Hikvision Amendment Briefing

The amendment

> To move the following Clause— "Removal from the procurement supply chain of physical surveillance equipment produced by companies subject to the National Intelligence Law of the People's Republic of China
>
> (1) Within six months of the passage of this Act, the Secretary of State must publish a timeline for the removal from the Government's procurement supply chain of physical surveillance equipment produced by companies subject to the National Intelligence Law of the People's Republic of China.
>
> (2) The Secretary of State must lay the timeline before Parliament."

Overview

The world's largest manufacturers and suppliers of video surveillance equipment are companies owned by the Chinese government, Hikvision and Dahua. The Chinese government has utilised Hikvision and Dahua surveillance technology to facilitate its mass-crackdown on the Uyghur population and transform the Region into a 'high-tech penal colony'.[1] Hikvision and Dahua are subject to the National Intelligence Law of the People's Republic of China. Today, Chinese state-owned surveillance cameras are found across UK public buildings, putting UK society at risk of security breaches and complicity in genocidal crimes.

The Uyghur Genocide

Since 2017, the Uyghur people have been subjected to a campaign of surveillance, repression and genocide at the hands of the Chinese government. Satellite images, drone footage, leaked documents and testimonies from concentration camp survivors have exposed that Uyghur people do not have access to basic cultural and religious freedoms or fundamental human rights. In December 2021, an independent Uyghur Tribunal determined that the Chinese government's policies amount to torture, crimes against humanity and genocide.

Hikvision/ Dahua's surveillance technology's role in the persecution of the Uyghurs

Hikvision and Dahua have signed contracts worth at least $1.2 billion for 11 separate, large-scale surveillance projects across the Uyghur region. The companies are contracted to develop, install and operate CCTV technology across the region's public checkpoints, mosques, factories and network of concentration camps.

Both Hikvision and Dahua have advertised "ethnic minority" detection software, which is able to 'automate the identification of Uyghur faces based on physiological phenotypes' and track their

[1] Byler, Darren. *In the Camps: Life in China's High-Tech Penal Colony*. Atlantic Books, 2022.

movements. This intelligence is used to substantiate the arbitrary detention of Uyghurs and other Turkic ethno-religious groups in the Region.

Mass-surveillance has a devastating impact on the psychological wellbeing of the Uyghur population. A former employee of a state-owned surveillance firm in the Region claims that every person he encountered who'd been subjected to this digital surveillance, 'would criticize their own behaviour … instead of directing hatred towards the Chinese authorities.' He believes that the infrastructure was designed 'to install this [...] mindset in every Uyghur mind." Another Uyghur whistleblower describes how data collection 'haunts' the lives of the community: '"Uyghurs are alive, but their entire lives are behind walls…it is like they are ghosts living in another world."[2]

Testimony from survivors:

Abdurehim*, a young Uyghur concentration camp survivor, on how surveillance is used to control behaviour within the Region's network of concentration camps*:*

> *In the camps, 'we were not allowed to move. Because of the cameras we had no option but to sit still and wait. If someone moved or spoke and they would be seen by the police and they would come, take the person away and torture them. This happened to me."*

Ali … on how surveillance cameras are operationalised in the camps:

> *''They deliberately place Uyghurs in one place, the cameras in the cell record everything round the clock, and automatically translate the recordings into Chinese"*

Adil*, a former employee of a Chinese surveillance company on the psychological impact of mass-surveillance:

> *"Psychologically (this system) makes people think that they themselves are criminals and guilty. In reality, this system has no ability to identify if someone is guilty of crime or not."*

The National Security Risk

Hikvision and Dahua are both subject to China's National Intelligence Law which stipulates that "any organisation or citizen shall support, assist, and cooperate with state intelligence work according to law."[3] The law also permits authorities to detain or criminally punish those who "obstruct" intelligence activities.[4] The presence of vendors who are subject to extrajudicial directions from a

[2]https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition
[3] https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/
[4] https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

foreign government, which conflict with UK law, may risk failure by the carrier to adequately protect networks from unauthorised access or interference.[5]

Hikvision's presence in the UK

Research undertaken by Big Brother Watch has revealed the ubiquity of Hikvision cameras across the UK's public buildings. As of 2020, over half of NHS trusts, one third of police forces and 60% of schools were using CCTV implicated in the Chinese government's human rights abuses.[6] The UK's Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner, review on UK surveillance systems found that the procurement of unethical surveillance systems has produced a legacy akin to a 'digital asbestos' within the UK's public surveillance infrastructure.[7] Sampson calls on the UK government to implement a 'moratorium on any further installation' until forensic due diligence has been undertaken.[8]

Policy responses

There is a growing global legislative agenda to tackle the exportation of unethical surveillance tech. In 2020, the US banned the import or sale of Hikvision and Dahua telecoms and video surveillance products, in response to the security concerns outlined above.[9] The EU[10] has now removed Hikvision cameras from their parliaments and in February this year Australia stripped its cameras from its defence sites.[11]

So far, the UK has committed to removing Hikvision and Dahua CCTV from government buildings at the cessation of their contracts. Councils across Wales, Scotland and Kent have independently pledged to terminate their contracts with surveillance companies that are subject to the Chinese national security laws. Despite this positive momentum, this year the government rejected Lord

---

[5] https://www.cnbc.com/2018/08/23/huawei-and-zte-banned-from-selling-5g-equipment-to-australia.html

[6] https://bigbrotherwatch.org.uk/campaigns/ban-hikvision/

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135384/Biometrics__Surveillance_Camera_Commissioner_Annual_Report_21-22.pdf

[9] https://www.forbes.com/sites/emmawoollacott/2022/11/28/us-bans-chinese-telecom-kit-over-national-security-concerns/

[10] https://ipvm.com/reports/hik-eu

[11] https://www.bbc.co.uk/news/world-australia-64577641

Alton's 'Hikvisoin' amendment to the Procurement Bill, claiming that the evidence linking Hikvision and Dahua to egregious human rights abuses is 'highly contested.'[12]

As it stands, the government's policy is insufficient to tackle the scale of the problem. Not only does this strategy fail to protect sensitive sites which fall outside the government's remit, including police stations, councils, military bases and educational institutions, it also does little to address the huge amount of public money being funnelled into companies with known complicity genocide.

Why support this amendment?

1) **Scope:** This amendment would ban **all UK institutions** from procuring surveillance technology from companies that are subject to the National Intelligence Law. This extends the scope of the current legislation to schools, hospitals and military bases, protecting a host of vulnerable sites from security breaches and data infringement.

2) **Urgency:** This amendment calls on public bodies to terminate their contracts with relevant companies within 6 months of its passage. As things stand, government departments are not required to rip out unethical surveillance tech until the contracts' cessation date. This puts long-term contract-holders at risk of security breaches for up to *four years.*

3) **Global leadership:** This amendment offers the UK an opportunity to become a world leader in this crucial area of national security. If passed successfully, the UK would be the first European country to take authoritative action to tackle the importation of surveillance technology complicit in human rights abuses.

4) **Protection of consumers and citizens:** This amendment would stop a significant proportion of the British taxpayers money being funnelled into the development of technology which strips minoritised groups of their most basic human rights.

   Furthermore, reducing exports would cut off a vital lifesource of this technology and would go someway to limiting the Chinese government's development and exportation of increasingly invasive technology. This ultimately safeguards UK citizens from future infringements on their right to privacy and data protection.

[12]https://hansard.parliament.uk/commons/2023-02-07/debates/237d01ac-578d-4083-8ad3-1b53bf032d78/ProcurementBill(Lords)(SixthSitting)