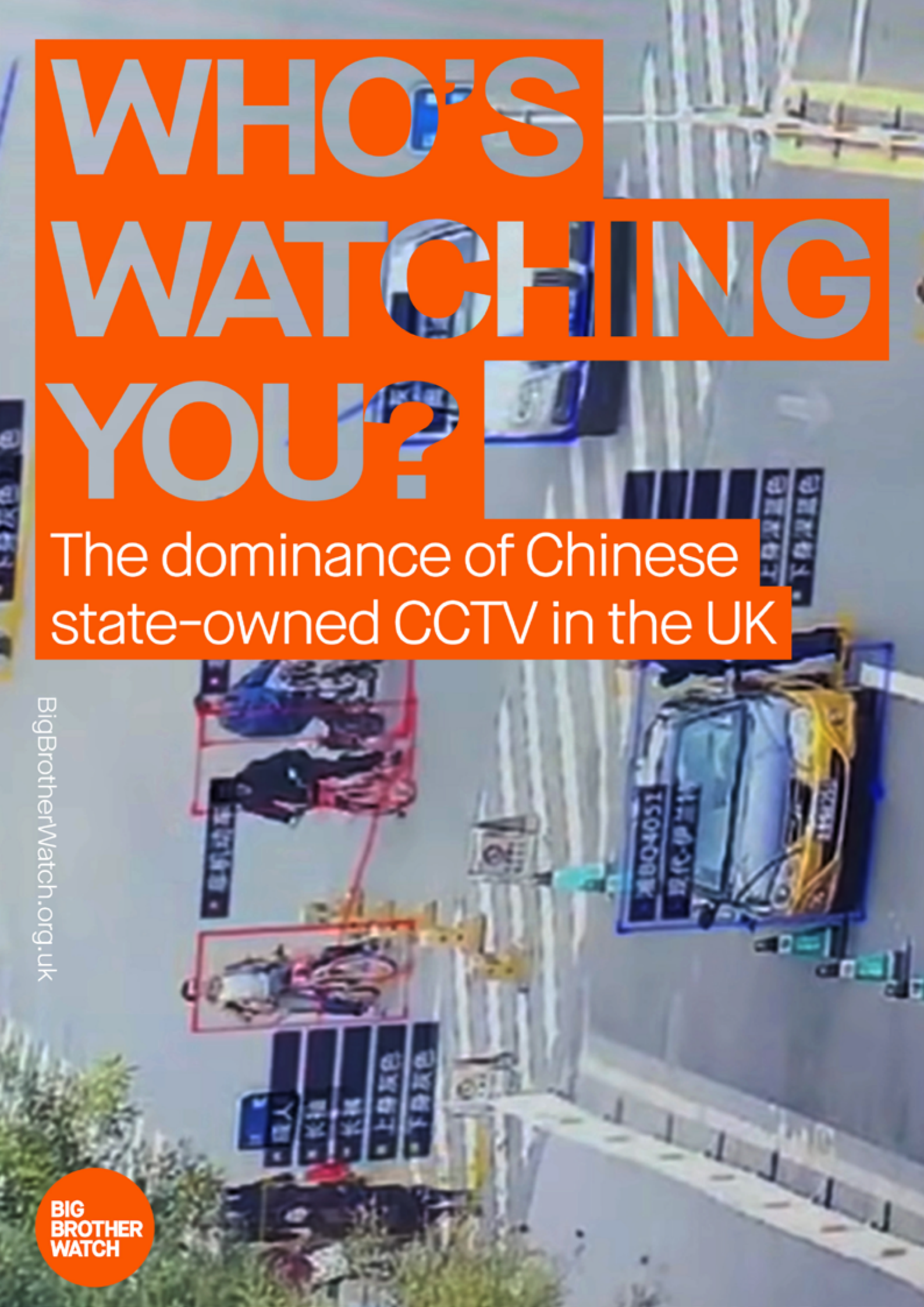

WHO'S WATCHING YOU?

The dominance of Chinese state-owned CCTV in the UK

BigBrotherWatch.org.uk

BIG BROTHER WATCH

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact
Silkie Carlo
Director
Email: silkie.carlo@bigbrotherwatch.org.uk

Jake Hurfurt
Head of Research & Investigations
Email: jake.hurfurt@bigbrotherwatch.org.uk

Acknowledgements

Thanks to Free Tibet and Will Hoyles for sharing vital data on council and government department FOI responses, helping take our findings further and correcting some wrong responses.

Thanks also to Dovydas Joksas for his important help with research for this report, particularly on the technical capabilities of the two companies.

Date published: 7th February 2022

Contents

Introduction

The UK is one of the most surveilled countries in the world with an estimated 6 million CCTV cameras across the nation.[1] London has become the most surveilled city outside of China, and even has more cameras per person than Beijing.[2] Cameras can be seen in every public building, business and on every high street – and our investigation has found that a huge number are made by controversial Chinese surveillance companies Hikvision and Dahua.

Open source data suggests that there are hundreds of thousands of internet-connected CCTV cameras made by these two companies in the UK, as well as a huge number of cameras that are not indexed online. Hikvision is the biggest CCTV manufacturer in the world, with 2020 revenues of almost £7.5 billion, while Dahua may be the second-largest CCTV maker in the world with annual revenues of just under £3 billion.[3,4]

Both brands are becoming increasingly dominant in the UK, with almost two thirds of public bodies who responded to Big Brother Watch's mass Freedom of Information requests admitting to using Chinese-made CCTV.

Advanced surveillance capabilities come as standard on many of Hikvision and Dahua's new camera models, from object detection and behavioural analysis to facial recognition. The Chinese CCTV giants market their products' smart features and algorithmic processing as much as they push their hardware. High tech equipment is becoming alarmingly widespread and threatens to normalise AI-powered surveillance of the British public without justification.

The international context is of great importance when considering why the use of Hikvision and Dahua in Britain is so concerning. Entities ultimately controlled by the Chinese Communist Party [CCP] have significant shareholdings in both companies, with Hikvision having the larger state shareholding. Both companies are known to supply surveillance equipment that has been used to target ethnic minorities in the north-western Chinese province of Xinjiang.[5]

1 One CCTV camera for every 10 people. Daily Mail, 26th October 2016, https://www.dailymail.co.uk/news/article-3872818/One-CCTV-camera-10-people-Report-says-six-million-UK-useless.html

2 Surveillance camera statistics – Paul Bischoff, Comparitech, 17th May 2021: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

3 Hikvision 2020 Annual Report, April 17th 2021, https://www.hikvision.com/content/dam/hikvision/en/brochures/hikvision-financial-report/Hikvision-2020-Annual-Report.PDF

4 Dahua Technology 2020 Annual Report, 24th March 2021, https://www.dahuasecurity.com/newsEvents/pressRelease/5087

5 'There's cameras everywhere': testimonies detail far-reaching surveillance of Uyghurs in China,

The Uyghurs, a predominantly Muslim ethnic group, are the majority population in Xinjiang. They are subjected to a brutal campaign of persecution and repression by the Beijing regime. A massive state surveillance apparatus with huge technological capability monitors the population while thousands of people are detained in detention camps that the Chinese government claims are anti-extremism education centres.[6,7]

Hikvision and Dahua have been accused of providing equipment to be used both for the general surveillance of the people of Xinjiang and to guard government-run concentration camps in the region.[8] Mass surveillance in any situation is an unjustifiable encroachment on individual rights but it is even more concerning when the technology behind Big Brother is actively implicated in the brutal persecution of ethnic minorities – a crime against humanity.

There is a significant difference, both in purpose and technological capability, between how these cameras are used in China and their use in the UK, but there remains serious privacy, legal and ethical issues when foreign companies involved in ethnic persecution watch British streets.

Security on both a national and individual basis is a further cause for concern with these cameras. Hikvision and Dahua, among other Chinese technology companies, were placed on a US list of firms that pose a threat to American national security by the Federal Communications Commission, a move that was backed by huge bipartisan majorities in both houses of Congress.[9,10] Vulnerabilities in both companies' technology and their links to the Chinese regime were key reasons behind the US blacklisting of their equipment.

Significant vulnerabilities have been identified in Dahua and Hikvision cameras on multiple occasions. Regardless of whether the security flaws are by accident or design, the frequency with which they have been flagged poses privacy and security risks.[11,12]

The Guardian, 30th September 2021, https://www.theguardian.com/world/2021/sep/30/uyghur-tribunal-testimony-surveillance-china

6 China has created a dystopian hellscape in Xinjiang, Amnesty report says, BBC News, 10th June 2021, https://www.bbc.co.uk/news/world-asia-china-57386625

7 Xinjiang: China defends 'education' camps, BBC News, 17th September 2020, https://www.bbc.co.uk/news/world-asia-china-54195325

8 Chinese CCTV cameras monitoring Britons in more than 275,000 separate networks are identified at five Uighur internment camps, The Mail on Sunday, 28th November 2021, https://www.dailymail.co.uk/news/article-10250261/Chinese-CCTV-monitoring-Britons-275-000-networks-identified-five-Uighur-camps.html

9 Congress passes bill banning new FCC equipment authorizations for Hikvision, Dahua and others, Security InfoWatch, 29th October 2021, https://www.securityinfowatch.com/video-surveillance/article/21243600/congress-passes-bill-banning-new-fcc-equipment-authorizations-for-hikvision-dahua-and-others

10 Secure Equipment Act Votes By Party, 20th October 2021, https://clerk.house.gov/Votes/2021323

11 Dahua New Critical Vulnerabilities 2021, IPVM, 7th September 2021, https://ipvm.com/reports/dahua-21-critical

12 Hikvision Has "Highest Level of Critical Vulnerability," Impacting 100+ Million Devices, IPVM, 20th

Big Brother Watch is opposed to mass surveillance in all its forms. The human rights concerns, security risks and normalisation of highly advanced camera technology make the Hikvision and Dahua takeover of British CCTV systems particularly alarming. If these cameras are used to profile and persecute ethnic minorities abroad, what could bad actors use them for at home?

The UK Government should ban the sale and operation of Hikvision and Dahua surveillance equipment in the UK and condemn their involvement in technology-enabled human rights abuses in China.

Our report also points to the benefits of Government commissioning an independent review of the scale, capabilities, ethics and rights impact of modern CCTV in the UK.

September 2021, https://ipvm.com/reports/hikvision-36260

Methodology

Over 5 months, Big Brother Watch submitted more than 4,500 Freedom of Information requests to a range of public bodies to establish where Hikvision and Dahua equipment is in use and what advanced capabilities this equipment has. Some subsequent focused requests were submitted to public bodies who confirmed they do use Hikvision cameras. The public bodies included all secondary schools and FE colleges in England, all UK universities, police forces, NHS Trusts, all Oxbridge Colleges, all central government departments, the House of Commons, the three devolved administrations and the Greater London Assembly.

We also used our social media channels and email newsletters to share call outs for the public and our supporters to let us know if they saw Hikvision and Dahua cameras being used in their communities, particularly by private businesses.

Desk research complemented this to corroborate reports of the cameras being used and to find further examples across the country. Searches on Internet of Things scraper Shodan were also informative in establishing the potential scale of the internet-connected Hikvision and Dahua networks across the country.

For statistical purposes, all figures refer to percentages of public bodies who responded to our requests for information and did not refuse to disclose details in their reply. For example, if requests about the use of Hikvision were sent to 10 schools which yielded 5 responses, two yes, two no and one refusal due to an exemption, the findings would be that 50% of respondent schools use Hikvision.

Headline findings

Summary

There are thousands and thousands of Hikvision and Dahua cameras in use by the public sector all over the United Kingdom. Three out of every five of the 1,300 public bodies who responded to our requests for information said they have equipment made by these two companies, adding up to almost 800 public bodies confirmed as actively using the controversial cameras.

At the time of publication, fewer than three in ten public bodies responded to our Freedom of Information requests, with the response rate varying significantly between different types of authority. Considering the high proportion of respondents that did confirm they use Hikvision or Dahua cameras, it is reasonable to assume that there are thousands of public bodies who are using equipment from the two manufacturers.

An extrapolation of the Big Brother Watch data would suggest that around 2,800 public bodies, i.e. 60.8% of all public bodies, may use Hikvision and Dahua surveillance.[13]

As most surveillance systems involve a multi-camera set up it would only require each public sector user of Chinese CCTV to operate a handful of cameras to put the number of cameras above 10,000. With a single contract between two London councils and Dahua totalling 900 cameras, it is fair to assume that the number of cameras made by the two controversial companies may be significantly greater than 10,000 from public bodies alone.[14]

Both companies' cameras are also often rebranded and sold under other names, including Honeywell and Toshiba, so the figures throughout this report may significantly under-report the true number of Hikvision and Dahua made products operating in the UK.[15]

Freedom of Information responses suggest that at least one in ten UK public bodies have some kind of algorithmic capability in their surveillance cameras made by these two

13 806 of 1,289 public bodies said they use Hikvision and/or Dahua, totalling 62.5%. If the same percentage was applied to all public bodies covered by this investigation this would extrapolate to 2,865 using the equipment. Allowing for a 10% drop in usage rates in the non-respondents provides an estimate of 2,580 public sector users.

14 UK Boroughs £1.3million, 900-Camera End-to-End Dahua Project, IPVM, 19th January 2022, https://ipvm.com/reports/uk-councils-dahua

15 Hikvision OEM Directory, IPVM, 3rd June 2021, https://ipvm.com/reports/hik-oems-dir

companies. Functions range from unattended object detection to gender recognition, facial detection and behavioural analysis such as "fight detection". There is a growing advanced video surveillance capability in the British public sector among organisations who should find it hard to justify using it, although many say they have but do not use the sophisticated capabilities their technology offers.

Information on private sector use is more difficult to obtain but Big Brother Watch is working hard to establish which private businesses are also using Chinese state-owned CCTV. Major supermarkets and fast food chains are already known to be among the private businesses using the two companies's cameras.


3 OUT OF 5 SCHOOLS
USE CCP-LINKED
SURVEILLANCE


NHS
10
OVER HALF OF NHS TRUSTS USE CCTV
IMPLICATED IN HUMAN RIGHTS ABUSES


男
短发
黑色短袖
31%
OF POLICE FORCES
USE *HIKVISION* TECH

Overall

- 60.8% of public bodies who responded to our FOI requests confirmed that they use Chinese-made CCTV.
- 89% of these use Hikvision made equipment and 12% use Dahua made equipment.[16]
- More than 10% of public bodies had advanced CCTV capabilities, including thermal scanning or facial detection.

Schools

- 63.4% of schools use Chinese-made CCTV.
- 82.1% of these use Hikvision cameras and 10.4% use Dahua equipment.
- At least 40 schools have facial recognition capabilities although most say it is not active.
- 14 have demographic detection, such as age and gender, and 17 have thermal surveillance.
- One multi-academy trust disclosed in an FOI response it has face mask detection and people-tracking capable cameras, and some of its CCTV can use AI to recognise a fight.
- A Norfolk school put Hikvision cameras in the toilets

Further Education Colleges

- 66.2% of colleges use Chinese-made CCTV
- 81.6% of these use Hikvision cameras and 14.2% use Dahua equipment.
- A handful of FE colleges bought Chinese-made thermal scanners during the pandemic
- One FE college admits to having mask detection

Universities

- 53.8% of higher education bodies use Chinese-made CCTV
- 89.7% of these use Hikvision cameras and 14.3% use Dahua equipment.

16 Some public bodies used both makes, while a small number said they used other Chinese CCTV manufacturers, so the numbers may not exactly total 100%.

Police Forces

- 34.9% of UK Police Forces use Chinese-made CCTV equipment
- All of these use Hikvision cameras
- Police forces were reluctant to answer questions about any advanced capabilities, while some refused to say if they used Chinese brands at all.

NHS Trusts

- 60.3% of NHS Trusts use Chinese-made CCTV equipment
- 85.7% use Hikvision and 14.3% use Dahua
- One hospital appears to have a mask detecting camera at the door to A&E.
- A specialist hospital in north west London uses a combined metal detector arch and thermal scanner at the entrance.

Local Authorities

- 73.2% of local authorities use Chinese-made CCTV
- 90.4% use Hikvision while 10.2% use Dahua
- Manchester and Glasgow, home to some of the highest populations of Chinese descent in the UK, both use Hikvision.
- Some local authorities are acting on concerns about Hikvision's controversial record.

Government Departments

- Of the 4 departments who responded to the request without a refusal 1, the Department for Work and Pensions, said it used Hikvision cameras.
- This is despite the Ministry of Defence advising that Hikvision should not be used in schools.

Advanced surveillance capabilities

Both Hikvision and Dahua use their websites to boast about the technology that comes with their CCTV cameras. As two of the biggest players in the global CCTV market, it is no surprise that they are at the bleeding edge of surveillance technology - and their dominance in the UK's CCTV market is normalising high-tech surveillance in the UK. The public and policy-makers alike should know that when they look at a Hikvision or Dahua lens, the camera might be doing a lot more than recording a video.

This section primarily focuses on advanced CCTV and analytics rather than general technical progress in CCTV such as enhanced night vision or colour reproduction. All findings are based on English-language marketing materials and websites suggesting that these technologies are available in the West. Hikvision and Dahua are not the only companies who offer these kind of smart features, but there are unique issues given the dominance and human rights records of these particular companies.

Hikvision Technology Overview

AcuSense

AcuSense adds deep learning capabilities, with a focus on sifting through video footage, to certain models of CCTV camera or older cameras through a networked video recorder (NVR) rather than through in-camera technology.[17]

The range of capabilities includes:

- live facial recognition[18]
- face search —administrators can search past footage by providing an image of a face.[19]
- detecting when humans or vehicles enter a restricted area[20]
- sorting footage by whether human or vehicle was detected

17 Hikvision, TurboHD X brochure, accessed on 18th January 2022, www.hikvision.com/content/dam/hikvision/en/brochures/core-technology/acusense/TurboHD%20X%20Brochure.pdf

18 Hikvision, AcuSense NVR infographic, accessed on 18th January 2022, https://www.hikvision.com/content/dam/hikvision/uk/products/acusense/AcuSense_NVR_Infographic-.pdf

19 DVSLTD, Hikvision facial recognition camera review & how to guide, 3rd April 2018, https://www.youtube.com/watch?v=8upp8w_voPw

20 Hikvision Corporate Channel, Hikvision AcuSense camera,11th March 2020, https://www.youtube.com/watch?v=_oiWSL5xSGA

- sorting footage by event type including alarm input, motion, face, vehicle, line crossing, region entrance, region exiting, loitering, people gathering, unattended baggage, object removal, sudden change of sound intensity
- mask detection[21]

DeepinView/DeepinMind

DeepinView and DeepinMind is another series of Hikvision products with a focus on the detection of people and objects. There are both cameras and NVRs offering DeepIn technology with a range of capabilities including[22]:

- facial recognition
- gender and age recognition[23]
- clothing and glasses detection
- baggage and bicycle detection
- mask and hard hat detection
- queue detection and counting
- vehicle detection and recognition
- expression and emotion detection

Heat Mapping

Hikvision's Heat Mapping technology uses cameras with built-in temperature sensors to create heat maps of where and for how long people stay in a given area, and to understand customer activity over time. Hikvision suggests that the technology could be used in retail, to understand what the most popular items or parts of a shop are, or in advertising, to understand "whether the promotional goods or activities successfully attract the customers".[24,25]

21 Hikvision, Hikvision mask detection solution., accessed on 18th January 2022, https://www.hikvision.com/uk/solutions/solutions-by-function/mask-detection-solution/

22 Hikvision DeepInView Press Release, accessed 18th January 2022, https://www.hikvision.com/europe/products/IP-Products/Network-Cameras/DeepinView-Series/DEDICATED-DEEPINVIEW-SERIES/6-Switchable-Algorithms/

23 Hikvision DeepinView video, 21st February 2019, https://www.youtube.com/watch?v=TRWf08mMoI4

24 Hikvision, Heat mapping, accessed on 18th January 2022, https://www.hikvision.com/uk/solutions/solutions-by-function/heat-mapping/

25 Hikvision Europe, How to configure heat map function of fisheye camera, 28th June 2019, https://

The vast majority of Hikvision cameras marketed on the company's website offer a degree of advanced capability, though not all come with the wide range of tools marketed with the deep-learning and AI-powered models. However, even some of the models in the brand's "value" range offer some functions such as unattended baggage detection, which suggests that algorithmic CCTV monitoring is being normalised in their CCTV packages.[26]

Dahua Technology Overview

Dahua has also created branding for its smart and AI features. WizMind and WizSense, can be deployed either via equipped cameras or NVRs. The Wiz line of algorithm-driven CCTV claims to offer:[27,28,29,30,31]

- face detection and facial recognition
- facial image enhancement
- gender and age recognition*
- glasses and clothing analysis
- facial hair detection
- mask detection
- bag and umbrella detection
- PPE detection
- emotion recognition including anger, calm, happiness, sadness, disgust, surprise, confusion, fear
- detecting "VIPs" and specific human targets from external sources or local databases
- heat mapping

*One Dahua infographic implies that the software performs demographic analysis within 10-year age ranges— an example of a male in the 30–39 age group is given.[32]

www.youtube.com/watch?v=HR6jyvjpwA0

26 Hikvision DS-2DE3404W-DE(T5) listing, accessed 18th January 2022, https://www.hikvision.com/uk/products/IP-Products/PTZ-Cameras/Value-Series/ds-2de3404w-de-t5-/

27 Dahua, IPC-HDBW5442E-ZE listing, accessed on 25th January 2022, https://www.dahuasecurity.com/ products/All-Products/Network-Cameras/WizMind-Series/5-Series/4MP/IPCHDBW5442E-ZE

28 Dahua, IPC-HFW5849T1-ASE-LED listing, accessed 25th January 2022, https://www.dahuasecurity.com/products/All-Products/Network-Cameras/WizMind-Series/5-Series/Fullcolor/ IPC-HFW5849T1-ASE-LED

29 Dahua, Video Metadata 2.0, accessed 25th January 2022, https://www.dahuasecurity.com/products/keyTechnologies/742/92

30 Dahua, Privacy Protection 2.0, accessed 25th January 2022, https://www.dahuasecurity.com/products/keyTechnologies/742/197

31 Dahua, Heat Map, accessed 25th January 2022 https://www.dahuasecurity.com/products/keyTechnologies/742/142

32 Dahua, Develop smarter strategies with deeper business insights, accessed 25th January 2022, https://www.dahuasecurity.com/asset/upload/uploads/soft/20210104/Leaflet_Dahua-Smart-Retail-

As with Hikvision, even many lower end Dahua models offer a degree of "smart" or algorithmic video analysis. Cameras in the "Lite" range are marketed as containing algorithms that can detect area intrusion or tripwire crossing in a manner that goes beyond traditional motion sensors.[33]

Discussion

Hikvision and Dahua are primarily responsible for the normalisation of high-level video analytics for even basic CCTV systems in the UK, rapidly expanding the surveillance state. Some of their advanced features pose extreme human rights risks – particularly ethnicity detection/alert systems. Whilst CCTV operators are obliged to disclose sensitive data processing in a Data Protection Impact Assessment, there is little oversight of this requirement and in practice it is difficult to discover where such capabilities may be in use.

One in six public bodies who have Chinese CCTV said they had some degree of analytical capability, from object detection to temperature checks. This amounts to more than 10% of all public bodies who responded to our Freedom of Information requests. Many public bodies, schools in particular, told us that although they have advanced capabilities they are not in use.

There is little reason for a school to own surveillance cameras that can detect the age or gender of pupils in the corridor or for a hospital to have facial recognition, yet some do. AI-monitoring of the general public is becoming increasingly normalised, sometimes for little more than £100 per camera.[34]

Security camera experts, such as IPVM founder John Honovich, have suggested that Hikvision's rise to the top of the global CCTV market is due to the company's incredibly low prices.[35,36] This, combined with the increasingly standard inclusion of some algorithmic capability, is a clear signal that high-tech surveillance is becoming the norm rather than the exception at almost every price point.

Operation-Solution_V1.0_EN_202012(8P).pdf

33 Dahua Lite Series Lite Series |DH-IPC-HDW2439T-AS-LED-S2 listing, accessed 25th January 2022, https://www.dahuasecurity.com/asset/upload/uploads/cpq/DH-IPC-HDW2439T-AS-LED-S2_datasheet_20201215.pdf

34 Hikvision DS-2CD2365G1 listing, accessed 31st January 2022, https://www.scan.co.uk/products/hikvision-ds-2cd2365g1-i28mm-6mp-camera-28mm-fixed-ir-lens-easyip-poe?gclid=Cj0KCQiArt6PBhCoARIsAMF5wahUZAZAQvNgvq8VSDFmUjOq1o_7eLblLOW636X4ntyxfmfxyVDduysaAh8yEALw_wcB

35 John Honovich, IPVM Forum, 18th February 2015, https://ipvm.com/forums/video-surveillance/topics/ip-cameras-price-competition

36 John Honovich, IPVM Forum, 15th April 2016, https://ipvm.com/forums/video-surveillance/topics/hikvision-where-margins-don-t-matter

The quiet rise of machine-monitored cameras in the modern British surveillance state, where face-analysing cameras are popping up on ordinary high streets, is alarming. Whether made by a Chinese stated-owned megacorporation or a UK start-up, high-tech video monitoring of innocent people must not be normalised.

Technology-enabled human rights abuses

Overview

Mass surveillance raises serious human rights concerns, particularly concerning privacy, freedom of expression and freedom of assembly. The growing use of Hikvision and Dahua raises additional rights and ethics concerns. Both companies supply technology that is used in Xinjiang where there is overwhelming evidence that serious human rights abuses are being committed against ethnic minorities by the Chinese state.[37]

In December 2021, an unofficial tribunal based in London alleged that Uyghurs, the region's largest ethnic group, were victims of genocide in a campaign of repression that involves torture and attempts to suppress the Uyghur birth rate.[38] Tribunal chair Sir Geoffrey Nice QC, a barrister who previously prosecuted the former Yugoslavian President Slobodan Milošević for war crimes, said that the crimes against humanity being committed would require cooperation from the highest echelons of state power.[39]

Human rights groups and the UK House of Commons Foreign Affairs Select Committee have alleged that Uyghurs are subject to atrocities ranging from forced labour in so-called education centres to the repression of Islamic cultural practices and an environment of mass surveillance.[40,41] The details of these abuses should prompt a serious review of the legality, ethics and rights and security risks of trading with Hikvision and Dahua. Both companies have been repeatedly named as providing equipment to the internment camps holding thousands of people and for the mass surveillance apparatus in the region as a whole, including by Amnesty International and the Foreign Affairs Select Committee.[42,43]

---

37 'There's cameras everywhere': testimonies detail far-reaching surveillance of Uyghurs in China, The Guardian, 30th September 2021, https://www.theguardian.com/world/2021/sep/30/uyghur-tribunal-testimony-surveillance-china

38 Uyghurs subjected to genocide by China, unofficial UK tribunal finds, The Guardian, 9th December 2021, https://www.theguardian.com/world/2021/dec/09/uyghurs-subjected-to-genocide-by-china-unofficial-uk-tribunal-finds

39 Ibid.

40 China's mass internment, torture and persecution of Muslims in Xinjiang, Amnesty International, 10th June 2021, https://www.amnesty.org/en/wp-content/uploads/2021/07/ASA1741372021ENGLISH.pdf

41 Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond, House of Commons Foreign Affairs Committee, 29h June 2021, https://committees.parliament.uk/publications/6624/documents/71430/default/

42 Chinese CCTV cameras monitoring Britons in more than 275,000 separate networks are identified at five Uighur internment camps, The Mail on Sunday, 28th November 2021, https://www.dailymail.co.uk/news/article-10250261/Chinese-CCTV-monitoring-Britons-275-000-networks-identified-five-Uighur-camps.html

43 US Towns Are Buying Chinese Surveillance Tech Tied to Uighur Abuses, TechCrunch, 24th May 2021, https://techcrunch.com/2021/05/24/united-states-towns-hikvision-dahua-surveillance

Hikvision refused to deny the claims though stated that they were "unsubstantiated"[44] - months before IPVM identified several Hikvision cameras in a video of the camps.[45]

Rights Abuses in Xinjiang Detention and the Presence of CCTV Cameras

In 2021, an Amnesty International report alleged that the Chinese regime is responsible for crimes against humanity and had created a "dystopian hellscape".[46] Amnesty collected evidence from dozens of people who had been detained in Xinjiang who outlined the efforts being made by the Chinese government to suppress the religious and ethnic identities of local Muslim ethnic groups, including Uyghurs and Kazakhs.

The Amnesty report said that hundreds of thousands of people from Muslim ethnic groups had been sent to prison and further hundreds of thousands of people had been sent to what the Chinese government describes as training or education centres under the banner of anti-extremism.

Despite deflection from Beijing, it is alleged that these "education camps" are centres of indoctrination, abuse and brainwashing aimed at replacing faith in Islam with faith in Chinese state ideology.[47]

There are also reports from Xinjiang's prisons of direct physical abuse such as beatings, solitary confinement and electric shocks. Evidence from people detained in the prisons suggested that psychological and physical harm is commonplace and Amnesty said it was aware of deaths following the abuse.[48]

Other reports say that women in the camps are the victims of harrowing incidents of sexual violence. Former female detainees have given accounts of being raped by several attackers and witnessing countless other women being sexually assaulted by masked

44 CCTV watchdog criticises Hikvision Uyghur response – Chris Vallance, BBC News, 14th August 2021, https://www.bbc.co.uk/news/technology-58188325
45 Video Reveals Hikvision Cameras Surveilling Xinjiang Concentration Camps – Charles Rollet, IPVM, 19th November 2021, https://ipvm.com/reports/hik-video-xinjiang.html
46 China: 'Crimes against humanity' being committed in Xinjiang, Amnesty International, 10th June 2021, https://www.amnesty.org.uk/press-releases/china-crimes-against-humanity-being-committed-xinjiang-new-report
47 China's mass internment, torture and persecution of Muslims in Xinjiang, Amnesty International, 10th June 2021, https://www.amnesty.org/en/wp-content/uploads/2021/07/ASA1741372021ENGLISH.pdf
48 China: 'Crimes against humanity' being committed in Xinjiang, Amnesty International, 10th June 2021, https://www.amnesty.org.uk/press-releases/china-crimes-against-humanity-being-committed-xinjiang-new-report

men.[49] This large scale use of sexual violence is coupled with efforts to reduce the Uyghur birth rate through involuntary sterilisation, contraception and abortion.[50]

Even when someone is allowed to leave a re-education camp their destination is often state-backed forced labour programmes in industries such as cotton picking.[51] Written evidence to the Foreign Affairs Committee suggested that huge parts of the UK's textile industry is connected to forced-labour cotton picking in Xinjiang.[52] More than half a million people are subject to forced labour conditions in the region and last year the US began to ban imports of products linked to human rights violations from the area.[53,54]

The Modern Slavery Act 2015, places an obligation on UK businesses to ensure both themselves and their supply chains are free of forced labour. If either Hikvision or Dahua cameras are used to monitor and control prisoners in Xinjiang forced into slave labour, there are significant questions for UK organisations using their equipment.[55] Both companies deny modern slavery within their companies and value chains, and Hikvision claimed to oppose forced labour in a 2020 statement to the House of Commons Business, Energy and Industrial Strategy committee.[56] However, this does not address the use of their products by the Chinese state for modern slavery.

Hikvision provides the "primary camera technology" for the internment camps in Xinjiang, according to the House of Commons Foreign Affairs Committee in 2021. Against the background of the litany of horrifying abuses committed in detention facilities, the use of Hikvision technology in British schools and other public settings is alarming and raises serious ethical questions.

---

49 'Their goal is to destroy everyone': Uighur camp detainees allege systematic rape, BBC News, 2nd February 2021, https://www.bbc.co.uk/news/world-asia-china-55794071

50 China cuts Uighur births with IUDs, abortion, sterilization, Associated Press,29th June 2020, https://apnews.com/article/ap-top-news-international-news-weekend-reads-china-health-269b3de1af34e17c1941a514f78d764c

51 Never Again: The UK's Responsibility to Act on Atrocities in Xinjiang and Beyond, House of Commons Foreign Affairs Committee, 29h June 2021, https://committees.parliament.uk/publications/6624/documents/71430/default/

52 Written submission by Anti-Slavery International and the CORE Coalition to the House of Commons Foreign Affairs Committee, 30th October 2020, https://committees.parliament.uk/writtenevidence/13587/pdf/

53 U.S. Bans All Cotton and Tomatoes From Xinjiang Region of China, The New York Times, 13th January 2021 https://www.nytimes.com/2021/01/13/business/economy/xinjiang-cotton-tomato-ban.html

54 Xinjiang: more than half a million forced to pick cotton, report suggests, The Guardian, 15th December 2020, https://www.theguardian.com/world/2020/dec/15/xinjiang-china-more-than-half-a-million-forced-to-pick-cotton-report-finds

55 Transparency in Supply Chains 2017, Home Office, accessed 31st January 2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1040283/Transparency_in_Supply_Chains_A_Practical_Guide_2017_final.pdf

56 Written evidence submitted by Hikvision (FL0026), BEIS Select Committee, October 2020, https://committees.parliament.uk/writtenevidence/13768/pdf/#:~:text=In%20the%20UK%2C%20Hikvision%20UK,supply%20chains%20involve%20forced%20labor

The company's UK and Ireland subsidiary said that the committee's findings were "unsubstantiated." However, when pressed in further correspondence with Professor Fraser Sampson, the Surveillance Camera Commissioner, Hikvision UK and Ireland did not explicitly deny their cameras are used in the Xinjiang camps.[57,58,59] The surveillance company also claimed that they had little to do with the cameras once they are given to the end-user but Professor Sampson had further doubts. The Commissioner pointed to contracts in Hikvision's 2020 Annual Report to Shareholders, in which a £39million "social prevention and control system" tender from a local government in Xinjiang won by Hikvision contained language that suggested the system would be run as a joint enterprise rather than by the municipality alone.

Reporting by IPVM also identified some Hikvision cameras in use in and around detention camps in Xinjiang. Based on analysis of a YouTube video of internment camps uploaded by a Chinese vlogger, several advanced cameras made by Hikvision were observed around the facilities. IPVM identified these as AI-capable equipment able to analyse the scenes caught on camera and provide alerts.[60]

BBC News also captured evidence of a Hikvision DarkFighter camera, designed to perform well in low light conditions, when touring a Uyghur re-education camp in 2019.[61] Further reports identified Hikvision as having won another contract for the video surveillance of re-education camps in Moyu County, Xinjiang.[62,63]

Dahua cameras have also been identified at the entrances of internment camps in Xinjiang. Whilst they are identified as being used in the camps less commonly than Hikvision, they are a major player in mass surveillance in the region.[64]

57 Hikvision Letter on the Foreign Affairs Committee Report, 12th July 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004414/UK_Partner_Letter_on_Foreign_Affairs_Committee_Report_12_July_2021.pdf

58 Letter from Professor Sampson to Hikvision, 16th July 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004416/BSCC_Letter_to_Justin_Hollis_Hikvision_July_2021.pdf

59 Letter from Hikvision to Professor Sampson, 10th August 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010166/Letter_Surveillance_Commisioner_10_August_2021.pdf

60 Video Reveals Hikvision Cameras Surveilling Xinjiang Concentration Camps, IPVM, 29th November 2021, https://ipvm.com/reports/hik-video-xinjiang.html

61 Inside China's 'Thought Transformation' Camps, BBC News, 17th June 2019, https://www.bbc.co.uk/news/av/world-asia-china-48667221

62 Chinese Frism Cash in on Xinjiang's Growing Police State, AFP, 27th June 2018, https://www.afp.com/en/chinese-firms-cash-xinjiangs-growing-police-state

63 Hikvision Wins Chinese Government Forced Facial Recognition Project Across 967 Mosques, IPVM, 16th July 2018, https://ipvm.com/reports/hik-mosques

64 Chinese CCTV cameras monitoring Britons in more than 275,000 separate networks are identified at five Uighur internment camps, The Mail on Sunday, 28th November 2021, https://www.dailymail.co.uk/news/article-10250261/Chinese-CCTV-monitoring-Britons-275-000-networks-identified-five-Uighur-camps.html

There is overwhelming evidence that Hikvision surveillance equipment is watching over sites where some of the worst crimes against humanity in the 21st Century are taking place, and as such, is contributing to the atrocities. The same technologies, including AI-powered video analytics and DarkFighter, that are used in Chinese concentration camps are in use on Britain's streets, in schools and hospitals. How this technology is used abroad raises serious questions as to why public and private organisations in the UK continue to use the cameras.

Mass Surveillance in Xinjiang and the role of Hikvision & Dahua

Almost everyone in Xinjiang, not just those in detention, live under the watchful eye of Big Brother. Surveillance companies, including Hikvision and Dahua, have profited handsomely from major contracts to provide the apparatus to monitor and control millions of people. The two companies have won almost £900 million ($1.2 billion) worth of contracts in the region to work on massive surveillance projects.[65]

Muslims living in the region are "are among the most heavily surveilled populations in the world" according to Amnesty International. CCTV cameras, digital monitoring and police checkpoints contribute to an all-encompassing surveillance state.[66] One group of journalists visiting towns in the region over the last few years described surveillance cameras looming "every few feet" while others dubbed Xinjiang a surveillance laboratory.[67]

Exactly how many CCTV cameras are active in Xinjiang is not known, but the sheer size of the contracts awarded to Hikvision and Dahua offer some insight into the scale of the surveillance. Many of the contracts are for public-private partnerships with municipalities supposedly focussed on making areas safe and secure.[68]

One £58 million contract awarded to Hikvision to create a "safe zone" in the city of Ürümqi, with a population of around 3.5 million, included 30,000 new CCTV cameras, a video analysis centre and a comprehensive monitoring operation over a 10 year co-operation period.[69] A significant number of additional contracts were awarded to Dahua

65 In China's Far West, Companies Cash in on Surveillance Program That Targets Muslims, Foreign Policy,13th June 2018, https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/

66 China's mass internment, torture and persecution of Muslims in Xinjiang, Amnesty International, 10th June 2021, https://www.amnesty.org/en/wp-content/uploads/2021/07/ASA1741372021ENGLISH.pdf

67 Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life, Wall Street Journal, 19th December 2017, https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355#

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

69 Hikvision contract announcement, accessed 25th January 2022, https://web.archive.org/

and Hikvsion for projects with similar names that were signed in the late 2010s by other Xinjiang municipalities, worth tens of millions of pounds.[70]

From the high value of the contracts, spanning several cities, it is clear that the two companies have supplied equipment for growing mass surveillance networks in Xinjiang. However, it is not just the scale of the surveillance that is concerning when considering how similar cameras are used in the UK, but the technological capabilities that are being developed given their deployment to persecute Muslim minorities in China.

Both Hikvison and Dahua have developed advanced CCTV that can and do racially profile individuals passing by the cameras.[71,72,73] It has been reported that racial profiling surveillance is not limited to Xinjiang but is used in other large Chinese cities to target Uyghurs living elsewhere in the country.[74]

The Dahua ethnicity profiling algorithms were found by an engineer who posted his discovery on Twitter, highlighting a Uyghur classification in the camera's software. However, Dahua reportedly deleted the code after being contacted by journalists.[75] Hikvision also quickly deleted a product listing, which suggested the camera could identify whether someone was of Uyghur or Han [the dominant ethnic group in China] background.[76] It has been reported that the Dahua technology provided police with real-time "Uyghur alerts".[77]

Big Brother Watch does not have any evidence that any UK public sector organisation is using race-detecting algorithms developed by Hikvision or Dahua. However, we have found that at least two dozen public bodies have similar capabilities, though they are not necessarily in use. Freedom of Information responses to us found that 24 public sector organisations, including 14 schools, six councils, two hospitals, a university and a further education college, have cameras capable of profiling an individual's age and gender.

---

web/20191202173217/http://www1.hikvision.com/cn/news_detail_63_i2394.html

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

71 Hikvision DS-2CD7A2XYZ-JM/RX Chinese Listing, accessed on Wayback Machine 25th January 2022, https://web.archive.org/web/20191107042500/http://www1.hikvision.com/cn/prgs.aspx?c_kind=2&c_kind2=2&c_kind3=445&c_kind4=446&id=42808

72 Dahua Racist Uyghur Tracking Revealed, IPVM, 4th November 2020,https://ipvm.com/reports/dahua-uyghur

73 One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, The New York Times, 14th April 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

74 Ibid.

75 Dahua Racist Uyghur Tracking Revealed, IPVM, 4th November 2020,https://ipvm.com/reports/dahua-uyghur

76 Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up, IPVM, 11th https://ipvm.com/reports/hikvision-uyghur

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

Likewise, the underlying technology algorithmically analyses individual faces to identify their characteristics. These advanced capabilities are highly intrusive and prone to abuse, regardless of whether they are active, the technology has no place in public bodies in the UK.

Ethnicity profiling AI is just one of the high-tech facial recognition based tools used against ethnic minorities in China. Emotion detection AI has also been trialled on Uyghurs with computer software analysing people's faces in attempt to detect their inner feelings.[78] A whistleblower said the systems have been included in places such as police stations and compared them to an advanced lie detector. It was claimed that the software goes beyond flagging somebody as happy or sad, using AI to generate emotional pie charts with segments including anxiety.

Emotional and ethnicity detection AI are branches of facial detection - technology that has been widespread in Xinjiang for several years.[79] Algorithm-driven facial analysis is built on software that can detect and recognise faces and the difference between estimating age and race is little more than a software update away.

Face-detecting Hikvision cameras, with TV screens showing faces in green boxes, are already in use in locations as sensitive as the A&E reception of some hospitals. We recommend that close attention is paid to the more than 5% of public bodies with Hikvision or Dahua-made facial or demographic detection capabilities, to make sure theydo not enter common use.[80]

78 AI emotion-detection software tested on Uyghurs, BBC News, 26th May 2021, https://www.bbc.co.uk/news/technology-57101248

79 In Xinjiang, China, surveillance technology is used to help the state control its citizens, CBC,1st November 2019, https://www.cbc.ca/passionateeye/features/in-xinjiang-china-surveillance-technology-is-used-to-help-the-state-control

80 Analysis of FOI Responses Received by Big Brother Watch, January 2022

Tower Hamlets Rejects CCP Surveillance

The London Borough of Tower Hamlets has been a strong voice in local government on the suffering of Uyghurs, opposing Chinese plans to relocate their embassy to the former site of the Royal Mint in the East End of London.[81] Streets and buildings surrounding the proposed site could be renamed to support human rights in China. Despite being the planned home of Beijing's London outpost, the Borough told us it does not use Hikvision or other Chinese CCTV companies due to their role in persecuting ethnic minorities.

In an FOI response to Big Brother Watch, Tower Hamlets said, "The council is aware of the Human Rights issue with Hikvision and other Chinese CCTV companies and has made a conscious decision over a year ago to ensure that any of these products are not procured. Instructions have been given to all contractors, housing, regeneration etc not to allow these products to be used or installed," showing that local authorities can lead the line in opposing the use of oppressive technologies in the UK.

Summary

Hikvision and Dahua-developed surveillance equipment are at the heart of China's persecution of Uyghurs, both in the camps where the worst atrocities take place and as the framework for the Big Brother state that monitors millions of people going about their daily lives. There is little doubt that their products facilitate atrocities and there is significant evidence to suggest that Chinese surveillance companies do more than sell cameras to local municipalities, instead taking an active role in partnerships to manage surveillance networks.

The rising numbers of Chinese CCTV cameras used to monitor schools, hospital corridors and public buildings raise serious concerns given thatsimilar cameras made by the same companies guard the gates of internment camps abroad. Some of the most alarming technology has already crossed over into their Western product lines and the abuse potential of advanced surveillance must be accounted for when Hikvison and Dahua cameras are bought and operated in the UK.

81 Tiananmen Square, Uyghur Court: Tower Hamlets plans name changes in solidarity, The Guardian, 19th March 2021, https://www.theguardian.com/uk-news/2021/mar/19/uyghur-court-hong-kong-road-tower-hamlets-plans-name-changes-in-solidarity

The Chinese state's atrocities in Xinjiang are technology-enabled human rights abuses, involving companies that dominate the CCTV market in the UK. It is incumbent on the UK Government to review the sale and operation of such companies in the UK.

Free Tibet View on Human Rights Abuses

In recent years, the Chinese government has taken advantage of the expertise Hikvision's success around the world gives it, to support the creation of a massive surveillance state where everyone is watched all the time by some of the most advanced camera technology in the world. While state surveillance affects everyone living under Chinese Communist Party rules, it is particularly focused on those who are not part of the majority Han Chinese ethnicity, and especially in countries that China occupies. As a result, Tibet is now the least free country in the world according to Freedom House, and several countries, including the USA[1], have said that the persecution of the Uyghur people in occupied East Turkestan is a genocide.

It is a genocide enabled in large part by Hikvision. In July 2021, UK Members of Parliament on the influential Foreign Affairs Select Committee said that Hikvision cameras are "deployed throughout Xinjiang [the name the Chinese government gives East Turkestan], and provide the primary camera technology used in the internment camps."[2] At least 1 million, largely Muslim, Uyghurs have been sent to these internment camps under the pretence of countering "extremism" but in practice, researchers have noted that detainees have been targeted based on their religious and cultural identity.

On two occasions Hikvision has been discovered to be marketing cameras that can distinguish between Han Chinese and members of what the Chinese government refers to as 'ethnic minorities',such as Uyghurs or Tibetans. Hikvision has quickly covered up that it sold the cameras but the use of artificial intelligence to track individuals and those from certain ethnicities is still well established in Chinese-controlled areas.

Hikvision might want to hide its racist technology but it proudly advertises its role in providing surveillance on the controversial Qinghai-Tibet Railway which is having devastating environmental impact and allows the rapid deployment of troops to the disputed Indo-Tibet border area.[3] There is also strong evidence that Hikvision supplied the equipment that allowed the creation of, former Chinese Communist Party chief of Tibet, Chen Quanguo's surveillance state in Tibet.[4] The so-called 'iron grid' divided the Tibetan capital Lhasa into small sections each patrolled by Communist party officials and

1 US Says China's Repression of Uighurs is 'Genocide', The New York Times, 19th January 2021, https://www.nytimes.com/2021/01/19/us/politics/trump-china-xinjiang.html

2 Never Again, House of Commons Foreign Affairs Select Committee, 8th July 2021

3 Hikvision's Network DVRs Secure Qinghai-Tibet Railway, Hikvision, accessed 25th January 2022, https://www.hikvision.com/pl/newsroom/success-stories/traffic/hikvision-s-network-dvrs-secure-qinghai-tibet-railway/

4 Developing technological totalitarianism in Tibet: Huawei and Hikvision, International Campaign for Tibet, 17th December 2018, https://savetibet.org/developing-technological-totalitarianism-in-tibet-huawei-and-hikvision/#2

local volunteers in order to monitor the movements of anyone who might be problematic to the state, and included a police station every 500m in Lhasa. Chen later became the party leader for Xinjiang where he established similar policies.

In 2022, surveillance is everywhere the CCP reaches. In Tibet, government cameras are even inside monasteries and nunneries, where they monitor Tibetan Buddhists and ensure that portraits of Xi Jinping are not replaced by the illegal image of the Dalai Lama. In taxis, passengers encounter real-time facial recognition cameras inside taxis. The impact on Tibetans is huge with many telling Free Tibet that they are scared to catch the eye of officials in public or to do anything that those watching on the cameras might interpret as dissent. None of this would be possible without the complicity of companies like Hikvision and their customers around the world.

Security Threats

Despite the significant role Hikvision and Dahua play in Beijing's state surveillance apparatus, both companies have track records of significant cybersecurity problems and glitches that could put the privacy of individuals and organisations at risk. Generally, the security threats affect internet-connected [IP] cameras and several public bodies clarified to Big Brother Watch that their surveillance systems are not internet-connected. However, with most newer Hikvision and Dahua models being IP cameras, the issues outlined in this section can only become more pertinent over time.

In the US the Federal Communications Commission [FCC], later backed up by an almost unanimous vote in Congress, has effectively banned the import and sale of Hikvision and Dahua products, among others.[82] Steve Scalise, the Republican Congressman who introduced the bill formalising the FCC ban on the companies, said the restrictions were aimed at stopping "compromised" Chinese equipment from putting communications networks at risk and protecting both national and individual security.[83]

The FCC gave more detail about why the two brands were among several Chinese companies placed under restrictions when its commissioners approved the initial ban. One commissioner explained that he could not "continue to authorise, import and use equipment from companies deemed to present a national security threat".[84]

This all came two years after a ban on Hikvison selling to American government agencies that dates back to summer 2019 and initial steps to restrict both brands' use in the USA due to national security and human rights concerns.[85,86]

Australian authorities have also banned Hikvision cameras, with the federal government reportedly removing the equipment from public sector buildings due to major security

82 Congress passes bill banning new FCC equipment authorizations for Hikvision, Dahua and others, Security Ingo Watch, 29th October 2021, https://www.securityinfowatch.com/video-surveillance/article/21243600/congress-passes-bill-banning-new-fcc-equipment-authorizations-for-hikvision-dahua-and-others

83 House Passes Scalise, Eshoo Bill, 20th October 2021, https://scalise.house.gov/media/press-releases/house-passes-scalise-eshoo-bill-protecting-us-telecom-networks-against-chinese

84 FCC Explains Why They Plan To Ban Dahua And Hikvision, IPVM, 23rd June 2021, https://ipvm.com/reports/fcc-ban-plan

85 Hikvision, a surveillance powerhouse, walks US-China tightrope, Reuters, 29th August 2019,https://www.reuters.com/article/us-hikvision-china-insight/hikvision-a-surveillance-powerhouse-walks-u-s-china-tightrope-idUSKCN1VJ05C

86 The United States Blacklisted 28 Chinese Entities over Repression of Muslim Minorities in Xinjiang. What Does This Mean for Human Rights? Centre for Strategic and International Studies, 11th October 2019, https://www.csis.org/analysis/united-states-blacklisted-28-chinese-entities-over-repression-muslim-minorities-xinjiang

concerns and state governments expected to do likewise.[87] The state government in South Australia moved in early 2020 to remove Hikvision cameras from any buildings it owns.[88] Technical and security issues were given as the reason for pulling out of the partnership that saw Hikvision cameras trialled in state government buildings. Before this, it has been the policy of the Australian military since 2018 to remove and not use Hikvision cameras.[89]

The government of the People's Republic of China, through state-owned companies and their subsidiaries, is the controlling shareholder of Hikvision despite the company claiming it is independent. There is also a significant link between the formal state apparatus in Beijing and the company's leadership with Hikvision Chairman Chen Zongnian joining the National People's Congress, the Chinese Parliament in 2018.[90]

Dahua is less directly controlled by the Chinese government, although there is still a significant state-backed shareholding. State-run investment companies control around 2.9% of Dahua while China Mobile, the PRC-owned mobile operator, bought 10.4% of the company in 2020.[91,92]

Both companies have significant state links and this is important context when considering who may have access to their software and technology as well as any security backdoors, accidental or not, that may exist in their products.

Dahua's cybersecurity record over the past few years is littered with examples of serious vulnerabilities. In the last six months alone, high-risk vulnerabilities have been identified in the company's camera software.[93,94] According to Dahua itself, the most recent breach was in the password reset process and could have given bad faith actors access to many internet-connected camera models and allowed them to change access passwords.[95] In autumn 2021, vulnerabilities were flagged in the login process that could have given

87 Banned Hikvision Cameras Surfaces in Australia as Ezviz, The Gadget Guy, 12th September 2020, https://www.gadgetguy.com.au/banned-hikvision-cameras-surface-in-australia-as-ezviz/

88 Chinese surveillance cameras removed due to security concerns, Sydney Morning Herald, 21st January 2020, https://www.smh.com.au/politics/federal/chinese-cameras-removed-out-of-security-concerns-20200121-p53t7u.html

89 Ibid.

90 Hikvision, Corporate Governance, and the Risks of Chinese Technology, Centre for Strategic and International Studies, 6th August 2020, https://www.csis.org/blogs/technology-policy-blog/hikvision-corporate-governance-and-risks-chinese-technology

91 Dahua Annual Report 2019. http://www.szse.cn/disclosure/listed/bulletinDetail/index.html?41435ae8-8fae-427e-b7a9-fd1afb47f24d

92 State-Owned China Mobile Acquires 10% of Dahua, IPVM, 29th March 2020 https://ipvm.com/reports/china-mobile-dahua

93 Dahua Broken Access Control Vulnerability, IPVM, 25th January 2022, https://ipvm.com/reports/dahua-33046.html

94 Dahua New Critical Vulnerabilities 2021, IPVM, 7th September 2021, https://ipvm.com/reports/dahua-21-critical

95 Dahua Security Advisory 12st January 2022. https://www.dahuasecurity.com/uk/support/cybersecurity/details/987

hackers administrator access to different Dahua camera models without the need for identity verification.

An older security flaw found in several Dahua cameras in 2019 would have allowed attackers to access embedded microphones and turn affected devices into eavesdropping tools, even when audio functions were turned off.[96] Initially identified in a Dahua-made camera sold under a different brand, the vulnerability was found to affect millions of cameras globally.

As far back as 2018 John Honovich, founder of security industry publication IPVM, criticised Dahua's cybersecurity record as "terrible" after significant coverage of the company's security from vulnerabilities to hacks and cover-ups.[97]

Hikvision equipment has also been found to be open to attack through vulnerabilities and security issues flagged over recent years, although less frequently than Dahua. In September 2021, researchers identified a critical vulnerability impacting millions of Hikvision cameras that could have allowed malicious parties to override and take control of affected cameras all over the world.[98]

Another Hikvision vulnerability from 2017 was described by US cybersecurity officials as requiring only minimal technical knowledge to exploit and would have allowed an attacker to access user accounts on the camera software or give themselves administrator privileges.[99]

Although the two CCTV companies are not alone in having security flaws in their software and hardware, concerns about privacy and national security have been raised in the context of the relationships between the Chinese state and the manufacturers.[100] John Honovich has speculated that the particularly close links between Hikvision and the Beijing regime increases the chance of state access to the cameras.[101]

---

96 Warning As Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users: Report, Forbes, 2nd August 2019, https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/

97 Dahua's Terrible Cybersecurity, Buys Credibility From PSA And SIA, IPVM, 4th June 2018, https://ipvm.com/reports/dahua-psa-sia

98 Cybersecurity Vulnerability Could Affect Millions of Hikvision Cameras, Info Security Magazine, 24th September 2021, https://www.infosecurity-magazine.com/news/vulnerability-hikvision-cameras/

99 ICS Advisory (ICSA-17-124-01), Cybersecurity and Infrastructure Security Agency, 4th May 2017, https://www.cisa.gov/uscert/ics/advisories/ICSA-17-124-01

100 Chinese cameras banned in US monitor Lithuanian leaders, Lietuvos radijas ir televizija, 2nd June 2020, https://www.lrt.lt/en/news-in-english/19/1139300/chinese-cameras-banned-in-us-monitor-lithuanian-leaders-lrt-investigation

101 John Honovich 11th August 2016, IPVM Forums, https://ipvm.com/forums/video-surveillance/topics/hikvision-is-it-true-hikvision-has-a-backdoor-to-the-chinese-government

Hikvision has denied that government-mandated backdoors exist and Watchful_IP [sic], the researcher who discovered the critical 2021 vulnerability, said that that particular glitch was not a backdoor for Beijing.[102,103]

Concerns about Chinese state access to cameras made by the two companies were exacerbated by a 2021 Italian investigations which found that Hikvision equipment installed at the national broadcaster was communicating with servers in China.

The report by state broadcaster Rai in May 2021, titled "L'Occhio del Dragone" [the eye of the dragon], focussed on Hikvision inside the TV network's buildings. Rai journalists discovered that data was being sent to a server in the US and then on to another server in China.[104] In transcripts of interviews from the television investigation, a senior official from Hikvision Italia implied that the findings were a glitch and that he was unaware of data from internet-connected Hikvision cameras flowing to China.[105] Cybersecurity experts told the Italian program that the risk was most acute when cameras are open to the wider internet, either due to updates or due to poor installation.

Rai identified a second, potentially more serious example, of Hikvision cameras accessing unknown servers. In 2015 CCTV at Rome's Fiumicino Airport, which had 45 million passengers a year before the pandemic, saw more than 100 Hikvision cameras suddenly try to connect to an unknown external IP address a significant number of times – more than 1.5 million requests were identified in total.[106]

Although the country origin of the unknown IP address was never identified, cyber security experts pointed to similarities between issues at the airport and the broadcaster. The president of Genetec, the security company which installed the cameras, said it would not be comfortable with Hikvision cameras being installed in sensitive areas today.[107]

---

102 Hikvision Security Advisory FAQs, accessed 26th January 2022, https://www.hikvision.com/uk/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/faqs-command-injection-vulnerability/

103 Article on Hikvision Vulnerability CVE-2021-36260, Watchful_IP on Github, 18th September 2021, https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html#is-this-a-chinese-government-mandated-backdoor

104 L'Occhio del Dragone, RAI, 10th May 2021, https://www.rai.it/programmi/report/inchieste/Locchio-del-Dragone-91d2b796-2cb6-411f-a4ea-a261b6267396.html

105 L'Occhio del Dragone Transcript, RAI, 10th May 2021, lhttps://www.rai.it/dl/doc/1621017918431_occhio_dragone_report_ok.pdf

106 Il Ritorno del Dragone, Rai, 20th December 2021, https://www.rai.it/programmi/report/inchieste/Il-ritorno-del-dragone-428f747d-93fe-48f6-bb7e-10f60b8f4539.html

107 Il Ritorno del Dragone Transcript, Rai, 20th December 2021, https://www.rai.it/dl/doc/1640086902246_Il%20ritorno%20del%20dragone%20-%20di%20Giulio%20Valesini%20e%20Cataldo%20Ciccolella.pdf

There is no direct evidence in the public domain that Hikvison or Dahua provide data to the Chinese state or that their security vulnerabilities are exploited by Beijing. Allegations of such matters are appropriately national security issues for our security and intelligence agencies to consider. However, persistent security issues and the growing chorus of experts expressing concern about the security of the two companies' systems makes the dominance of the two brands in the UK all the more concerning.

Hikvision in School Toilets

Hikvision equipment is used in sensitive areas and in places where people have a heightened expectation of privacy all over the UK. In 2019, Smithdon High Shool in West Norfolk put cameras made by the Chinese state-owned firm in the school toilets, claiming they would protect student safety. The school said the cameras could only see the door and the sinks, that access to camera feeds was restricted and that CCTV in pupil toilets was "common".

Private sector use

Public bodies are not alone in using Hikvision and Dahua surveillance equipment – there are a large number of private businesses and even individual home owners who make use of the controversial companies' technology. There are thought to be hundreds of thousands of internet-connected cameras made by the two companies in the UK at the very least.

Analysis of data from Internet of Things search engine Shodan, which collates metadata from servers and web-connected products, found more than 180,000 networks of Hikvision and Dahua products openly connected to the internet in the UK. The true number of devices is likely to be much larger as each network may contain multiple cameras and there will be many devices not connected to the open internet or not online at all.

Hikvision IP Cameras found on Shodan, Top 5 Cities

UK Wide Total	164,000+
London	27,000+
Birmingham	6,000+
Manchester	4,900+
Sheffield	4,400+
Leeds	3,300+

All Dahua tagged products on Shodan, Top 5 Cities

UK Wide Total	14,000+
London	3,200+
Birmingham	460+
Manchester	400+
Liverpool	270+
Sheffield	230+

There is much less known about which private organisations use CCTV made by the two companies or what capabilities they have as they are not subject to transparency rules, such as the Freedom of Information Act.

Big Brother Watch has identified the Hikvision being used on these companies' premises:

- Tesco

- Starbucks branches* [108]

- Southern Co-Op

- The Co-Operative Food

- Royal Botanic Gardens

- Burger King branches*

- Dominos Pizza branches*

- Costa*

- McDonald's*

Dahua is used at:

- PetsCorner

* May be franchised outlets.

108 FLA Fire & Security Facebook post, 5th February 2021, https://webcache.googleusercontent.com/search?q=cache:Eu9UESSmGD8J:https://ne-np.facebook.com/1981878598784402/posts/another-starbucks-completed-up-redditch-kit-supplied-by-dvs-ltd-hikvision-ip-cct/2573478572957732/+&cd=2&hl=en&ct=clnk&gl=uk

Southern Co-Op's Facial Recognition Watchlist

The Southern Co-Operative uses Hikvision cameras with a facial recognition system active in at least 35 shops developed by private surveillance company FaceWatch.[109] Hikvision cameras scan customers' faces as they enter the store and software developed by FaceWatch compares these to a secret watchlist complied by the Southern Co-Op and FaceWatch, alerting staff to any potential matches.

Photos are not provided by the police and instead, the Southern Co-Op itself saves CCTV images of customers alleged by staff as being involved in theft or antisocial behaviour. The company has refused to give details about how accurate the system is or the results it has yielded. Although the Southern Co-Op says it keeps images of alleged suspects to itself, FaceWatch claims that all its subscribers share images of subjects of interest with one another via the system across a range of between 8 miles (in London) or up to 43 miles in very rural areas.[110]

FaceWatch requires an HD IP CCTV camera that can send its video feed over the internet to the company's cloud where the facial detection algorithms run, meaning that other organisations could use other camera brands.[111] It is unclear whether a Hikvison IP camera would still also connect to Hikvision or not.

109 Co-op supermarkets are using facial recognition cameras made by Chinese state-owned company 'to track its shoppers', The Mail on Sunday, 15th January 2022, https://www.dailymail.co.uk/news/article-10406421/Co-op-using-cameras-Chinese-state-owned-company-track-shoppers.html
https://www.facewatch.co.uk/
https://www.facewatch.co.uk/wp-content/uploads/2020/03/Facewatch-Single_page_fact_sheet-v1b.pdf

Conclusion

Over the past 20 years, the UK has become a surveillance state. The UK's CCTV coverage per capita is exceeded only by China, and the renewed legal framework for investigatory powers permits the most intrusive surveillance of any democracy in history.

The technology-enabled human rights abuses in China should prompt policy-makers and the public alike to review the rights and security risks of mass surveillance architecture, and to deeply consider the legal and ethical standing of dealing with the specific companies involved in those atrocities.

Our investigation has uncovered that over 60% of public bodies in the UK currently operate Chinese state-owned surveillance cameras – from councils, to schools, universities and hospitals. The mass scale coverage is staggering and shows that these companies dominate the UK's surveillance architecture. We have also shown that, as a result, Chinese-pioneered advanced analytical capabilities ranging from behavioural analysis to object detection are being normalised in the UK's CCTV, despite remarkably little public or political knowledge.

The sale and operation of Hikvision and Dahua cameras in the UK raises a range of legal questions, from compliance with the Data Protection Act to the Modern Slavery Act. It poses a serious question about how Britain views the right to privacy in a period of rapid technological development, and the security and liberty the British public should be entitled to. Further, it poses a question about the UK's integrity and duty to avoid complicity with actors involved in crimes against humanity.

Therefore, we **recommend a ban on the sale and operation of Hikvision and Dahua surveillance equipment in the UK and we condemn their involvement in technology-enabled human rights abuses in China.**

Further, we call on the Government to commission an independent national review of the scale, capabilities, ethics and rights impact of modern CCTV in the UK.

Appendix: Detailed Findings

Education

Schools Raw

Number of Requests	Responses	Refused	Use Hikvision	Use Dahua	Other/un-confirmed Chinese CCTV brand
3343	676	13	352	45	43

Schools Percentages

Hikvision and/ or Dahua %	Hikvision %	Dahua %
57.3%	52.2%	6.7%

Schools Advanced Capabilities

Total[112]	Face Detecting	Thermal Scanning	Demographic Detection	Behavioural Analysis	Object Detection
72	45	17	14	28	37

112 It may be less than the sum of the capabilities as some public bodies have several advanced capabilities

Schools by Region

Region	Total Schools	Responses	Total Hik and/or Dahua	% Hik and/or Dahua	Hikvision	% Hikvision	Dahua	% Dahua
North East	176	34	20	58.8%	18	52.9%	3	8.8%
North West	457	107	55	51.4%	51	47.7%	6	5.6%
Yorks & Humber	312	68	48	70.6%	46	67.6%	2	2.9%
East Midlands	287	56	38	67.9%	38	67.9%	0	0%
West Midlands	408	63	34	54%	29	46.%	8	12.7%
South East	498	78	44	56.4%	39	50%	5	6.4%
South West	334	74	38	51.4%	32	43.2%	9	12.2%
London	492	124	70	56.5%	65	52.4%	7	5.6%

Further Education Colleges Raw

Number of Requests	Responses	Refused	Use Hikvision	Use Dahua
324	74	8	40	7

Further Education Colleges Percentages

Hikvision and/or Dahua %	Hikvision %	Dahua %
66.2%	54.1%	9.5%

Further Education Colleges Advanced Capabilities

Total[113]	Face De-tecting	Thermal Scanning	Demograph-ic Detection	Behavioural Analysis	Object Detection
13	8	7	1	1	3

113 It may be less than the sum of the capabilities as some public bodies have several advanced capabilities

Analysis

Of the roughly 20% of schools who responded to our Freedom of Information request with information on their use of Chinese CCTV, 57% said they use Hikvision or Dahua surveillance equipment.

Extrapolating from these findings and even allowing for a lower proportion of the remaining schools to say they use CCTV from the two companies it is fair to conclude that a huge proportion of children in the UK are caught on cameras made by companies implicated in human rights abuses and subject to warnings from numerous cybersecurity experts every time they go to school.

If only half of the remaining schools [a 12.5% drop in users compared to respondent schools] use Hikvision or Dahua we would expect to find the number of schools using the Chinese brands exceeding 1,700.

The data does not tell us how common IP cameras, which pose the biggest risk to security and privacy, are in schools, but with internet-connected cameras now making up the bulk of both companies' catalogues it is fair to assume IP cameras are used in a large share of the 380 schools with Chinese-made equipment.

With vulnerabilities in both companies and suggestions that some Hikvision cameras connect to China, and in the light of the obvious links to atrocities, parents should be questioning if these cameras are appropriate to watch their children.

One in six schools using Chinese state-owned CCTV admitted to having some kind of advanced capabilities, a number that is likely to be an underestimate as many Hikvision and Dahua products have these tools as standard even if users are not aware of them. A large proportion of schools that were aware of possessing advanced capabilities, particularly those with facial recognition, told us that they do not use them.

Of the schools who did not deny using algorithmic CCTV, one admitted to having face mask detecting tools while another said its surveillance equipment could search footage by clothing colour and even automatically detect fights. Several schools also said they had specifically brought in thermal scanning cameras in the wake of the pandemic.

Even in small numbers, the automated monitoring of children is an alarming prospect the fact that a significant proportion of schools have these capabilities, that could be used in the future, undermines the ability of children to feel comfortable without knowing they are being spied on by an algorithm.

The regional differences in the data were surprising even if some of the disparity would be ironed out by greater response rates. Almost three in five schools across England use Dahua or Hikvision, but in Yorkshire that jumps to more than seven in ten. The figure in the North West is much lower at 51 per cent. There was also a gap in brand popularity with one in eight south western schools using Dahua but none in the East Midlands, from our responses. There is no obvious reason for these differences at a regional level but may inform campaigners wanting to affect change in their areas.

Further Education colleges reflect a much smaller set of institutions but our FOI data suggests that they are more likely to use Hikivison and Dahua than secondary schools. They are also significantly more likely to have facial detection and thermal scanning capabilities, while 17% have some advanced tools, compared to 10% of schools - perhaps reflecting the fact FE pupils are much closer to adulthood. However, once again there are questions about whether these capabilities need to exist in an educational setting.

Universities

Universities Raw

Number of Requests	Responses	Refused	Use Hikvision	Use Dahua
149	91	18	44	5

Universities Percentages

Hikvision and/ or Dahua %	Hikvision %	Dahua %
53.8%	48.4%	5.5%

Universities Advanced Capabilities

Total[114]	Face Detecting	Thermal Scanning	Demographic Detection	Behavioural Analysis	Object Detection
19	3	1	1	3	5

Analysis

Universities appear to use Hikvision and Dahua at slightly lower rates than other educational settings. However, the companies still have cameras on more than half of campuses. The concerns are broadly similar to those about the two brands in general. However, there is the additional factor of the large international community at most universities. If the connections to Chinese servers and other security backdoors are or become tools for state-sponsored actors, the ability of international students of Uyghur backgrounds and other oppressed minorities to remain safe could be threatened.

114 It may be less than the sum of the capabilities as some public bodies have several advanced capabilities

Councils

Data on local authorities were collected in co-operation with Free Tibet, which campaigns for human rights in the Tibetan region. These figures reflect shared data and where a disparity was found it has been assumed that any affirmative answer is correct. Free Tibet's co-operation has been invaluable in holding some councils to account and making sure we received the correct information.

Councils Raw

Number of Requests	Responses	Refused	Use Hikvision	Use Dahua
420	343	18	227	35

Councils Percentages

Hikvision and/or Dahua %	Hikvision %	Dahua %
73.2%	66.2%	36%

Councils Capabilities

Total[115]	Face Detecting	Thermal Scanning	Demographic Detection	Behavioural Analysis	Object Detection
24	12	6	6	7	15

115 It may be less than the sum of the capabilities as some public bodies have several advanced capabilities

Councils by Region

Region	Number	Responses	Hikvision	Hikvision %	Dahua	Dahua %	Hikvision or Dahua	Hikvision and/or Dahua %
East Midlands	40	31	21	67.74%	4	12.9%	23	74.19%
East of England	51	42	28	66.7%	4	9.52%	33	78.57%
London	33	31	18	58.1%	0	0%	18	58.1%
North East	33	25	18	72%	2	8%	20	80%
North West	44	36	21	58.33%	1	2.78%	22	61.11%
Northern Ireland	20	10	9	90%	3	30%	10	100%
Scotland	30	29	27	93.1%	4	13.79%	28	96.55%
South East	75	64	42	65.63%	3	4.69%	45	70.31%
South West	39	27	16	59.26%	6	22.22%	19	70.37%
Wales	22	20	11	55%	4	20%	14	70%
West Midlands	33	28	17	60.71%	5	17.86%	19	67.86%

Analysis

Unsurprisingly cash-strapped councils who monitor huge swathes of public space in Britain operate large numbers of cameras made by Hikvision and Dahua. With three-quarters of local authorities using one of the two large brands, there are few places in the UK where it is possible to walk down the high street without a council-owned CCTV camera made by a company part-owned by the Chinese state watching. Once again, there are no figures on whether internet-connected cameras are used in each area or not.

These findings show that the vast majority of the population are subject to surveillance by cameras linked to persecution. There are some interesting regional differences with near-total coverage from Scottish and Northern Irish local authorities, excluding those who did not answer or refused to answer Big Brother Watch's requests. Some parts of England, including London, appear to have a lower, but still significant, saturation of cameras made by the two companies.

Invasive advanced capabilities are less common than in schools but there are still some councils with face detecting cameras monitoring their constituents. Our findings did yield the occasional concerns, with Tower Hamlets in London saying they do not use Hikvsion

due to human rights concerns while Dacorum in Hertfordshire noted they do use some older models while not buying new ones going forward.

Of the 5 local authority areas with the highest population of people of Chinese descent, according to the UK census, only Manchester and Glasgow used Hikvision or Dahua with Barnet in London and Birmingham both saying they do not.[116]

With Hikvision and Dahua being cheap it is not shocking that many councils use them but these findings underline just how hard it is to avoid the glare of the controversial Chinese-state owned CCTV companies while in any public space in the UK.

116 Chinese Ethnic Facts and Figures, UK Government, 27th January 2020, https://www.ethnicity-facts-figures.service.gov.uk/summaries/chinese-ethnic-group

NHS Trusts

Response rates for NHS Trusts were low. However, this FOI campaign was done as coronavirus cases spiked in the UK and there was an acknowledgement from many trusts that these pressures could delay FOI responses significantly.

NHS Trusts Raw

Number of Requests	Responses	Refused	Use Hikvision	Use Dahua
208	58	8	30	5

NHS Trusts Percentages

Hikvision and/ or Dahua %	Hikvision %	Dahua %
60.3%	51.7%	8.6%

NHS Trusts Capabilities

Total[117]	Face Detecting	Thermal Scanning	Demographic Detection	Behavioural Analysis	Object Detection
11	5	3	2	1	5

Analysis

NHS trusts use equipment from the two companies at a level that closely mirrors the findings for the public sector as a whole. However, like in schools there is a particular vulnerability to many of the people who may get caught on these cameras due to their health status and hospitals are another environment where the privacy risks of equipment made by the two brands and the context of their use in Xinjiang provides for an alarming contrast.

Some particular examples of how Hikvision tools are used in hospitals are particularly shocking. At the entrance to accident and emergency at a west London hospital over the winter, there was a large Hikvision camera that was linked to a screen that looked to show facial detection. A specialist hospital, in north west London, makes use of Hikvision thermal

117 It may be less than the sum of the capabilities as some public bodies have several advanced capabilities

surveillance technology that is embedded as part of a walk through metal detector.

Whilst hospitals can be targets for crime, intimidatory surveillance can result in anxiety for patients and undermine the privacy most people expect when entering a hospital.

Police

Police Raw

Number of Requests	Responses	Refused	Use Hikvision	Use Dahua
47	44	4	15	0

Police Percentages

Hikvision and/ or Dahua %	Hikvision %	Dahua %
34.1%	34.1%	8.6%

Analysis

One in three police forces uses Hikvision equipment for some purpose, whether general monitoring or ANPR. This is an alarming figure when considered alongside the fact that Hikvision and its equipment are intrinsically linked to abuses by law enforcement in Xinjiang. If hostile actors wanted to monitor sensitive situations and areas in the UK, accessing police-run CCTV systems would be an excellent place to start.

Unfortunately, little is known about whether the 15 police forces which use Hikvision have cameras with advanced capabilities as Big Brother Watch's questions about facial recognition and other AI-driven tools were mostly met with refusals to answer under a range of FOI exemptions.

Two of the UK's biggest police forces, the Metropolitan Police and Greater Manchester Police, were unfortunately among those who refused to answer any of the questions put to them about whether they used Hikvision at all.

Government Departments

Number of Requests	Responses	Refused	Use Hikvision	Do Not Use Hikvision	Do Not Know
19	16	10	1	2	3

Analysis

Freedom of Information Requests to all 19 Government departments asking for lists of Hikvision products they use and any relevant contracts for were sent in late October 2021.

Only the Department for Work and Pensions confirmed it used Hikvision-supplied CCTV but declined to give further details about any additional capabilities.

Four departments still have not responded to the requests while the Attorney General's Office, the Scottish Office and the Department for International Trade all held no information as the Government Property Agency, an arm of the Cabinet Office, manage their buildings.

The Welsh Office and the Department for Levelling Up, Housing and Communities said their departments do not use Hikvision equipment.

Seven departments, including the Cabinet Office, refused the request citing national security grounds and did not disclose any information. This also included the Treasury, the Northern Irish Office and the Education, Health, Environment and Business departments. The Ministries of Defence and Justice, and Home Office relied on cost grounds to refuse the request.

Other coverage of Chinese CCTV at the heart of government has previously uncovered that the Ministry of Justice and Department of Health both do operate Hikvision equipment, in addition to the Department for Work and Pensions.[118] The Freedom of Information Requests, submitted by Free Tibet who have worked with Big Brother Watch on parts of this investigation, suggest that the DWP's Hikvision equipment is used at many JobCentre Plus sites across the country.[119,120]

118 UK Ministry of Defence "Guidance Is Not To Use / Install Hikvision", IPVM, 22nd November 2021, https://ipvm.com/reports/uk-mod-no-hik

119 https://s.ipvm.com/uploads/embedded_file/acb0257059b1ce3991571311069eb384c54cfdd458ac89b5328865a922182e53/12b8d166-5dc5-4aab-920d-f645ea5c38c4.pdf

120 https://s.ipvm.com/uploads/embedded_file/

It is also known that both Hikvision and Dahua provide significant amounts of hardware for other large CCTV manufacturers such as Honeywell, which may mean that equipment made by these two companies could have found its way into Whitehall under a different logo. One such camera was identified at the Home Office's Marsham Street headquarters in late 2021 which lead to the ostensibly Honeywell branded piece of equipment, mostly made by Dahua, being quickly removed.[121]

d4edf959f9bafe76c7ec585d79d2478960f65d183f728e041c3ea19276684839/f2dfb5d4-4b83-400d-82eb-c1d599be03e0.pdf

121 Whitehall security scare after discovering CCTV in London HQ was made by Chinese firm Dahua, The Mail on Sunday, 21st November 2021, https://www.dailymail.co.uk/news/article-10225833/Whitehall-security-scare-discovering-CCTV-London-HQ-controversial-Chinese-firm.html