/10/three-tibetans-arrested-for-sharing-photos-of-an-official-event-in-wechat-group ; Founder of Chatgroup released in critical health, (Tibet Watch, December 23, 2021), https://freetibet.org/latest/founder-of-chat-group-released-in-critical-health/ ; Two sisters detained after chatgroup messages, (Tibet Watch, December 5, 2023), https://freetibet.org/latest/two-sisters-detained-for-chat-group-messages/ , Retrieved 16 January 2024

10 China continues to push “underworld forces” campaign in Tibet, (Tibet Watch, July 3, 2018), https://www.tibetwatch.org/news/2020/7/3/china-continues-to-push-underworld-forces-campaign-in-tibet

11 Tibetans blocked at Kalachakra on boders and on WeChat, (The Citizen Lab, January 10, 2017), https://citizenlab.ca/2017/01/tibetans-blocked-from-kalachakra-at-borders-and-on-wechat/

12 In a voice message, heard by Tibet Watch, a Tibetan mother in Lhasa recently told her son to tell his

wife to stop contacting her because of a photo of Sangye (Buddha) , a reference to an image of the Dalai Lama on her WeChat profile. The message followed a WeChat call the daughter-in-law made from India after which everyone in the family except for those in India disappeared from the chat group. In another example of using less sensitive coded phrases, an eight-year-old Tibetan girl, now in exile, consistently used Lama, a general honorific title for spiritual leaders in Tibetan Buddhism, instead of other specific words Tibetans normally use for the Dalai Lama, such as Gyalwa Rinpoche (Tibetan) and Gongsa Chok (Tibetan). See interview here: https://www.tibetwatch.org/news/2023/10/12/a-photo-of-lama-hidden-in-a-box

[13] China's National Anti-Fraud Centre – Security Assessment (Open Technology Fund, Wed, 2022-09-21 13:47) https://www.opentech.fund/news/chinas-national-anti-fraud-Centre-security-assessment/ Retrieved 2023-11-14

Editor's Note: The auditors did not go through a coordinated disclosure process regarding the vulnerabilities discovered in this report due to the risks involved with engaging a potentially sensitive adversary. A copy of the full security assessment can be obtained by emailing OTF.

[14] 中华人民共和国反电信网络诈骗法 (Anti-Telecommunications and Internet Fraud Law of the People's Republic of China) 2022-09-02 22:21 Source: Xinhua News Agency. Retrieved 2024-01-09.

https://www.gov.cn/xinwen/2022-09/02/content_5708119.htm

[15] Full text (English version): China's Law-Based Cyberspace Governance in the New Era. 中华人民共和国国务院新闻办公室 (State Council Information Office of the People's Republic of China) Retrieved 2024-01-09.

[16] https://apps.apple.com/cn/app/%E5%9B%BD%E5%AE%B6%E5%8F%8D%E8%AF%88%E4%B8%AD%E5%BF%83/id1552823102

[17] 何清怡 (2021-04-23). "中國大陸推反詐騙 APP，被指強制民眾下載、侵犯私隱等，你如何看?". Initium Media (Hong Kong). Archived from the original on 2021-06-28. Retrieved 2024-01-10.

[18] "国家反诈中心"App正式上线，快来安装吧！". Changjiang Daily (China). Ministry of Public Security News Centre, Henan Province. 2021-04-30. Archived from the original on 2021-05-14. Retrieved 2024-01-09.

[19] 古莉 (2021-09-14). "中国警方利用两亿手机反欺诈APP 识别看境外金融新闻者" ["Chinese police use anti-fraud app installed on 200 million phones to identify people who access financial news from abroad"]. Radio France internationale. Archived from the original on 2021-10-24. Retrieved 2024-01-09

[20] Sun, Yu; Liu, Nian (2021-09-14). "China uses anti-fraud app to track access to overseas financial news sites". Financial Times. Beijing. Archived from the original on 2021-12-03. Retrieved 2024-01-08.

[21] 反诈中心 site:chinadigitaltimes.net/chinese/ https://www.google.com/search?q=%E5%8F%8D%E8%AF%88%E4%B8%AD%E5%BF%83+site%3Achinadigitaltimes.net%2Fchinese%2F

[22] Three Tibetans arrested after Tibetan election, (Free Tibet, April 4, 2016), https://web.archive.org/web/20191029132437/http://freetibet.org/news-media/na/three-tibetans-arrested-after-tibetan-election

[23] Tibetan man imprisoned for sharing books on Tibet, (Tibet Watch, November 18, 2019), https://www.tibetwatch.org/news/2019/11/18/tibetan-man-imprisoned-for-sharing-books-on-wechat ; Three Tibetans arrested for sharing photos of an official event on WeChat group, (Tibet Watch, August 10, 2021), https://www.tibetwatch.org/news/2021/8/10/three-tibetans-arrested-for-sharing-photos-of-an-official-event-in-wechat-group ; Founder of Chat group released in critical health, (Tibet Watch, December 23, 2021), https://freetibet.org/latest/founder-of-chat-group-released-in-critical-health/ ; Two sisters detained after chat group messages, (Tibet Watch, December 5, 2023), https://freetibet.org/latest/two-sisters-detained-for-chat-group-messages/ , Retrieved 16 January 2024

[24] China continues to push "underworld forces" campaign in Tibet, (Tibet Watch, July 3, 2018), https://www.tibetwatch.org/news/2020/7/3/china-continues-to-push-underworld-forces-campaign-in-tibet, Retrieved 15 January 2014

[25] Tibetans blocked at Kalachakra on borders and on WeChat, (The Citizen Lab, January 10, 2017), https://

citizenlab.ca/2017/01/tibetans-blocked-from-kalachakra-at-borders-and-on-wechat/

26 In a voice message heard by Tibet Watch in December 2023, a Tibetan mother in Lhasa told her recently married son to tell his wife to stop contacting her because she had an image of the Dalai Lama on her WeChat profile. The mother referred to this as a photo of the Buddha, knowing her son and his wife would understand. The message followed a WeChat call the daughter-in-law made to her from India after which the latter found that except for her, everyone in their family chat group had disappeared. An eight-year-old Tibetan girl, now in exile, consistently used Lama, a general honorific title for spiritual leaders in Tibetan Buddhism, instead of other specific words Tibetans normally use for the Dalai Lama, such as Gyalwa Rinpche (རྒྱལ་བ་རིན་པོ་ཆེ།) and Gongsa Chok (གོང་ས་མཆོག). See interview here: https://www.tibetwatch.org/news/2023/10/12/a-photo-of-lama-hidden-in-a-box ;

27 Search operations conducted to find the source of Tenzin Nyima's news, (Tibet Watch, April 9, 2021), https://www.tibetwatch.org/news/2021/4/9/search-operations-conducted-to-find-the-source-of-tenzin-nyimas-news

28 Interviews with Tibetan cybersecurity experts in the Central Tibetan Administration, Dharamsala (September 2023)

29 (海南藏族自治州, Hainan Tibetan autonomous prefecture, Qinghai)

30 Surveillance and Censorship in Tibet, (Tibetan Centre for Human Rights and Democracy, September 2020), https://tb.tchrd.org/wp-content/uploads/2020/09/Tibet-surveillance-censorship-.pdf

31 祁连县 Qilian County

32 海北藏族自治州 Haibei Tibetan Autonomous Prefecture

33 ibid.

34 比如县 Biru County

35 Driru County: The New Hub of Tibetan Resistance, (Tibet Watch, April 2014), https://static1.squarespace.com/static/5c6d7c35b2cf790541327f25/t/5c922aa29140b7d5faf86d48/1553083047669/driru_county_thematic_report.pdf

36 Tibetans in Driru County arrested for speaking to Tibetans in exile, (Tibet Watch, 25 June 2021), https://www.tibetwatch.org/news/2021/6/25/tibetans-in-driru-county-arrested-for-speaking-to-tibetans-in-exile

37 (National anti -fraud) Driru County Public Security Bureau to further raise a new upsurge in the prevention of telecommunication and network related fraud publicity, Driru County Public Security Bureau WeChat

https://mp.weixin.qq.com/s/RE91yigHNCxCqvDhvuSGXw , 22 November 2021

38 '"Always adhere" to COVID-19 test, "Not lose" in the counter propaganda fight', Driru County Public Security Bureau, https://mp.weixin.qq.com/s/-neN-bo3hII8StpDFjTT_Q , 6 October 2022

39 'Forced to install phone app at security checkpoints' (Tibet Watch, September 6, 2023) https://www.tibetwatch.org/news/2023/9/6/forced-to-install-phone-app-at-security-checkpoints

40 Interview conducted on 22 December 2023

41 In dynamic analysis, the software is executed in a controlled environment (the sandbox) to observe its behaviour and interactions with the system in real-time. This contrasts with static analysis, where the software is not executed but instead analysed in its dormant state, focusing on examining its code structure, contents, and other characteristics without running the program

42 'Forced to install phone app at security checkpoints' (Tibet Watch, September 6, 2023) https://www.tibetwatch.org/news/2023/9/6/forced-to-install-phone-app-at-security-checkpoints

[43] Khalil, J. “Cellebrite: The mysterious phone-cracking company that insists it has nothing to hide”. (TechRadar). Archived from the original on 2021-07-31. Retrieved 2024-01-12

[44] Hvistendahl, M. CHINESE POLICE KEPT BUYING CELLEBRITE PHONE CRACKERS AFTER COMPANY SAID IT ENDED SALES (The Intercept, August 26 2021, 2:49 p.m.) Retrieved 2024-01-12

https://theintercept.com/2021/08/26/cellebrite-china-cellphone-hack/

[45] 西藏警官高等专科学校-网络攻防模拟实验室和电子物证取证实验室（三次）中标公告 (2023-05-17) https://m.xkzbw.com/detail_1/2500849.html (Tibet Police College - Network Attack and Defense Simulation Laboratory and Electronic Evidence Forensics Laboratory (Three Times) Winning Bid Announcement). Retrieved and archived: https://archive.is/GyMN0 2024-01-16

[46] https://www.meiyapico.com/mobile-forensics-system_p7.html Retrieved 2024-01-12

[47] Byler, D. “Within the Operational Enclosure: Surveillance and Subversion in Northwest China” First Edition of Issue 19 of Logic Magazine: Supa Dupa Skies (Move Slow and Heal Things), MAY 17, 2023. https://logicmag.io/supa-dupa-skies/within-the-operational-enclosure-surveillance-and-subversion-in-northwest/ Retrieved 2024-01-12

[48] https://en.wikipedia.org/wiki/Jingwang_Weishi A copy of the full security assessment of this app can be obtained by emailing OTF.

[49] Wang, M. China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App (Human Rights Watch. May 1, 2019) English version. Retrieved 2024-01-12 https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

[50] Schwarck, E., Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China (The China Journal 2018 80:, 1-23) https://www.journals.uchicago.edu/doi/abs/10.1086/697089

[51] Wang, M. Big Data Fuels Crackdown in Minority Region, (Human Rights Watch news release, February 26, 2018) https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region Retrieved 2024-01-12

[52] Zenz, A. and Leibold, J., “Chen Quanguo: The Strongman Behind Beijing’s Securitization Strategy in Tibet and Xinjiang,” China Brief, Vol.17 Issue 12, (The Jamestown Foundation) https://jamestown.org/program/chen-quanguo-the-strongman-behind-beijings-securitization-strategy-in-tibet-and-xinjiang/ Retrieved 2024-01-13

[53] 2020年西藏黑恶犯罪情报综合应用平台升级改造项目单一来源采购邀请公告 (“Announcement of Single Source Procurement Invitation for the 2020 Tibet Underworld Criminal Integrated Intelligence Application Platform Upgrade and Renovation Project”) http://wx.51zhengce.com/index.php?m=activity&a=view&id=301947 (Archived and retrieved 2024-01-13: https://archive.is/xrZLU) Editor’s note: a detailed 107 page system description document with the same title was attached to the original procurement notices and retrieved by another research team, who shared a copy with us. While this document is no longer available online we cite it a number of times in this bulletin and Turquoise Roof will therefore make it available to researchers upon request.

[54] Notice of the Tibet Autonomous Region Public Security Department on Reporting Leads on Crimes and Violations by Underworld Forces (西藏自治区公安厅关于举报黑恶势力违法犯罪线), TAR Public Security Bureau, February 7, 2018, see https://www.chinalawtranslate.com/en/notice-of-the-tibet-autonomous-region-public-security-department-on-reporting-leads-on-crimes-and-violations-by-underworld-forces/ Retrieved 2024-01-13

[55] “Illegal Organizations”: China’s Crackdown on Tibetan Social Groups (Human Rights Watch, July 30, 2018) https://www.hrw.org/report/2018/07/30/illegal-organizations/chinas-crackdown-tibetan-social-groups Retrieved 2024-01-13

[56] https://www.tibet3.com/news/zangqu/sch/2020-11-23/194060.html

[57] https://www.tibetwatch.org/news/2021/4/9/search-operations-conducted-to-find-the-source-of-tenzin-nyimas-news

[58] Measures for rewarding informants to eliminate pornography and illegal content (西藏自治区“扫黄打非”工作举报奖励办法), See

https://mp.weixin.qq.com/s/-6HnJIwbN8Y2QAW_4hV0dQ, 16 November 2023

[59] Middle Way Policy and All Related Documents, The Department of Information and International Relations, Central Tibetan Administration, https://tibet.net/wp-content/uploads/2012/06/MIDWAY-ENGLISH.pdf

[60] Measure for rewarding informants to eliminate pornography and illegal content (西藏自治区“扫黄打非”工作举报奖励办法), See

https://mp.weixin.qq.com/s/-6HnJIwbN8Y2QAW_4hV0dQ, 16 November 2023

[61] United Nations Convention against Transnational Organized Crime and the Protocols Thereto (Adopted by the UN General Assembly: 15 November 2000, by resolution 55/25) https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html Retrieved 2024-01-13

[62] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime https://eur-lex.europa.eu/eli/dec_framw/2008/841/oj Retrieved 2024-01-13

[63] Uprising in Tibet, (Tibet Watch, March-September 2008) https://www.tibetwatch.org/2008-protest-timeline Also ‘A Great Mountain Burned by Fire: China’s Crackdown in Tibet’, International Campaign for Tibet, 9 March 2009, https://savetibet.org/wp-content/uploads/2013/05/ICT_A_Great_Mountain_Burned_by_Fire.pdf

[64] Self Immolation Fact Sheet, International Campaign for Tibet, https://savetibet.org/tibetan-self-immolations/ Accessed 15 January 2014

[65] Ingram, R., How China abuses the Interpol Red Notice system to persecute Uyghurs (The China Project) Published April 27, 2023 https://thechinaproject.com/2023/04/27/how-china-abuses-the-interpol-red-notice-system-to-persecute-uyghurs/ Retrieved 2024-01-13

[66] Oracle 11.2 or above.

[67] ibid.

[68] ibid.

[69] KingbaseES is the suggested solution. 2020年西藏黑恶犯罪情报综合应用平台升级改造项目单一来源采购邀请公告 (“Announcement of Single Source Procurement Invitation for the 2020 Tibet Underworld Criminal Integrated Intelligence Application Platform Upgrade and Renovation Project”) [attachment]

[70] 2020年西藏黑恶犯罪情报综合应用平台升级改造项目单一来源采购邀请公告 (“Announcement of Single Source Procurement Invitation for the 2020 Tibet Underworld Criminal Integrated Intelligence Application Platform Upgrade and Renovation Project”) [attachment]

[71] For a detailed analysis of this term (“གཙོ་གནད་མི་སྣ།”) in the Tibetan context refer to the entry in: ‘Tibet: A Glossary of Repression’ (Human Rights Watch, June 19, 2017) https://www.hrw.org/video-photos/interactive/2017/06/20/tibet-glossary-repression Retrieved 2024-01-13

[72] ‘Trajectory’, and ‘trajectory information’ in PSB big data specifications, standards, and exposed systems typically refer to the physical movement patterns and historical locations of individuals. This data can be derived from various sources like GPS tracking, mobile phone location services, or surveillance camera footage. Analysing these trajectories and plotting them within PoliceGIS systems or other surveillance systems (see Screen 18 in HRW’s IJOP report), allows the PSB to monitor and understand (and increasingly, predict) individuals’ movement habits and routines - i.e. ‘patterns of life’ analysis, which is then used for policing purposes.

[73] 2020年西藏黑恶犯罪情报综合应用平台升级改造项目单一来源采购邀请公告 (“Announcement of Single Source Procurement Invitation for the 2020 Tibet Underworld Criminal Integrated Intelligence Application Platform Upgrade and Renovation Project”) [attachment]

[74] ibid.

[75] ibid.

[76] Essentially the PRC equivalent of the 999 emergency system in the UK - but only for police services (fire and ambulance services having their own dedicated phone numbers).

[77] 2020年西藏黑恶犯罪情报综合应用平台升级改造项目单一来源采购邀请公告 (“Announcement of Single Source Procurement Invitation for the 2020 Tibet Underworld Criminal Integrated Intelligence Application Platform Upgrade and Renovation Project”) [attachment]

[78] ibid.

[79] ibid.

[80] See https://gosherabgyatso.com/ for information on Go Sherab Gyatso’s family history and publications on religion, philosophy, politics and democracy

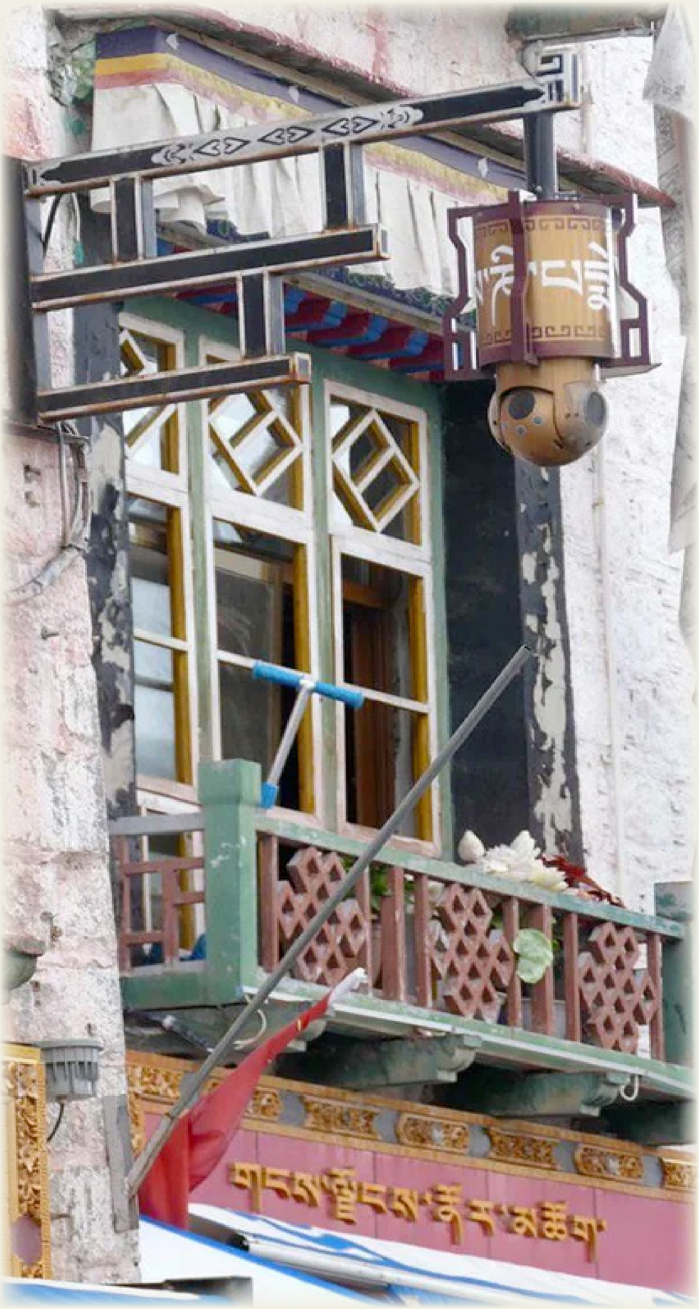
[81] Chinese government officially confirms the detention of two Tibetans, https://www.tibetwatch.org/news/2021/10/7/chinese-government-officially-confirms-the-detention-of-two-tibetans (Tibet Watch, October 7 2021)

[82] Release Tibetan scholar Go Sherab Gyatso from arbitrary detentio, (Tibetan Centre for Human Rights and Democracy April 16, 2021) https://tchrd.org/china-release-tibetan-scholar-go-sherab-gyatso-from-arbitrary-detention/

[83] In a letter from The Permanent Mission of the People’s Republic of China to the Office of the High Commissioner of Human Rights, it said: “On 26 October 2020, the Chinese State security organs placed Go Sherab Gyatso in criminal detention in accordance with the law on suspicion of inciting secession; on 3 February 2021, the Lhasa City People’s Procuratorate instituted a public prosecution proceeding against him…” See https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=36528

[84] Imprisoned Tibetan monk’s health in peril, (Human Rights Watch, February 9, 2022), https://www.hrw.org/news/2022/02/09/china-imprisoned-tibetan-monks-health-peril

> *"In the past, we can see Tibetans secretly talking about everything among themselves in tea stalls at Barkor Street but you cannot do so these days."*
>
> A Tibetan woman from Lhasa, in exile since 2023



Prayer wheels are found everywhere in the Tibetan Buddhist civilisation. A cylinder with wooden spokes, or metal bars with concave ends radiating from its base to be spun by hand, wind and water, prayer wheels contain a single sheet of paper with a single mantra repeating n times into a roll. The same mantra is engraved outside the cylinder case - mostly in Lantsa or Tibetan Uchen script. They are built as a solo giant wheel, or in rows around temples and monasteries. Tibetans spin it clockwise during their clockwise kora (circumambulation). An act of generating merit for this life and the next, and purifying unvirtuous karma of body, mind, and speech of oneself and for other beings.

This prayer wheel embedded with a surveillance camera is static, caged, and most possibly empty, despite showing Om Mani Padme Hum - the mantra of compassion of the Bodhisattva Avalokiteshvara, whom Tibetans believe came to this world in an incarnation as His Holiness the Dalai Lama. Barkor, literally meaning middle circumambulation, is a circumambulation path around the seventh-century Jokhang Temple which saw a series of demonstrations, mass arrests, and police shootings at sight in 2008 when protests against the Chinese government erupted across Tibet.

Surveillance camera in prayer wheel,

Barkor, Lhasa, 2017.

Source: Tibet Watch

TIBET WATCH
བོད་གནས་ལྟ་ཞིབ་
TURQUOISE ROOF