Witness Name: Conor Healy		
Witness category:	fact ☐	expert ☒
Date of testimony: 12 September 2021		
Link to recording*: https://www.youtube.com/watch?v=tFkr3pC1BmI&t=20235s		
Time stamp (start/end): 01:18:00 – 02:19:15		
Report included:	yes ☒	no ☐
Statement included:	yes ☐	no ☒
Transcript included:	yes ☒	no ☐
Presentation included:	yes ☒	no ☐

*Please note that all recordings of the Uyghur Tribunal hearings can be found on You Tube: Uyghur Tribunal - YouTube

IPVM

Uyghur Surveillance & Ethnicity Detection Analytics in China

Expert Report Presented to the Uyghur Tribunal

August 20, 2021

Author Information:
Conor Healy, chealy@ipvm.com
Government Director, IPVM
Bethlehem, PA, USA

Contents

About IPVM & Expert Background

IPVM is an independent, US-based research and media organization focused on surveillance technologies and businesses. The IPVM team publishes 3-4 reports each weekday on these topics, with particular emphasis on exposing unethical surveillance use by governments or corporations. We dedicate significant resources to covering China as the world's largest market for surveillance, and the home of the industry's most prominent companies. It is also the nation in which unethical surveillance use is arguably the most widespread, and large public projects over the last decade have significantly increased the scope and capabilities of China's national surveillance apparatus. IPVM has been following these developments for many years, particularly in Xinjiang, where advanced 'AI' surveillance technologies have been deployed specifically to target Uyghurs. Since 2018, we have published dozens of reports on these issues, with many garnering international coverage in publications such as the *New York Times*, *Washington Post*, *BBC*, and others.

As Government Director, I lead IPVM's efforts to research and communicate how surveillance technologies impact society, particularly in the context of government use. Since joining in May 2020, I have been directly involved in our investigations of surveillance technologies used on Uyghurs, and I have been responsible for communicating IPVM's

findings to the public. As such, I can offer the Tribunal insight into and answer questions about the technical capabilities of surveillance networks in Xinjiang, Uyghur face detection and its applications, and which corporate and government entities are involved in developing these technologies.

1. Overview of Uyghur Face Detection

The deployment of advanced analytic technologies ('AI', 'big data analysis') has been a signature element of China's massive state surveillance expansion. In general, these technologies empower surveillance cameras and other devices to automate, to an extent, the otherwise manual tasks of public security officials: collecting data on citizens' whereabouts, activities, associations, characteristics, etc. One such technology is Uyghur face detection (UFD), a system trained to determine if a person in an image or video is Uyghur on the basis of their facial features. In April, 2019, a New York Times investigative report found that China's authorities are "using a vast, secret system of advanced facial recognition technology to track and control the Uyghurs."[1] This facial recognition, the report said, "looks exclusively for Uyghurs based on their appearance and keeps records of their comings and goings for search and review," and it is "potentially ushering in a new era of automated racism."

Demographics classification systems such as those capable of detecting ethnicity are often marketed as extensions of face recognition products, but in fact these are distinct technologies. In terms of the development process, building ethnicity detection is not an extension of the technical work required to build a face recognition system, but a separate process and a significant investment. For UFD, manually-curated datasets containing thousands of Uyghur faces would be necessary, and creating such datasets likely involves thousands of hours of labor.

Several UFD systems have been created in China, and they are known to have been applied in many ways. Heart of City (HOC), a "smart city" software designed by Dahua Technologies integrated it into police operations systems, calling the functionality "real-time Uyghur warnings."[2] UFD has also been used in online content moderation, such as in Alibaba's "Cloud Shield" solution, which could automatically recognize Uyghur faces in online images or videos, and flag the content for review or removal.[3]

2. Uyghur Face Detection in PRC National Standards and Tenders

The proliferation of Uyghur face detection is an outcome of state policy, with UFD tacitly required in China's national standards for surveillance, and routinely specified in tenders for public surveillance projects.

In China, detailed standards are issued across all sectors of government which govern specifications in tenders for public projects and, in turn, the winning bidders for such projects. In December 2017, IPVM uncovered a draft of the Ministry of Public Security's standard for face recognition used in surveillance systems. The draft stated that "face attribute recognition" functionalities should include "Ethnicity recognition: (Uyghur/Non-Uyghur)."[4]

The draft was never published (which may, or may not, have been influenced by IPVM publishing the find). However, a similar national standard published the same year, GA/T1400.3—2017, requested face recognition systems detect "personal attributes" including "ethnicity" and "skin color," but did not specify which ethnicities should be detected. Several other national and provincial surveillance standards included the same or similar requirements, including GA/T 1756-2020, DB41/T 1514—2017, and DB4403/T 43—2020.[5] Notably, the latter is a Xinjiang provincial standard for police "technical database requirements" for "video and image" systems, which requested a statistical confidence score on a 0-100 scale

estimating whether someone belongs to a specific, unnamed ethnic group (or groups). To be sure, these standards officially list ethnicity detection features as "recommended". However, as noted by a supplier of the standards, "'Recommended' is not voluntary, it should be treated as 'mandatory'"[6].

In the standards, "ethnicity" is thought to be shorthand for "Uyghur." In addition to the draft standards uncovered in 2017, this is reinforced by the fact that Chinese authorities have explicitly requested UFD capabilities in tenders for public security camera networks. One example is a project to install "face recognition and analysis systems" in Yulin City, Guangxi, which required the systems to "support the facial attributes of the analyst's objectives (Uyghur, Han)." A similar project in Suqian City, Jiangsu, required face recognition to "Analyze the age, ethnicity, gender, whether you wear glasses, or Uyghurs" for "captured passerby pictures." Yet another project in Gangsu Province required "automatic labeling of captured faces or portrait images, including age, gender, ethnicity (Han and Uyghur)."[7] Even excluding projects in Xinjiang, tenders for PRC government surveillance projects which specifically require Uyghur face detection are commonplace.

3. PRC Corporations Offering Uyghur Face Detection

Several of China's technology companies have developed UFD systems. This section discusses them with the exceptions of Dahua and Hikvision which are addressed in their own, separate sections to account for a discussion of their broader involvement in Xinjiang.

3.1 Huawei

3.1.1 Huawei/Megvii "Uyghur Alarms"

Huawei is a well-known Chinese technology multinational, while Megvii is one of China's largest face recognition companies. A confidential Huawei report titled "Huawei Video Cloud Solution and Megvii Dynamic Face Recognition Interoperability Test Report" and dated January 8th, 2018, showed the two companies worked together to test and validate "Uyghur alarms". It was listed among the "basic functions of Megvii's facial recognition system" that Huawei "verified" could operate with Huawei technology, including a "Uyghur alarm" feature which was noted as having "passed" inspection (Figure 1). Despite being marked

Figure 1 - Huawei/Megvii Interoperability Report

confidential, the report was uncovered by IPVM via Google search and downloaded from Huawei's own website.[89]

3.1.2 Huawei Patent

In a July 2018 patent application, Huawei described a face recognition system capable of using surveillance to identify the race of passersby, and returning two possible results: Han or Uyghur. The patent application was submitted jointly with the Chinese Academy of Sciences, the PRC government's top research arm.[10]

3.2 Megvii Patent

6 of 22

In a June 2019 patent application, Megvii described a face recognition system with an "ethnicity classification" feature capable of analyzing if a person is "Han, Uyghur, non-Han, non-Uyghur, and unknown." The patent notes it "can also directly connect to the facial recognition that has been built by the public security organ."[11]

Several other Megvii patents mention "minority" or "ethnicity" detection, but without explicit mention of Uyghurs. These are searchable in any public patent database.

3.3 Alibaba

3.3.1 Alibaba Cloud Uyghur Content Moderation

Among Alibaba's divisions is Alibaba Cloud, China's largest cloud services provider. An Alibaba Cloud API guide, downloaded from the company's own website, lists "Is [the face] Uyghur?" as one of several 'face attributes' it can detect. The API guide mentions Uyghurs a second time, describing its ability to detect "Whether [the face] is a minority (Uyghur)", with the brackets specifying that "minority" is equivalent to "Uyghur."[12]

The API guide stated this technology was part of Alibaba's "Cloud Shield" solution. Alibaba describes Cloud Shield as "a pioneer in the field of Content Security," and states it "detects and recognizes text, pictures, videos, and voices containing pornography, politics, violent terrorism, advertisements, and spam, and provides verification, marking, custom configuration and other capabilities." Although most applications of Uyghur face detection are intended for video surveillance, this suggest's Alibaba intended it for internet content moderation. It is well-known that the PRC government strictly censors its internet, an effort increasingly driven by AI moderation and censorship solutions created by private firms. However, Alibaba's "minority" detection can be used for surveillance as well. Two other Alibaba API

guides for "sensitive video facial recognition" include a feature for detecting "whether [the face] is an ethnic minority."[13]

3.3.2 Alibaba Patent for Ethnicity Detection

In 2018, Alibaba was granted a patent filed in 2016 for an "image set generation method, device, and image recognition module." The patent lists "race" and "ethnicity" detection capabilities in illustrating a use case, "For example, if a company wants to use face recognition technology to check attendance, then each employee of the company can be regarded as a category, so that after classifying the image, you can identify which person it is. Of course, in other applications, categories can be divided according to race, ethnicity, or region." Uyghurs are not mentioned explicitly in the patent.[14]

3.4 Tiandy

Tiandy is one of China's largest surveillance companies, with 2019 sales of $620 million and branches in ~60 countries.

3.4.1 Tiandy Ethnicity Detection

A publicly available Tiandy SDK dated July 2020 has "race" analytics, with possible results as "yellow", "black", "white", and "the Uyghurs," and Tiandy's own website touts the ethnicity detection capabilities of their cameras.[15]

3.4.2 Tiandy "Smart Interrogation Table"

Tiandy also offers a 'one stop shop' police solution called the "Tiandy Law Enforcement and Case Handling Management Center" which includes a "Smart Interrogation Table" (Figure 2) that uses tiger chairs.[16]

Figure 2 - Tiandy Smart Interrogation Table

Human Rights Watch has reported that tiger chairs are used for torture by police, who "strap [detainees] into these metal chairs for hours and even days, depriving detainees of sleep, and immobilizing them until their legs and buttocks were swollen."[17]

3.4.3 Tiandy Xinjiang Presence

Tiandy has publicized selling and installing integrated police security solutions for numerous PRC police authorities and court systems. The company has a Xinjiang office in Urumqi that has promoted its work helping Xinjiang's "safety and stability maintenance" and projects in "safe cities, roads, hotels, courts, [and] mosques." Tiandy's Xinjiang office promoted an interrogation solution that has been they said is

being used by police and courts in Xinjiang, and in recent months, Tiandy has posted numerous job listings for police, military, and court-related staff in Xinjiang.[18]

3.5 Kingsoft API Guide

Kingsoft is a PRC cloud services provider worth ~$10 billion USD that went public on the NASDAQ stock exchange in May, 2020. An API guide downloaded from Kingsoft's website included "Uyghur, non-Uyghur" face detection claiming to detect with 48.7% confidence if a sample face is Uyghur.

3.6 SenseTime Patent

Sensetime is the PRC's largest face recognition/AI startup, with a reported $750m USD in 2019 sales. A patent filed in July 2019 describes the ability to classify individuals with "structured attribute tags such as age group and ethnicity…it can be divided according to Han, non-Han and unknown, or according to Han, Uyghur, non-Han, non-Uyghur, and unknown." The patent gives the example of using the system to search for "a middle-aged Uyghur man with sunglasses and a beard" by inputting those variables to find matching individuals.

3.7 Intellifusion Patent

Intellifusion is a PRC AI/face recognition startup which raised nearly $141 m USD in a pre-IPO funding round last year. An Intellifusion patent filed in 2018, for an "image retrieval method and device", described Uyghur face detection.

3.8 SensingTech Patent

SensingTech, another China face recognition/AI startup, filed a patent in 2019 for an "aggregation method of pedestrian [image] library based on face recognition" which picks out Uyghurs as one of "two categories".

3.9 Baidu Patent

Baidu is known as the 'Google of China'. In 2019, Baidu filed a patent which includes "ethnicity" in its "attribution recognition" AI model. The patent does not explicitly mention Uyghurs, or any other ethnicities in particular.

4. Hikvision

4.1 Hikvision Overview, Origins & Ownership

Hangzhou Hikvision Digital Technology Co. is the world's largest surveillance manufacturer, with greater than 40,000 employees, operations in 150+ countries, and 2020 revenue of RMB 63.5 Billion (~$10B USD).

Hikvision originated from the No. 52 Research Institute of the China Electronics Technology Group Corporation (CETC), a PRC state-owned entity. CETC remains Hikvision's controlling shareholder to this day through a wholly-owned subsidiary, CETHIK. The Director of the No. 52 Research Institute, Chen Zongnian, is a member of the National People's Congress; he is also Hikvision's Chairman.[19]

Hikvision has touted its "substantial fiscal subsidies", having received several billion USD in investment from the PRC government. The company's financial filings have stated that the PRC government could "exert significant influence over our business and other matters of significance to us."[20]

4.2 Hikvision in Xinjiang

Hikvision has a substantial presence in Xinjiang, where the government has contracted them to directly build and operate multiple large surveillance projects.

One contract is a $46M USD "Social Defense System" in Xinjiang's Moyu county. The project included surveillance cameras for both re-education centers and

mosques; specifically, it required "facial recognition cameras to be placed at the entrance of each of the 967 mosques in Moyu County." Mosques were also to be set up with video conference systems allowing sermons to be centrally delivered from a studio run by the Moyu County Ethnic Affairs Commission.[21]

Another is a $53 M USD contract in Xinjiang's Pishan County for a mass facial recognition system. Contract documents described the installation of a surveillance system for the Justice Bureau's "Transformation Through Education Center" or "司法局教育转化基地监控系统" in Chinese. This term is used by Chinese authorities to refer to Uyghur re-education camps. The project also included a mosque surveillance and video conferencing system.[22]

Hikvision has received several other contracts for surveillance in Xinjiang. It should be noted that these projects are 'Private-Public Partnerships' between Xinjiang authorities and Hikvision, meaning Hikvision constructs, finances, and operates the installations for several years with government support under the "DBFOT" or Design-Build-Finance-Operate-Transfer model. The Pishan County project, for example, expires in 2040 according to Hikvision's own financial disclosures. Despite evidence of direct operational involvement, Hikvision has claimed it has no control or knowledge of how its technology is used in Xinjiang.

On its China website, Hikvision published a map of its "R&D Centers" showing a location in Xinjiang. Job postings described it as the "Hikvision Xinjiang Research Institute", stating that staff would live and work at an "Armed Police Forces camp" in Urumqi located "500 meters behind the Fuqian Road Chinese Medicine Hospital." This location corresponded to a PAP camp visible in satellite imagery. The workers would be "mainly responsible for labeling image or video samples in an

office working environment with computers." Applicants were required to be of "Han nationality".[23]

Prior to discovering the job postings, IPVM researchers asked Hikvision about the map. It was promptly removed and the company stated, "Hikvision does not have a research institute in Xinjiang." Later, when asked about the job postings for the "Hikvision Xinjiang Research Institute", the company deleted the postings, stated they were intended "to service commercial enterprises and not work on government projects," and reiterated that the Hikvision Xinjiang Research Institute does not exist.[24]

The manual labelling of images/videos is a key part of training deep learning-based analytics, such as Uyghur face detection. But it is unclear which projects the job postings were meant to serve.

4.3 Hikvision Uyghur Detection Cameras

In 2018, Hikvision inadvertently showcased an "ethnic minority" detection feature in a demonstration at the AI Cloud World Summit. (Figure 3) The demonstration did not specify which ethnic minority was being detected.

Figure 3 - Hikvision Minority Detection at AI World Cloud Summit

In November, 2019, it was discovered that Hikvision developed software that would specifically identify ethnic Uyghurs, according to the product description of a "smart" camera on Hikvision's own China website.

Figure 4 - Hikvision Uyghur Face Detection Camera

4.5 CETC and the Integrated Joint Operations Platform

Hikvision's parent company CETC, which was created to supply technology to the People's Liberation Army[25], is reported to have been an architect of the Integrated Joint Operations Platform (IJOP), a system used by Xinjiang authorities to monitor Uyghurs.[26] According to Human Rights Watch, "The Program aggregates data about people - often without their knowledge - and flags those it deems potentially threatening to officials". IJOP takes data from multiple sources, with face recognition-enabled surveillance representing a critical part of the system. IJOP also uses surveillance in combination with "wifi sniffers", which collect the unique identifiers of networked devices (smartphones, etc.) in their vicinity, to associate devices to individuals captured by cameras. Although Hikvision is not known to

have worked directly with CETC to design IJOP, it should be noted that its surveillance devices form a critical component of the system.

5. Dahua

5.1 Dahua Overview, Origins, and Ownership

The Hangzhou-based Zhejiang Dahua Technology Co., Ltd. is the world's second-largest surveillance manufacturer. With 16,000 employees, Dahua's operations span more than 180 countries.

Although Dahua's operations are comparable in many ways with its crosstown rival Hikvision, the company's origins and ownership are private. Dahua's controlling shareholders are founder and Chairman, Fu Liquan, and his wife Chen Ailing. State-owned enterprises hold 13.3% of Dahua shares.[27]

5.2 Dahua Contracts in Xinjiang

With nearly $1 B USD in contracts, Dahua is the PRC's largest Xinjiang surveillance supplier on record.

Among these is a $686 M surveillance project in Xinjiang's Yarkant County. Dahua was contracted to build and operate, for a period of 9 years, a mass surveillance network, and multiple 'convenience police stations'. Construction of thousands of new police stations has been a signature move by Xinjiang's top official Chen Quanguo; Reuters has reported these can be found at "almost every corner" of major cities.[28] This project is notable for its massive size, an $807 USD expense for each of the 850,000 residents of Yarkant County.

In 2017, Dahua and local firm Leon Technology won a surveillance project for Xinjiang's Qiemo County worth $61 M. It included "a system that captures the features of wireless MAC addresses," technology also known as 'WiFi sniffers'. As

discussed in 4.5, WiFi sniffers combined with surveillance cameras are used to track Xinjiang residents in IJOP.

5.3 Dahua Xinjiang Industry Park

Dahua built a large-scale facility in Changji City, Xinjiang, the "Dahua Security Science and Technology Information Industry Park," which includes an R&D center, a manufacturing center, a logistics center, a management center, and a monitoring center. Local Changji media reported that the park will "support and meet the demand for various security technologies that are required for ensuring stability in Xinjiang" and "carry out customized research and development." Dahua's Chairman Fu Liquan was pictured attending the groundbreaking ceremony. During a separate visit to Xinjiang, Mr. Fu said "with the strong support of all parties in Xinjiang, Dahua has become one of the most important security products and solutions providers in the Xinjiang market."[29]

5.4 Dahua Uyghur Face Detection, "Real-time Uyghur Warnings"

A Dahua SDK shows the company has developed Uyghur face detection. The SDK listed "Ethnicity Recognition: (Uyghur/Non-Uyghur" under "Face Attribute Recognition" capabilities. This SDK was downloaded from Dahua's own website, but deleted after the Uyghur detection references were discovered. The same SDK also showed Dahua offered beard analysis.[30]

Dahua Technologies build UFD into Heart of City (HOC), a "smart city" software integrated into mass surveillance which Dahua describes as "tapping the potential of big data resources to build a new AI-driven 'Smart Policing' model, driving front-line teams to operate accurately, efficiently and intelligently." In a December 2019 company document, Dahua described this system as providing police with "Real-time Uyghur warnings". This means if a Dahua surveillance camera sees what it

believes is a Uyghur, HOC's functionality allows a report to be automatically sent to the police.[31]

Figure 5 - Dahua HOC "Real Time Uyghur Warnings"

A separate March 2020 Dahua document said that Heart of City supports "real time Uyghur warnings." The document mentions various subcategories of individuals that can be tracked by HOC, including "Uyghurs with hidden terrorist inclinations." It is unknown what the assessment criteria are for "hidden terrorist inclinations", but reports have stated that mundane characteristics such as having a full beard, owning knives, or going to mosques can land an individual in this category.

6. Publications

Listed below are publications produced by our team which are relevant to the Tribunal. All have been made available for public access via the included links, and PDF copies are available upon request.

Rollet, C. (2018, 23 April). *Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang*. IPVM. https://ipvm.com/reports/xinjiang-dahua-hikvision

Rollet, C. (2018, 16 July). *Hikvision Wins Chinese Government Forced Facial Recognition Project Across 967 Mosques*. https://ipvm.com/reports/hik-mosques

Rollet, C. (2018, October 2). *Evidence Of Hikvision's Involvement With Xinjiang IJOP And Re-Education Camps*. IPVM. https://ipvm.com/reports/hikvision-xinjiang

Rollet, C. (2018, 28 November). *Evidence of Dahua's Involvement In Xinjiang Surveillance*. IPVM. https://ipvm.com/reports/dahua-xinjiang

Rollet, C. (2018, 7 December). *Infinova's Xinjiang Business Examined*. IPVM. https://ipvm.com/reports/infinova-xinjiang

Rollet, C. (2019, 20 February). *Massive Leak Of Chinese VMS Provider Exposes Xinjiang Surveillance*. https://ipvm.com/reports/leak-xinjiang

IPVM Team. (2019, April 26). *"Automated Racism": Chinese Tech Companies Profiling Ethnic Minority*. IPVM. https://ipvm.com/reports/uighur-ethnic

Rollet, C. (2019, November 11). *Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up*. https://ipvm.com/reports/hikvision-uyghur

C. Rollet. (2019, November 25). *China Government Spreads Uyghur Analytics Across China*. https://ipvm.com/reports/ethnicity-analytics

IPVM Team. (2019, 2 December). *China Uyghur Analytic Projects Require Intel And NVIDIA, Intel Condemns, NVIDIA Silent*. https://ipvm.com/reports/uyghur-intel-nvidia

IPVM Team. (2020, 10 March). *Hikvision AI Training In Xinjiang Paramilitary Base, Now Denies*. https://ipvm.com/reports/hik-xj-pap

Rollet, C. (2020, 21 May). *Hikvision Chairman Targeted For Sanctions As Federal Watchdog Calls Out Hikvision "Serious Religious Freedom Violations"*. https://ipvm.com/reports/hikvision-uscirf

Rollet, C. (2020, 23 June). *Hikvision Admits Minority Recognition, Now Claims Canceled*. https://ipvm.com/reports/hikvision-cancels

IPVM Team. (2020, November 4). *Dahua Racist Uyghur Tracking Revealed*. https://ipvm.com/reports/dahua-uyghur

Rollet, C. (2020, November 16). *Uniview Racist Uyghur Recognition Revealed*. https://ipvm.com/reports/uniview-uyghur

Rol let, C. (2020, November 30). *Hikvision Growing Xinjiang Operations*. https://ipvm.com/reports/hik-xinjiang

IPVM Team. (2020, December 8). *Huawei / Megvii Uyghur Alarms*. https://ipvm.com/reports/huawei-megvii-uygur

IPVM Team. (2020, December 16). *Alibaba Uyghur Recognition As A Service*. https://ipvm.com/reports/alibaba-uyghur

IPVM Team. (2020, December 22). *Alibaba Admits Developing Racist Uyghur Recognition*. https://ipvm.com/reports/alibaba-admits

IPVM Team. (2021, January 12). *Patenting Uyghur Tracking - Huawei, Megvii, More*. https://ipvm.com/reports/patents-uyghur

IPVM Team. (2021, February 9). *Dahua Provides "Uyghur Warnings" To China Police*. https://ipvm.com/reports/dahua-uyghur-warning

IPVM Team. (2021, February 9). *Dahua Offers Race Recognition - "Black", "White", "Yellow"*. https://ipvm.com/reports/dahua-racial-recognition

Honovich, J. (2021, February 11). *Dahua Responds, Caught Lying*. https://ipvm.com/reports/dahua-ethnicity-detection

IPVM Team. (2021, March 30). *Dahua and Hikvision Co-Author Racial And Ethnic PRC Police Standards*. https://ipvm.com/reports/racial-ethnic-standards

IPVM Team. (2021, April 5). *Video Analytics Demographics Guide (Age, Clothing, Emotion, Gender, Race)*. https://ipvm.com/reports/analytics-demographics

Rollet, C. (2021, April 14). *Dahua Operates China Police Surveillance*. https://ipvm.com/reports/dahua-police

IPVM Team. (20921, June 8). *The Security Industry Association Expels Dahua*.

https://ipvm.com/reports/sia-dahua-expel

Rollet, C. (2021, June 9). *Hikvision Alleges "Targeted" "Simply Because We

Happen To Be Headquartered In China"*. https://ipvm.com/reports/simply-hq-china

Jamaspishvili, J. & Rollet, C. (2021, June 29). *Hikvision Did Not "Knowingly"

Commit Human Rights Abuses, Despite Clear Evidence*. https://ipvm.com/reports/
arent-hikvision

Rollet, C. (2021, July 19). *Tiandy PRC China Surveillance Giant - Tiger Chairs,

Uyghur Tracking And Party Loyalty*. https://ipvm.com/reports/tiandy-cpc

7. References

[1] Mozur, P. (2019, April 14). *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

[2] IPVM Team. (2021, February 9). *Dahua Provides "Uyghur Warnings" To China Police*. https://ipvm.com/reports/dahua-uyghur-warning

[3] IPVM Team. (2020, December 16). *Alibaba Uyghur Recognition As A Service*. https://ipvm.com/reports/alibaba-uyghur

[4] C. Rollet. (2019, November 25). *China Government Spreads Uyghur Analytics Across China.* https://ipvm.com/reports/ethnicity-analytics

[5] IPVM Team. (2021, March 30). *Dahua and Hikvision Co-Author Racial And Ethnic PRC Police Standards*. https://ipvm.com/reports/racial-ethnic-standards

[6] ibid.

[7] C. Rollet. (2019, November 25). *China Government Spreads Uyghur Analytics Across China.* https://ipvm.com/reports/ethnicity-analytics

[8] IPVM Team. (2020, December 8). *Huawei / Megvii Uyghur Alarms*. https://ipvm.com/reports/huawei-megvii-uygur

[9] [WaPo Uyghur Alarms]

[10] IPVM Team. (2021, January 12). *Patenting Uyghur Tracking - Huawei, Megvii, More*. https://ipvm.com/reports/patents-uyghur

[11] ibid.

[12] IPVM Team. (2020, December 16). *Alibaba Uyghur Recognition As A Service*. https://ipvm.com/reports/alibaba-uyghur

[13] ibid.

[14] [14] IPVM Team. (2021, January 12). *Patenting Uyghur Tracking - Huawei, Megvii, More*. https://ipvm.com/reports/patents-uyghur

[15] Rollet, C. (2021, July 19*). Tiandy PRC China Surveillance Giant - Tiger Chairs, Uyghur Tracking And Party Loyalty*. https://ipvm.com/reports/tiandy-cpc

[16] ibid.

[17] Human Rights Watch. (2015, May 15). *Tiger Chairs and Cell Bosses: Police Torture of Criminal Suspects in China*. https://www.hrw.org/report/2015/05/13/tiger-chairs-and-cell-bosses/police-torture-criminal-suspects-china

[18] ibid.

[19] IPVM Team. (2021, May 3). *Hikvision: Created And Controlled By China PRC Government. IPVM*. https://ipvm.com/reports/hikvision-prc

[20] IPVM Team. (2018, March 28). *Hikvision: PRC Government "Exert Significant Influence Over Our Business*. IPVM. https://ipvm.com/reports/hikvision-influence

[21] Rollet, C. (2018, 16 July). *Hikvision Wins Chinese Government Forced Facial Recognition Project Across 967 Mosques*. https://ipvm.com/reports/hik-mosques

[22] Rollet, C. (2018, October 2). *Evidence Of Hikvision's Involvement With Xinjiang IJOP And Re-Education Camps*. IPVM. https://ipvm.com/reports/hikvision-xinjiang

[23] IPVM Team. (2020, 10 March). *Hikvision AI Training In Xinjiang Paramilitary Base, Now Denies.* https://ipvm.com/reports/hik-xj-pap

[24] ibid.

[25] Luce, M. (2012, February 21). *A Model Company: CETC Celebrates 10 Years of Civil-Military Integration.* The Jamestown Foundation. https://jamestown.org/program/a-model-company-cetc-celebrates-10-years-of-civil-military-integration/

[26] Rollet, C. (2018, October 2). *Evidence Of Hikvision's Involvement With Xinjiang IJOP And Re-Education Camps*. IPVM. https://ipvm.com/reports/hikvision-xinjiang

[27] Rollet, C. (2021, March 29). *State-Owned China Mobile Acquires 10% of Dahua*. https://ipvm.com/reports/china-mobile-dahua

[28] Wen, P. (2017, March 30). *Terror threats transform China's Uighur heartland into security state*. https://www.reuters.com/article/us-china-xinjiang-security-insight/terror-threats-transform-chinas-uighur-heartland-into-security-state-idUSKBN1713AS

[29] Rollet, C. (2018, 28 November). *Evidence of Dahua's Involvement In Xinjiang Surveillance.* IPVM. https://ipvm.com/reports/dahua-xinjiang

[30] IPVM Team. (2020, November 4). *Dahua Racist Uyghur Tracking Revealed*. https://ipvm.com/reports/dahua-uyghur

[31] IPVM Team. (2021, February 9). *Dahua Provides "Uyghur Warnings" To China Police*. https://ipvm.com/reports/dahua-uyghur-warning

12th September 2021 (1:18:00 – 2:19:15)

1

Conor Healy

2

3

COUNSEL – The next witness works for IPVM, an independent US-based research

4

organization focused on surveillance technologies and businesses. This organization

5

has dedicated significant resources to covering China as the world' largest market for

6

surveillance of the industry's most prominent companies. In his report to the Tribunal

7

titled "Surveillance Detection: Analytics in China", the witness covers the technical

8

capabilities of surveillance networks in Xinjiang including Uyghur face detection and

9

its application as well as which government/corporate entities are involved in

10

developing these technologies. Mr. Healy the Tribunal has received and read your

11

report they have done so in detail, so I'll invite you now to make a short presentation

12

but in the interest of time please do not let it go over 10 minutes.

13

CONOR HEALY – OK, I'll do my best to keep the time and thank you for having me. I

14

want to offer some context for my testimony just at the outset. Since out founding as

15

an organization IPVM mission has been to hold surveillance creators and users

16

accountable and we publish reports on unethical activities on everywhere from

17

Colombia to California – the People's Republic of China's unethical use of surveillance

18

against Uyghurs has been utterly unequal and deeply troubling to us as technologies.

19

Since 2018 we have published a dozen of reports on these issues that taken together

20

show that Chinese companies have designed, implemented advanced surveillance

21

designed to specifically to target Uyghur Muslims. In my testimony today, I'll speak

22

about two issues addressed in my expert report: certain government initiatives

23

executed by two prominent technologies…

24

25 *[interruption] PANEL – A little slower perhaps?*

26 CN – Yeah of course, I'll try to slow down. And then, second, mass surveillance

27 systems used to identify ethnic Uyghurs on the basis of their faith and facial feature.

28 So, this is HIKVISION, world's largest surveillance manufacturers, roughly 20,000

29 employees, 2020 global revenue of 10 million dollars, it operates globally and the UK

30 it has a 40 % market share, it originated from the China Electronics Group operation,

31 a PRC state owned entity created to supply the People Liberation Army and

32 HIKVISION continues to be state owned according to the Rome financial findings.

33 They've established a significant presence in Xinjiang, since being awarded multiple

34 security projects in 2017 for its installations. These both include the installation of

35 mosque surveillance and supplying surveillance to Xinjiang re-education camps. Ill

36 briefly explore both of these in greater detail. In Pishan County, Xinjiang HIKVISION

37 received a contract for "Security Protection and Prevention Control System": it

38 included camera installations in mosques and 'education through transformation

39 centres', a term I understand refers the infamous Uyghur re-education camps. Another

40 contract was in Xinjiang's Moyu county, for a social defence system, it included

41 surveillance in re-education centres and mosques specifically it specified facial

42 recognition cameras would be placed at each of the 966 mosques in Moyu County. So

43 facial recognition systems such as those installed such as the ones in Moyu and

44 Pishan County allow authorities to catalogue the identities of those attending mosques

45 and could proactively monitor attendance and identities of people attending in real

46 time. HIKVISION claims it has no knowledge and control over how its technology is

47 used in the region. It's important to note that these projects go beyond simply selling

48 the cameras, they're private-public partnerships meaning HIKVISION does not only

49 constructs but operates the installation for several years as shown in both tenders and

50   HIKVISION's own financial findings: the Pishan County project, for example it includes

51   direction operation into 2040, while the Moyu county project runs through 2035.

52   Turning now to DAHUA, which is the second surveillance manufacture. I think I need

53   some water… my mouth is getting dry

54   [*interruption*] *PANEL – A little slower still, please.*

55   CN – So, DAHUA's contracts span more than 180 million dollars. They're comparable

56   to HIKVISION. The companies' origins are private, however their contracts in Xinjiang

57   total a billion US dollars. Again, two of these: is 685 million USD surveillance project

58   in Yarkant County. DAHUA was contracted to build and operate for a period of 9 years,

59   a mass surveillance network and construct convenient police stations for its residents.

60   You do the math that's 7 USD for each of the county's 850,000 residents– I should say

61   that a contract of this size is virtually unheard of in the security sector. There are no

62   countries that have projects of this size.

63   A second one in Qiemo County worth 61 million dollars includes a system that captures

64   the features of wireless MAC addresses so known as WiFi sniffers rather. According

65   to reports by Human Rights Watch these devices, Integrated… or IJAW used in

66   combination used to identify users of network devices. So China's mass surveillance

67   such as those that have been installed in Xinjiang but installed across the country

68   made use of advanced analytical technologies to automate the process of data on

69   citizens characteristics and more importantly their ethnic characteristics. Here [on the

70   screen] you see an ethnic minority was inadvertently positioned 2018 conference. The

71   company was later found to be marketing specifically described as detecting Uyghurs

72   and such systems are trained to assess a person or an image on the facial features

73   alone. That require a significant amount of machine learning and effort known to have

been applied in many different ways. Here you see a technical document, Hara city, a smart city software designed by DAHUA, smart police management. This means that DAHUA surveillance seems to be what it believes to be a Uyghur, smart city management. This means a warning would be sent to the police, a real time Uyghur warning. The document various subcategories of individuals, including Uyghur with "hidden terrorist inclinations" as well as detection. I should note that this is not a single or accidental mention of real time Uyghur warnings, the term 14 separate times, in this document as well as in other DAHUWA documents, cities functionality. It is not exclusively used in surveillance, Uyghur face detection was employed by ALIBABA in cloud shield… here you see a screenshot of their own documentation, showing the solutions capability to detect whether or not a person detected an image or video posted online. A Uyghur… that could automatically flag the content for removal. Another reiteration in a confidential HUAWEI report regarding in-cooperability with *Makebi*– one of China's largest facial recognition developers. It showed the two companies worked together to test a "Uyghur alarm" featuring a Uyghur face recognition product... Huawei also patented this technology July 2018 patent application HUAWEI described the facial recognition technology using surveillance to identify and returning to possible results, or Uyghur the patent application was submitted jointly, science, the PRC top research arm. Numerous other Chinese technologies have filed for similar Uyghur detection including MEGVII, ALIBABA have filed for patents for ethnicity detection without mentioning the specific ethnicity. Others are known to have developed technology but not patent it. Uniview–which you see up there (on screen)–is the third largest corporation other large surveillance manufacturers… logo is not up there but many of these companies have deflected these findings. Huawei for example said, "it's a test with no real world application".

99   Irrespective of the validity of that statement. It should be noted that building ethnicity

100   detection requires significant effort in investment. For a Uyghur facial detection system

101   manual data set containing thousands of Uyghur faces would be necessary and this

102   would require thousands of hours of work. The proliferation of these technologies said

103   to be an outcome of state policy. In detailed standards are issues all sectors of govt

104   including in surveillance which specify how bidders would win government tenders.

105   December 2019, we uncovered this draft document which was a standard for face

106   recognition systems. And its specifically included ethnicity detection and in bracket

107   said Uyghur slash non-Uyghur. That standard not officially published however similar

108   national provincial standards have been published since requisite facial recognition

109   system used to determine skin colour as you can see from the example here. They do

110   not specify from what… detection. As you can see there, these are standards that

111   have been published. The fact that Chinese authorities have specifically requested

112   Uyghur face recognition technologies and tenders in security networks. here you see

113   a map of regions issues tenders and request explicitly Uyghur face detection from an

114   analysis we've done November 2019 since then several other example requesting

115   Uyghur face detection that are more recent. This next slide is taken from a recent BBC

116   panorama documentary and shows the testing of a face recognition product by an

117   unnamed company and what are by all appearances Uyghur detainees. Frist it should

118   be noted that for developers validate the performance of facial recognition products

119   Uyghurs are likely to used as test subjects. Second, camera-based analytics, are

120   being used to conduct continually advanced analyses for public security officials. This

121   system shown here (on the screen) is an emotional detection system. Uyghur

122   detection face system. It's intended to analyse a subject an emotional state. I'm

123   zooming in here on red which represents negative ... measured by the camera. We do

124 doubt if such a product performs very well. You know we can Nevertheless continue

125 to explore face recognition system that play a key role in China's policies towards

126 Uyghurs. And with that I've gone over my 10 minutes and would love to answer any

127 questions you may have.

128 *COUNSEL –: Thank you. My first question relates to the Uyghur face detection*

129 *technology that you've spoken about, and you did mention, to develop such*

130 *technology distinct processes and quite a bit of investment. This is not just a natural*

131 *extension general detection technology. So, two questions: you did mention some*

132 *standards, official documentation, requiring a focus on Uyghur detection. If you could*

133 *speak about that. And related– given that this technology had to be purpose built.*

134 *What in your view is the purpose?*

135 CH – Yeah so video analytics technology are often grouped in face recognition when

136 we talk about them and that's also the case in China when China's national

137 specification of these policies. They are in fact … in terms of the technology and

138 process then as an add on you pull the ability to recognize an ethnicity or a gender for

139 that matter etc. which other things these systems are trained to detect, so it is a

140 process that'll require a significant amount of– work. unfortunately, we don't know what

141 exactly the development process of any of these is like in China. WE can only speak

142 generally to what we would expect from a such a development process. Having said,

143 I did mention this in my report. There is some evidence that individuals are being hired

144 in Urumqi– we don't know what but that's exactly the kind of work you'd expect. You'd

145 have people manually going through images maybe drawing boxes around faces.

146 Setting up a database, so that a machine you could learn from that database. So that

147 it is accurate. As for the purpose for what this technology is: you know I can again

148 really speculate here because China– the state has not explained what the purpose

149   of this technology is. But if you look at real time Uyghur warnings by Dahua for example

150   so that's a smart policing solution and it would appear what they are specifically trying

151   to detect are Uyghur that are not supposed to be in the particular locale we're in- in

152   other words "unsuspected" Uyghur. In other places, the technology seems to be a sort

153   of preventative measure if you will. I can only describe it as bigoted prevention

154   measure. A simple example, there are various surveillance analytics that you could

155   use to detect intruders as they enter a building. And you know that is relatively

156   common, or detect persons engaged in suspicious activity sort of grouped in

157   technologies that you would be grouped in system now. And so, Uyghur detection

158   considered a useful functionality in the same context that intruder detection might be.

159   *COUNSEL – Thanks for that and just for the real time Uyghur warnings that you*

160   *mentioned. That send reports to police when the system detects a Uyghur of concern*

161   *for instance, so the system is able to discriminate between for example Han Chinese*

162   *and Uyghurs and is able to hone in and single out Uyghurs–*

163   CH – Yes.

164   *COUNSEL – Just because they are essentially Uyghur and it then has the ability to if*

165   *there is anything of concern and as you mentioned, it could be a matter simply an*

166   *Uyghur being in an area they're not expected to be by the system. Right?*

167   CH – Yeah and *Hyber* city, the city with real time Uyghur warnings. Like said it's a

168   smart city management solution, what it implies is that the police in a given area where

169   the software is used, you know they would have an operation centre that has lots of

170   surveillance software. It implies that one of the incidents reports they would be

171   processing and have people looking over and addressing would be Uyghurs detected

172   on the street and they would evaluate whether that is something they would need to

173   do something about. So yeah, if you're Uyghur and walking down the street, and you

174   get captured by a camera, it's not unreasonable to expect that seconds later there are

175   police evaluating whether or not requires intervention.

176   *COUNSEL – And thank you, I just have two brief questions and pass it to the panel.*

177   *The first is that yesterday that an 'open air' prison was used to describe the area in*

178   *Xinjiang because of the high tech. What do you make of that description?*

179   CH – I'm sorry, could you repeat that?

180   *COUNSEL – So, in the view of this intrusive surveillance and focus singling out*

181   *Uyghurs, the term "open air prison" was used.*

182   CH – To describe the province?

183   *COUNSEL – Yes to describe the province, what would you make of that description?*

184   CH – IPVM has evaluated a lot of surveillance projects, in many regions which are

185   sold to governments and prison systems. There is no system available to most of the

186   world as advanced and intrusive as what is being deployed in Xinjiang and for that

187   reason I would agree. I don't think there are prisons in the UK or the US that have

188   surveillance technologies as extensive as that

189   *COUNSEL – Thank you for that, and my final question. Where do we go from here?*

190   *And how likely is it that is not just surveillance or monitoring or controlling people can*

191   *be taken even further. In your report you refer to the Xindi law enforcement*

192   *management centre which include as much interrogation– tiger chair essentially.*

193   *Could you speak to us a little about what that could be? And where is this technology,*

194   *where could this technology go- with respect to focusing on an ethnic minority*

195   CH - Yes I didn't include that in initially my testimony, simply for the reason that there

196   is no evidence that product was developed specifically to evaluate Uyghurs. Having

197   said that these advanced technologies, I think you can expect them to be used in the

198   context of detention, which is happening They have capabilities, that are hard for us

199   to conceptualize but I imagine that such technology will be used its hard to say what

200   exactly we'll expect in the next couple of years. They have capabilities that are kind to

201   conceptualize, they are advancing very quickly but you know this is an–even now– an

202   unprecedented ability to analyse the population and identify people's characteristics

203   in this way. I think it will continue to continue to surprise us.

204   *COUNSEL – Thank you, I'll pass you on to the panel.*

205   *PANEL – The witnesses referred to the tiger chair, we've heard a lot of reference to it.*

206   *Those of us reading the papers have seen drawings of it. I don't know if Mr. Healy is*

207   *in the position to throw up on the screen image of one. Of an actual tiger chair? Is it*

208   *available on your screen? Probably not.*

209   CT – It's not in my presentation, is my report– if someone busy in the back could…

210   *PANEL – Thank you for your statement, can you give us a sense of when this ethnicity*

211   *detection intensified in Xinjiang.*

212   CT – Well I've personally seen patent applications that go back as far as 2012, the

213   vast majority of them have been patented 2019 and 2020. Tenders requesting this

214   technology go back as far 2017 and continue essentially to the present day,

215   *PANEL – OK, you mentioned a draft to the minister of public security, which you had*

216   *access to. Are you able to tell us how you had access? And how did you verify that it*

217   *was the authentic article?*

218 CT – Yes, so I put up on the screen. I just put up on the screen what you're referring

219 to. It was available online– most of what I've presented to you is online. One of the

220 surprising things about our research, is that– is that a lot of this isn't hidden very well.

221 Speaking of methodologies, our methodologies is to acquire on– is to rely on

222 documents– the documents of the Department/Ministry of Public Security of various

223 public bureaus. You know– I don't think this is very interpretive. We are relying on what

224 the government itself in China has said it wants and what companies said they've built.

225 *PANEL – Have you got any comment with regards to how accurate these analogies*

226 *deem to be. For instance, in the West, we're aware of facial recognition, there are*

227 *reports that are coming out from US and Europe. That technology cannot detect White*

228 *& Black faces so in China have you come across anything to say that– you know– that*

229 *people believe that it is 100% accurate or perhaps 50% accurate.*

230 CH – Yes, a few things come to mind. So, there are government standards that have

231 specified a level of accuracy. That they want for this technology. I may have included

232 that in the report, if not, I'm happy to provide that. I don't remember each number they

233 specified, but it was certainly over 50%– they put this on a 0 to 100 scale basically.

234 And we haven't tested these products so we don't know how accurate they are but

235 China has the world's leading AI and facial recognition and just about all of them have

236 been involved in developing Uyghur detection. When I say all of them, I mean all of

237 the prominent ones in general.

238 *PANEL – In your research, are you able to make any connection between detection*

239 *and something that's actionable afterwards. Uyghur alarms can you make further links*

240 *between the data the detection and anything that happens afterwards. For instance,*

241 *incrimination or….*

242   CH – In terms of how the alarms, what they then signify?

243   *PANEL – So what happens after?*

244   *CH – Unfortunately not, we've … our focus on the technology. I think that that is an*

245   *area research. If it's possible to determine how this is being used.*

246   *PANEL – You write in your report that ethnicity is thought to be Uyghur for short, how*

247   *did you come to that conclusion?*

248   CH – A few different ways, so if you look at the standard up on the screen. What the

249   standard refers to as ethnicity recognition– Uyghur/Non-Uyghur. I think that has more

250   significance than it appears to cause there are dozens of ethnicities in China so that

251   is a pretty specific statement about what the interpretation. In addition to that, in terms

252   of the actual implementation. The standards that precede the implementation, so that

253   adds that additional context that helps us– sort of make a claim that identity ethnicity

254   detection means Uyghur detention– and beyond that there's a company called *Breese*,

255   they are a– I believe a subsidiary of UNIVIEW which I mentioned is the largest

256   company in China. They've said in their own guidance, ethnicity detection refers to

257   Uyghur detection. You know, there are ppl who deal with government projects fairly

258   frequently.

259   *PANEL – And the next claim you made, is of automated racism so that follows from*

260   *the statement you just made. Does that come across as correct?*

261   CH – Yeah

262   *PANEL – I will come back to the Tiger Chair. But first Huawei, everyone knows about*

263   *Huawei, there is a high-profile case around Huawei. They've been accused of this that*

264   *and the other, Huawei comes back and always denies these allegations. I'm not aware*

265 *of them being called racist but that probably comes in with the fact that accused with*

266 *colluding with the PRC– if they are denying those allegations, what have you come*

267 *across in your research?*

268 CH – well when we first reported on Huawei's– it was the Uyghur alarm functionality

269 you refer to, Huawei said it was just a test. It wasn't meant for real world applications.

270 Its suspicious on its own, as I've mentioned it requires a lot to build these technologies,

271 it's a bit unusual that they would build these technologies and kind of ditch it after a

272 test. And after that denial, that the company did not do this, we then found that they

273 patented it. I mean they had a patent for the technology– and at the same time were

274 downplaying this as some fringe activity– you talked about collusion with the Chinese

275 government, I don't think its matter of making accusations. It was co-authored by the

276 Chinese Academy, so it did occur they developed this with the Chinese government.

277 Then we can make allegations about what that means and how it was used. But its

278 factual.

279 *PANEL – OK thank you. So, this technology and various technologies, they don't just–*

280 *they're not just distributed in Xinjiang nor n China but also elsewhere where PRC is*

281 *engaged in trade, so we've heard about the digital silk route. We've heard about such*

282 *technology being sold cheaply and even gifted to other countries. Could this be the*

283 *way of PRC extending not only influence but also control. Second question related to*

284 *that, is it something that these governments could also be party to enjoy in terms have*

285 *having technology, in order to control and perhaps even oppress their own population.*

286 CH – Yeah, it's entirely possible and we're talking about that issue, we need to speak

287 more broadly than ethnicity detection. These are systems that provide all sorts of

288 different insights even without being able to detect race. There are various reports that

289 China's been exporting these technologies to other countries– I mean China is already

290 the largest exporter of sort of conventional surveillance technologies. When I think

291 about these technologies, the term "techno-authoritarianism" comes up. That is what

292 they conceptually could be used for. I didn't include in my presentation or expert report

293 but there's a tender for mass surveillance system in the city of Yangkaw that our team

294 has analysed dating from March 2020 and that tender describes the ability– it does by

295 the way request Uyghur detection. But separate from that, it describes the ability to

296 conduct predictive analytics on the population that It could then be used to prevent

297 social unrest. So, in other words, if realized, we're talking about a system that

298 anticipates protests before they occur– you know dissident is always innovative and

299 always finds a way to operate in a distance, but I don't know how dissidents could

300 operate in those conditions. If their own actions are understood by these technologies,

301 sort of better than any human could do. To extent of predicting whether or not they're

302 engaging in behaviour that the government disagrees with that is very scary,

303 *PANEL* – In your report you also talk about Alibaba, that is in terms of video

304 surveillance which we've heard about. We haven't heard about the internet content

305 moderation. Could you elaborate on this?

306 CH – Yeah sure, so, I mean it's well known that China sensors its internet extensively.

307 And a big part of how they do that and frankly how other companies like Facebook

308 that they don't want on their site- its automated. They use machine learning systems

309 to flag content that should be potentially removed. And that's what Alibaba's cloud

310 shield solution does. And they thought it was useful to build Uyghur detection into that

311 solution. From what I understand– or not from what I understand, there have been

312 reports of Uyghurs having difficult posting images and things online. It's the kind of

313 technology that could be behind that.

PANEL – So, in their patents, they actually use the word race and ethnicity, and the patent is rewarded to them afterwards.

CH – Alibaba?

PANEL – With Alibaba, yes

CH – Yes

PANEL – Some of these companies obviously operate globally. The EURO Football tournament– Alibaba was everywhere. So basically, these companies are quite- you've already used the word- unethical globally as well. Is this suggestion? Am I taking this too far?

CH – I think it is very reasonable to say that they've acted unethical ways globally. You know this gets off the subject of Uyghur but if you take the example DAHUA, the South Korean equivalent of the FCC recently revoked all of their authorizations because they falsified their test results. HIKVISION and DAHUA have both made 100s and millions of dollars selling fever detection equipment that does not work across the world – we've actually published a peer reviewed in the Journal of Biomedical Optics to prove this. They applied an algorithm, that essentially adjusted the results so appeared normal. They were basically faking it but spent millions of dollars on this stuff. In terms of unethical use of surveillance, I think most of that ends up being the end user. So it might be too far that these companies are going through the UK or the United States making decisions that then result in unethical uses– government authorities are the ones making those decisions. In terms of more unethical examples more generally us.

PANEL – So there are many ways we are deeply implicated. We're not just talking about Xinjiang but we're talking about Xinjiang. The entire global position in it. Would you agree?

338   CH – Yes.

339   *PANEL – I'd like to talk about the tiger chair but you haven't really elaborated on it.*

340   *Could you please talk about this before I ask you a questions about it?*

341   CH – Tiandy smart interrogation table. Surveillance manufacturers they too have

342   developed Uyghur detection. And this is one of their other products: it's a smart

343   interrogation solution. There isn't much I can say in terms of what analytics used in

344   combination with this solution. There have been reports– if you sort of go back. If you

345   look at the motion detection solution I showed you, I would consider it likely that in

346   general technology is not specifically motion detection integrated into this so called

347   smart interrogation solutions. And yes that is a tiger chair– which human rights has

348   reported that are those used for torture of detainees that they are left in this group for

349   hours and hours on end and that is what comes with this one-stop-shop police

350   management system.

351   *PANEL – Did you get this from the internet?*

352   CH – Yes.

353   *PANEL – Available in China even tough initially they denied the existence of such a*

354   *chair?*

355   CH – I don't specifically recall if Tiandy denied the existence.

356   *PANEL – The PRC are denying it?*

357   CH – We didn't get any comment from the PRC. I believe the PRC has denied that

358   they've tortured detainees in general

359   *PANEL – But they've accepted the fact that they have a chair?*

360   CH – I'm not sure.

361   *PANEL – And is it in only in China? Is it also being distributed globally?*

362   CH – Well I think its only in China that Tiandy is selling it, if you're asking? But I think

363   Tiger chairs have a longer history. It would probably be in many places.

364   *PANEL – And my last question relates to the people's liberation army that HIKVISION*

365   *were supplying technology to the PLA and that this was transferred to the IJOP, the*

366   *integrated joint operations platform. Have you come across this technology by PLA by*

367   *any other way? What I'm trying to understand, how the civil and military are blurred–*

368   *how these areas come together?*

369   CH – I think HIKVISION's relationship with the People's Liberation Army is interesting

370   to discuss. We did a collaboration with the Wallstreet journal in which we've published

371   extensive evidence, of their work with the People's Liberation Army. There was a study

372   that one of their employees collaborated with the PLA on their, forced to improve their

373   lethality of their service to missiles to artillery using HIKVISION's technology. There

374   were listed as a Tier 1 supplier. They were at the highest possible level to the People's

375   liberation army. By the way–about the study, the one improving the lethality of missiles.

376   That was on HIKVISION's own website. That is where we found that study and the

377   researcher listed as a HIKVISION research. Their response to that was: "we had

378   nothing to do with this, and this employee was only acting in his personal capacity,

379   and so the counterpoint I suppose is that HIKVISION employees are working in their

380   capacity collaborate with the PLA in terms of missile technology.

381   *PANEL – I'm going to interrupt before we pass it on, for those who may not be familiar,*

382   *the tiger chair loops at the bottom which we can see, so the feet are immobilized but*

383   *what is not quite visible also is that there are restraints on the top so that your wrists*

384 *are immobilized and your ankles are immobilized and if it is torture. You're left there*

385 *for as long as it suits them- is that right?*

386 CH - Yes, that is how I understood it.

387 *PANEL – we have heard in some of the evidence of tiger chairs that the loops could*

388 *be tightened electrically. Are you aware of it?*

389 CH – I actually am not aware of that.

390 *PANEL – Could you tell us how advanced actual masked facial recognition are as*

391 *opposed to ethnicity detection?*

392 CH – Facial recognition systems in general are technology that sort of works in most

393 places. There have been some issues in placed like the US. With them not working

394 for every demographic equally, I think the facial recognition systems worked just fine

395 for their explicit purpose which is to identify people.

396 *PANEL – So what I am coming to is that it only works if you have a data bank to identify*

397 *from. What I was wondering was, what proportion of Uyghurs are on those databases*

398 *compared to Han people living in that region.*

399 CH – Interesting question. I think almost everyone in the region would have be in those

400 databases. There have been reports faces profiled, DNA taken and sort have had

401 finger prints– I think sort of done for the whole population. I think that in most of China

402 face recognition would probably recognize most people. I would note its actually not

403 the case you need the database for face recognition to work. You can still capture a

404 face profile you just wouldn't have an identity or a name. and you can sell get a lot of

405 data on people's movement and you could track an suspect/unknown person.

406   *PANEL – When you say the whole population, do you mean the Uyghur population or*

407   *the whole population of Xinjiang. What were you suggesting?*

408   CH – Certainly, the whole population of Uyghurs and Xinjiang. I think that the whole

409   population of the province. I wanted to clarify that I haven't seen any specific data on

410   exactly how well developed the database is. The data we do have is that China as a

411   a practice from relevant citizens to that could be used– that implies that most people

412   can be identified by– uncertainty as to exactly extensive their data is.

413   *PANEL – Who are the major funders of IPVM?*

414   CH – Subscribers! Basically, we're sort of like any other media organization. 90% of

415   our revenue comes from subscriptions and the other 10% comes from courses-

416   basically we teach people course son how to install surveillance. We do not have any

417   government funders or dubious financial ties. We certainly not being funded by the US

418   government except by the extent that an individual you know might buy a subscription.

419   *PANEL – Nor Apple, nor Microsoft– I take it?*

420   CH – Certainly not. Whoever buys Apple surveillance maybe they have subscription

421   *PANEL – Thank you very much. It is rather horrifying and rather interesting. Just going*

422   *back to the Tiger chair, how do you think this could help torture somebody? I mean*

423   *what are the parameters you might be taking from that big machine that we can see*

424   *there?*

425   CH – The chair itself or the machine?

426   *PANEL – Well the two are linked, aren't they? I'm just wondering what the machine*

427   *might be doing with the chair*

428 CH – I'm just thinking back to the report. I think we do go into some detail on exactly

429 what the solution offers and to the best of my recollection– to an extent its case

430 management– you know keep track, perhaps how long someone's being interrogated.

431 If they're using, analytics to evaluate somebody with the emotional state of the

432 detainee. But I wasn't totally expecting to talk about it so I'll have to refresh my mind

433 on all the details.

434 *PANEL – Fair enough. Obviously, these techniques will go on and on and develop. Do*

435 *you think they might be able to actually detect your DNA?*

436 CH – using a camera?

437 *PANEL – Yeah can't see how at this stage.*

438 CH – I don't see how.

439 *PANEL – One last question, maybe this is a bit facetious, how could one use this*

440 *technology in a good way? Here it's kind of to track the Uyghurs. Something we could*

441 *use the same technology for in hopefully better circumstances.*

442 CH – I think for the Uyghur face detection. I've spent some time thinking about this: I

443 cannot think of a single application of this technology that has a positive outcome for

444 anyone. If someone can, I'm happy to hear it. But realistically, this targets a particular

445 race and surveillance is used to monitor people- so it implies its for monitoring a race

446 in particular. I see nothing positive about that- there are no positive use cases and to

447 be honest this is a technology that shouldn't have been developed. And it's a shame

448 that it exists.

449 *PANEL – Thank you. In terms of these companies, to what extent would you describe*

450 *them as independent companies or actually government owned in a sense a level of*

451 *requisition, tendering that is going on. Are they China?*

452 CH – So many of these companies, they co-wrote the experience they are talking

453 about the ones that request HIKVISION or DAHUA- I'm certain they were co-authors

454 on at least 2 examples. And there are other Chinese countries that have been co-

455 authors so that partially answers the question. Also, by their own statements. They are

456 not independent from the government. HIKVISION says it's a state-owned company.

457 So, I think that is a pretty clear cut case. Their chairman, Chen Zongnian, holds the

458 role of being director of the research group and CCTC simultaneously. DHUWA,

459 they're only 13% government owned– they claim to be independent while at the same

460 time holding groups for their party ideology and making clear statements that you

461 always follow the party. And of course, working on all these projects in Xinjiang which

462 implies a certain level of dedication to the state goals.

463 *PANEL – In terms of the motion state, you referred to– I think you suggested implied*

464 *they are underdeveloped/inaccurate but do you foresee they are developed to a high*

465 *degree of accuracy following on Professor Kumar's question. How might you envision*

466 *it being used other than this example monitoring people who are being tortured for*

467 *example?*

468 CH – So most people that analyse surveillance technology are doubtful, a motion

469 recognition will ever be as accurate as you and I talking right now. But even then, this

470 interaction is a bit subjective, its hard to pin down the specific emotion of any particular

471 face greater than a particular accuracy. And to develop – adds a layer of complexity,

472 that being said I would caution people, the fact that they don't work actually makes this

473   worse, it's not whether they work but whether or not they're being used. And the

474   context of their use, seems to be evaluating their emotional states- and when I say

475   emotional states, I'm also referring to tendencies- aggressiveness, violence things that

476   could factor in on someone is treated. And if its inaccurate its probably worse.

477   *PANEL – Thank you. Can I just ask a little about government participation? Does the*

478   *Chinese government fund research into ethnic recognition technology? Or is it funded*

479   *through the companies getting these contracts.*

480   CH – I honestly am not sure. I can tell you they fund mass surveillance projects in

481   Xinjiang, they purchase the technology so they're buying it as per who's funding the

482   research, you could argue HIKVISION being a state-controlled company, they involved

483   Uyghur based detection. So, at a minimum the government has funded this through

484   their statement entities.

485   *PANEL – Do you know what entities the contracting parties are?*

486   CH – It varies widely but it's the security bureau, or police entities

487   *Panel, TC – National or provincial?*

488   CH – It is typically provincial from local authorities.

489   *PANEL – Is it part of the specification, sorry this will reveal my lack of technological*

490   *education. That they link into the job specification*

491   CH – Not exactly, it is part of the specification that they link into the government

492   surveillance networks. That is very normal to see, they want these unified systems

493   that many different security levels can access. But the tender notes specifically

494   mention the Integrated Joint Operation system. I can't definitely say that is what they

495   are referring to.

496 *PANEL – And last question for which I win the prize of naivety. Is there recourse under*

497 *Chinese law, regulation in relation to the use of stored information about them*

498 CH – If I'm not mistaken, discrimination is illegal on the basis of race or officially

499 speaking. The government has a position on that– I could be wrong.

500 *PANEL – But no wright of access to your information.*

501 CH – Not as far as I know. Including in practice. There is no right of access.

502 *PANEL – Just a couple of questions if I've got time. How should we imagine this*

503 *technology being used, standard on massive screens or is it much more sophisticated*

504 *than that. The machinery allows someone sitting in a local police state to be alerted to*

505 *a specific interest how does it work.*

506 CH – I think it would be both- this gets into a bit of speculation. Because we haven't

507 seen inside centres, or operation centres that would use these technologies. But I

508 believe you would be both.

509 *PANEL – With this number of cameras, you would need an army of people looking at*

510 *huge set of screens– or not?*

511 CH – Not necessarily a sort of mundane analogy. Let's take traffic cameras, traffic

512 camera up until recently would have required. If you wanted to watch traffic or look for

513 a particular car– you would need someone looking at the screens. I think this

514 demonstrates the software these days, rather than the hardware in terms of what the

515 system can really do or what it's for. Widely available technology, you have then

516 transformed that system where everyone is going- direction of travel the amount of

517 traffic, you can use to track people down, all sorts of analytic to traffic people and all

518 you've done, something that was done technology beforehand.

519   *PANEL – And you don't always need, it alerts different systems automatically*

520   CH – The system would create an alert based on whatever parameters they've set.

521   So I mean it eventually goes to someone, so you could filter through instances that

522   would be manually looked at by a person

523   *PANEL – Just to conclude, I could buy a tiger chair from Tiandy- nobody would object.*

524   CH – Yeah… I mean if you were a public security official, I would assume so.

525   *PANEL – Thank you very much indeed Mr Conor for coming to help us.*

526   CH – Thank you for having me.

IPVM

Surveillance and Uyghur Ethnicity Analytics in Xinjiang

Conor Healy - Government Director, IPVM - chealy@ipvm.com

Tuesday, 12 September 2021 - Uyghur Tribunal

HIKVISION
Public Projects in Xinjiang

Name	Year	Amount (Million USD)	Winner
Urumqi Hi-Tech Zone Safe City	2017	79	HIKVISION
Yutian County Safe City	2017	58	HIKVISION
Lop County Social Security	2017	57	HIKVISION
Pishan County Facial Recognition Systems	2017	53	HIKVISION
Karakax County Social Defence Systems	2017	46	HIKVISION
Moyu County Social Defense System	2017	46	HIKVISION
	TOTAL	$339 Million	

*HIK*VISION
Public Projects in Xinjiang

Pishan County, Xinjiang - "Security Protection and Prevention Control System"

- "Justice Bureau's Education through Transformation Center monitoring system"

- Mosque surveillance and video conferencing systems.

- Hikvision to operate through 2040.

Moyu County, Xinjiang - "Social Defense System"

- "967 facial recognition cameras to be placed at the entrance of each of the 967 mosques in Moyu County."

- Cameras for use in re-education centers.

- Hikvision to operate through 2035

Publicly Reported Projects in Xinjiang

Name	Year	Amount (Million USD)	Winner
Safe County in Yarkant County	2017	686	dahua
Shihezi Safe City	2016	94	dahua
Qiemo Safe County	2017	61	dahua + 立昂技术 Leon Technology
Hotan County Public Security Checkpoint	2017	40	dahua
Qira County Smart City	2016	30	dahua
Yopurga County Safe City	2017	30	dahua
TOTAL		**~$ 941 Million**	

Yarkant "Safe County" Project

- Build and operate mass surveillance network for 9 years.

- Construction of "convenience police stations."

- Notable for its massive $685 M USD size. $807 USD expense for each of the 850,000 residents of Yarkant County

Qiemo "Safe County" Project

- "a system that capture the features of wireless MAC [media access control] addresses via a mobile [movable] terminal", i.e. 'WiFi sniffers'
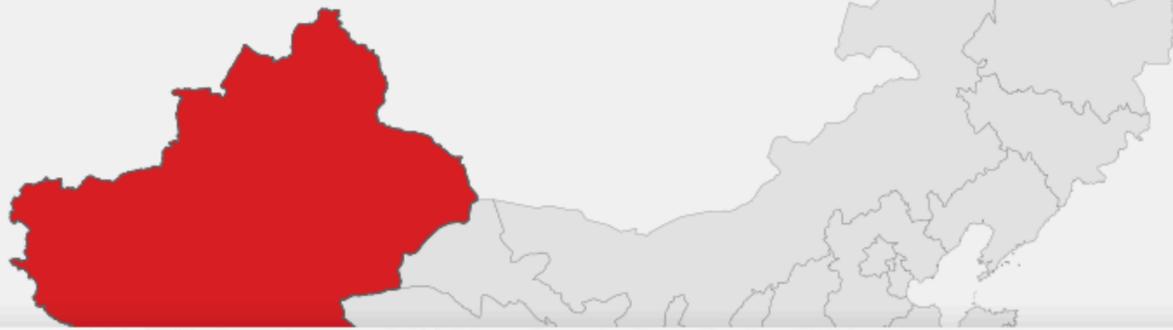
少数民族
Ethnic Minority

这套系统同时可以对特定游客进行定位
This system can also track specific visitors to monitor

https://supportkb.dahuatech.com/kbaseui-std/main.do

维吾 14/16

alhua

公告

Business Contact Person
业务联系人：谢凯伦 | 695602

IT Contact Person
IT部联系人：祝熔敬 | 657277

案例提交　　个人

产品支持中心

Solution Support Center
解决方案支持中心

Case Center
案例中心

Service Solution
服务方案

Training Certification
培训认证

📋 产品支持中心 ★
Product Support Center

▶ HDCVI产品
▶ 摄像机
▶ 存储
▶ 传输产品
▶ 显示产品
▶ 系统产品
▶ 软件平台
▶ 楼宇产品
▶ 智能交通
▶ 云计算
▶ 智能分析服务器
▶ 智慧消防产品
▶ 配件线
▶ RFID
▶ 百宝箱

首页　　搜索结果 ✕

📄 HOC智慧警务V1.1软

下 载
Download

维族人员实时预警
Real-time Uyghur Warnings

布控值守

人像大数据
Portrait Big Data

同行人分析，频繁出现

1.客户端，人脸识别-技战法查询-同行人，添加图片能够返回相应的同行人结果
2.客户端，人脸识别-技战法查询-频次查询，根据出现次数返回相应的结果

时空碰撞

1.客户端，人脸识别-技战法查询-时空碰撞，配置碰撞条件点击查询，返回正确结果

人脸技战法
Facial Technology Strategy

维族人员实时预警
Real-time Uyghur Warnings

1.web操作端，人脸系统-研判分析，配置维族人员模型
2.客户端，人脸识别-数据模型-模型查询，选择维族人员模型，查询到对应数据
3.前提需要前端支持上报维族属性

首次出现、落脚点分析、人员查重

定制支持

人脸红名单

红名单中的人脸在不能用以图搜图中被检索到（相似度支持自定义）

1.web操作端，人脸系统-人员管理，新增红名单库，添加红名单人员
2.客户端，人脸识别-抓拍检索-身份核查-同行人查询-一脸一档，非system用户进行添加红名单库中人员进行以图搜图，提示无权限查询

一脸一档

对相似或同一路人照片进行归类

1.web操作端，人脸系统-人脸设备，开启通道聚类分析
2.客户端，人脸识别-一脸一档，查询到对应人员档案信息，包含同一人的抓拍记录

56

Table 14. task.extras

name	Types of	Is it necessary	description
faceAttrs	String[]	no	Type of face attribute to be extracted, value: • `gender` : gender • `age` : age • `glasses` : glasses inspection • `facetype` : face detection • `smiling` : smile detection • `blur` : the degree of `blur` • `ethnic` : Is it Asian? • `weizu` : Is it Uighur • `binary` : whether it is a binary image • `standardFace` : Whether it is a standard face
minority	Boolean	no	Whether it is a minority (Uighur).

![Huawei logo] 华为视频云解决方案与旷视动态人脸识别系统互通测试报告 ![Face++ 旷视 logo]

		支持离线文件人脸抓拍功能	Passed
		支持离线文件设置告警阈值，告警底库	Passed
		支持离线文件抓拍/告警记录导出功能	Passed
		支持离线文件维族告警 ← **"Uyghur Alarm"**	Passed
		支持调整离线文件识别参数设置功能	Passed
		支持查看离线文件内播放浏览及告警视频回放功能	Passed

58

[0087] 其中，L为设定的值。对象的属性为具有语义的特征，例如，目标对象为行人，目标对象的属性可以是性别（男、女）、年龄（比如青少年、中年、老年）、种族（汉族，维族）、身材（胖，瘦，标准）、上衣款式（短袖，长袖）、上衣颜色（黑，红，蓝，绿，白，黄）等。

[For example, the target object is a pedestrian. The attributes of the target object can be gender (male, female), age (such as teenagers, middle-aged, old), **race (Han, Uighur)**…]

59

公安视频监控人像/人脸识别应用技术要求

Technical requirements for human body/face recognition application in video
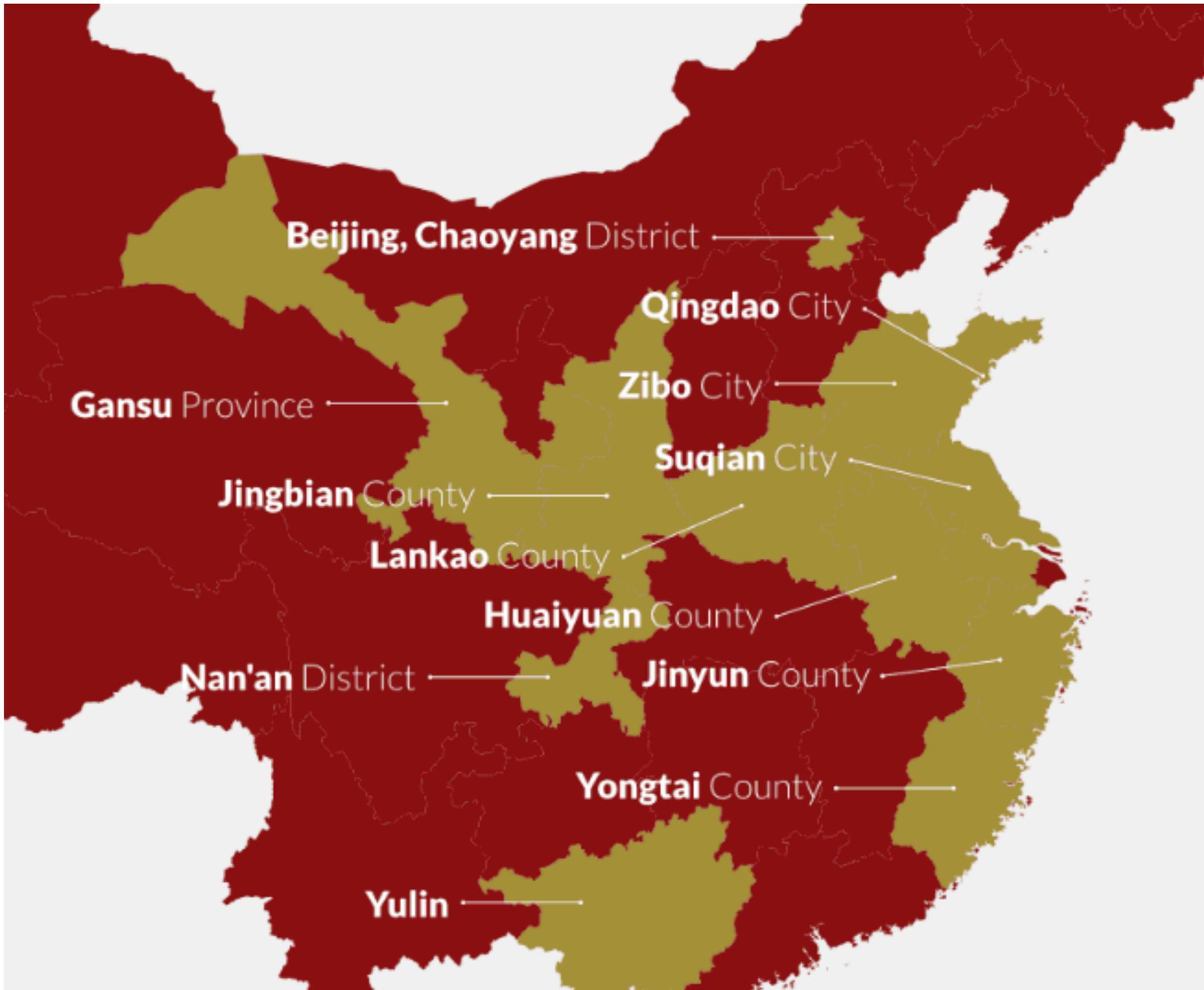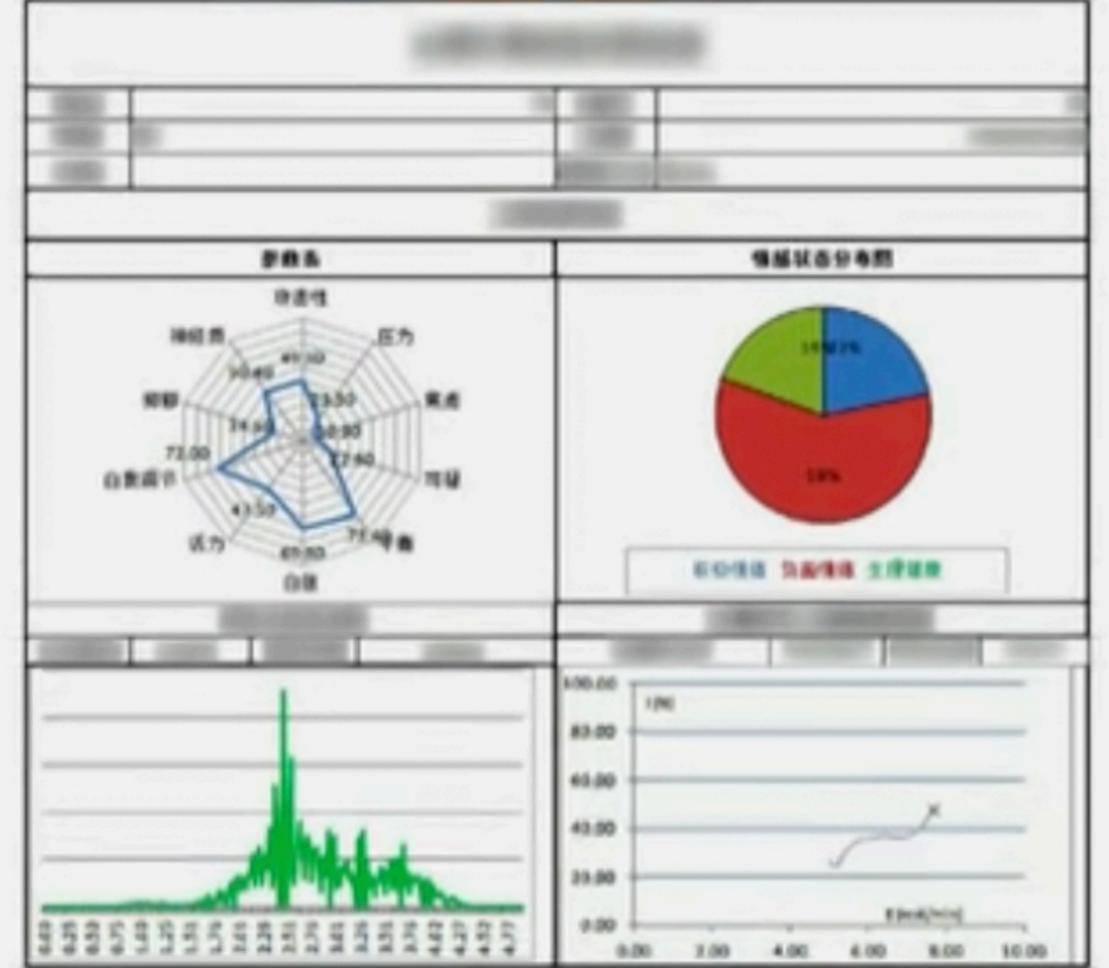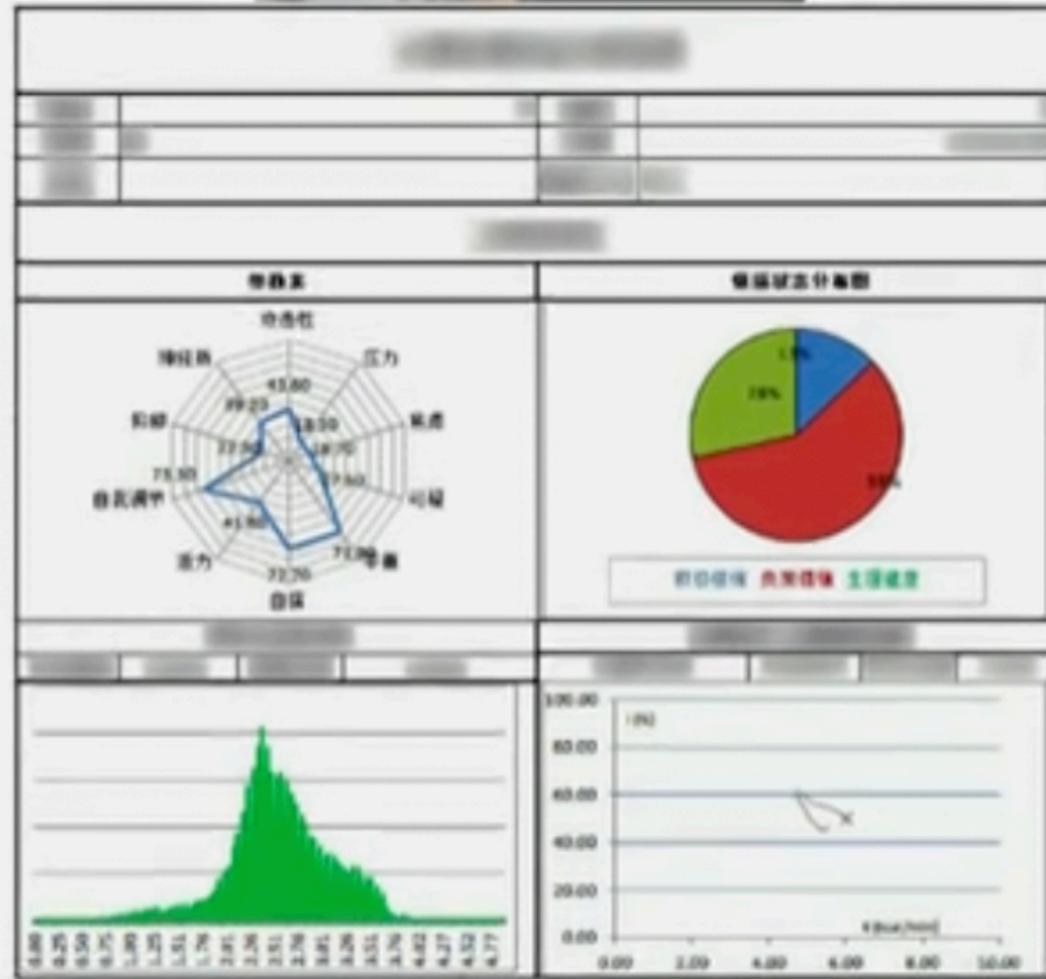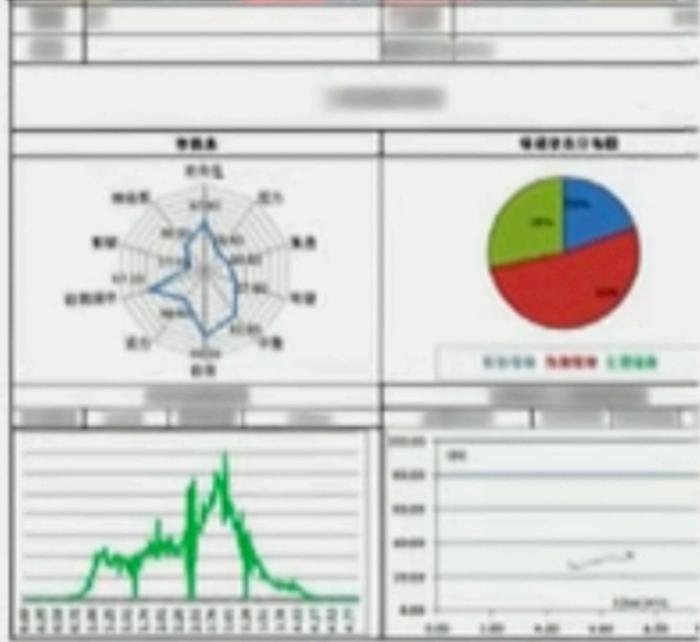
surveillance of public security

（征求意见稿）

2017-12-28

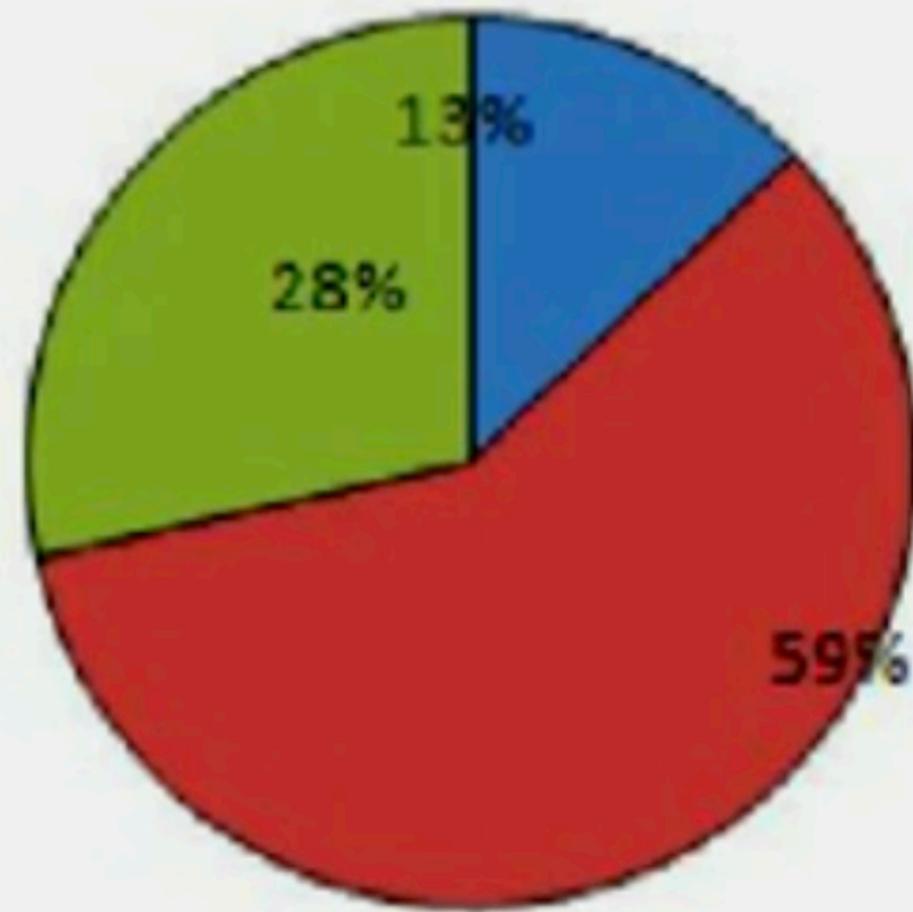| 人脸属性识别 Face Attribute Recognition	性别识别（男/女）Gender Identification (Male/Female)
	年龄识别（未成年/成年/老年）Age rec (minor/adult/old)
	民族识别（维族/非维族）**Ethnicity recognition: (Uyghur/ Non-Uyghur)**
	戴眼镜识别：（佩戴/未佩戴）Wearing glasses: (wearing/not wearing)

7.4.1　属性分析功能　**Face attributes**

人脸属性分析满足以下要求：**Face analysis satisfies the following requirements:**

a)　应支持性别分析；　**(gender)**

b)　应支持年龄段分析；　**(age group)**

c)　宜支持佩戴的附属物分析；**(wearable accessories)**

d)　宜支持是否有胡须分析；**(beard)**

e)　宜支持肤色分析。**should support skin color analysis**

Beijing, Chaoyang District

Qingdao City

Zibo City

Gansu Province

Suqian City

Jingbian County

Lankao County

Huaiyuan County

Nan'an District

Jinyun County

Yongtai County

Yulin

情感状态分布图

积极情绪　负面情绪　生理健康