BIG BROTHER WATCH

Big Brother Watch briefing on the Procurement Bill for Committee Stage in the House of Commons

January 2023

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 technological 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

Mark Johnson

Advocacy Manager

Direct line: 020 8075 8479

Email:mark.johnson@bigbrotherwatch.org.uk

Madeleine Stone

Legal & Policy Officer

Direct line: 07864733785

Email: madeleine.stone@bigbrotherwatch.org.uk

INTRODUCTION

We welcome the opportunity to provide this briefing to the Public Bill Committee for the Procurement Bill. Big Brother Watch believes that the Bill provides a vital opportunity for parliamentarians to protect the security and privacy of people in the United Kingdom from the serious risks posed by surveillance technology made by human rights-abusing foreign states.

The House of Lords passed a cross-party amendment to the Procurement Bill (Clause 65) which seeks to instigate the removal of technology and surveillance equipment where the provider has been involved in significant human rights abuses. We welcome this amendment and believe Clause 65 is a legislative landmark that both protects the security and privacy of people in the UK, and demonstrates the UK's intolerance of human rights atrocities overseas.

The Government has tabled an amendment (Amendment 49) which seeks to remove Clause 65. Members of the Committee should vote against this amendment.

Clause 65

Following the cross-party amendment, Clause 65 of the Procurement Bill requires that within 6 months of the passing of the Act, the Secretary of State must lay before Parliament a timeline for the removal of physical technology or surveillance equipment from the Government's procurement supply chain where the Secretary of State is satisfied there is established evidence that a provider has been involved in modern slavery, genocide, or crimes against humanity.

BRIEFING

What human rights abuses are Chinese state-owned surveillance companies linked to?

The Chinese government is pursuing the genocide of ethnic minorities, as declared by the House of Commons, the US, Canada and Holland.[1] Former Prime Minister Liz Truss also reportedly described the situation as a genocide,[2] as has US Secretary of State Antony Blinken.[3] The UN, Amnesty International and Human Rights Watch have warned

1 Uyghurs: MPs state genocide is taking place in China – BBC News, 23rd April 2021: https://www.bbc.co.uk/news/uk-politics-56843368
2 Liz Truss pulls no punches about 'genocide' of Uighurs by China – Matt Dathan, The Times, 1st November 2021: https://www.thetimes.co.uk/article/liz-truss-pulls-no-punches-about-genocide-of-uighurs-by-china-q8z90l798
3 UN Office of the High Commissioner for Human Rights Report on the Human Rights Situation in Xinjiang: Press Statement - Antony J. Blinken, Secretary of State, 1st September, 2022: https://geneva.usmission.gov/2022/09/01/statement-on-un-human-rights-office-report-on-xinjiang/

of the CCP's "crimes against humanity", including about the ways in which many of the atrocities are technology-enabled.

Chinese state-owned surveillance companies Hikvision and Dahua provide technology that is central to the regime of ethnic persecution of the Uyghur population in Xinjiang and both hold contracts to build and operate surveillance systems in the region.[4] Big Brother Watch has documented the companies' links to genocide and the operation of concentration camps in China extensively in our report, *Who's Watching You? The dominance of Chinese state-owned CCTV in the UK*.[5] Some of their surveillance technology's features, such as facial recognition and "Uyghur detection"/ethnicity recognition, directly enable the atrocities committed by the Chinese government.

In the Lord's Report Stage debate on the Procurement Bill, Lord Alton criticised the companies'

> "*(...) links to the internment camps in Xinjiang and their role working hand-in-glove with the CCP to construct the largest authoritarian surveillance state, which has surpassed even George Orwell's wildest dreams.*"[6]

The Foreign Affairs Committee's report on the UK's responsibility to act on crimes against humanity in Xinjiang, Never Again, concluded that these companies were involved in "technology-enabled human rights abuses" and should be banned in the UK.

What security risks could these companies pose?

Surveillance technology can pose risks to national security through hacking, technical vulnerabilities, or security 'back doors'. The Government's Biometrics and Surveillance Camera Commissioner, Professor Fraser Sampson, has repeatedly warned of the security and ethical risks posed by Hikvision and Dahua and describes their surveillance products as "digital asbestos".[7]

The security risks associated with Chinese state-owned surveillance companies Hikvision and Dahua are well-documented by security researchers, including in our

4 Hikvision, Xinjiang, Uyghurs & Human Rights Abuses – IPVM, Conor Healy, 17th May 2022: https://s.ipvm.com/uploads/eab3/fcde/Hikvision%20IPVM%20White%20Paper.pdf; Dahua Operates China Police Surveillance – Charles Rollet, IPVM, 14th Apriln2021: https://ipvm.com/reports/dahua-police

5 *Who's Watching You? The dominance of Chinese state-owned CCTV in the UK* – Big Brother Watch, 7th February 2022, p.26-30: https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-1.pdf

6 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col.1817

7 National security fears over police using Chinese tech – Fiona Hamilton, The Times, 2nd January 2023: https://www.thetimes.co.uk/article/national-security-fears-over-police-using-chinese-tech-bl0wrj2kl

report *Who's Watching You? The dominance of Chinese state-owned CCTV in the UK*.[8] Such risks include incidences of cameras sending unauthorised signals to China.

As early as 2017, the US Department of Homeland Security gave Hikvision its worst score of 10 out of 10, warning that the low-cost cameras were "remotely exploitable/low skill level to exploit" for "improper authentication."[9]

As recently as September 2021, Hikvision admitted a serious 9.8 vulnerability in its cameras[10] after it was discovered by a security expert who described it as "the highest level of critical vulnerability".[11] The publication IPVM, which describes itself as "the world's leading authority on physical security technology", estimated that over 100 million surveillance cameras could be affected.[12]

Many of these unsafe cameras are likely to be in the UK. Lord Blencathra told the House of Lords he has received estimates that there are over 1 million Hikvision cameras in the UK.[13] Big Brother Watch's own research has found that Hikvision and Dahua are widely used across the UK's public sector.

- **61% of our public bodies use Chinese-made CCTV (Hikvision or Dahua)**
- More than 10% of public bodies using this CTTV had advanced CCTV capabilities, including thermal scanning or facial detection
- 63% of schools, 66% of colleges and 54% of universities use Chinese-made CCTV
- 35% of police forces use Hikvision cameras
- 60% of NHS trusts use Chinese-made CCTV
- 73% of local authorities use Chinese-made CCTV.[14]

8 *Who's Watching You? The dominance of Chinese state-owned CCTV in the UK* – Big Brother Watch, 7th February 2022, p.26-30: https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-1.pdf

9 ICS Advisory (ICSA-17-124-01) – Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security, 4th May 2017: https://www.cisa.gov/uscert/ics/advisories/ICSA-17-124-01; see also Hikvision Backdoor Confirmed – Brian Karas, IPVM, 8th May 2017: https://ipvm.com/reports/hik-backdoor

10 Security Notification - Command Injection Vulnerability in Some Hikvision products – Hikvision, 19th September 2019: https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/security-notification-command-injection-vulnerability-in-some-hikvision-products/

11 Unauthenticated Remote Code Execution (RCE) vulnerability in Hikvision IP camera/NVR firmware (CVE-2021-36260) – Watchful_IP, 18th September 2021: https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html

12 Hikvision Has "Highest Level of Critical Vulnerability," Impacting 100+ Million Devices – John Honovich, IPVM, 20th September 2021: https://ipvm.com/reports/hikvision-36260

13 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1817

Lord Alton warned the House of Lords:

> "*(...) we have allowed our surveillance and technology supply chain to be dominated by Chinese surveillance companies with credible links to the genocide taking place in the Uighur region.*"[15]

Lord Alton further questioned:

> "*Do we really want the prying eyes of an authoritarian state that has been accused of genocide, (...)in our schools, hospitals, and local council buildings? Similarly, how can the Government justify public contracts and taxpayers' money going into companies where there are credible links of complicity in genocide and the internment camps in Xinjiang?*"[16]

Lord Blencathra drew attention to the legal obligations Chinese technology companies have to the Chinese government:

> "*After all, Hikvision and Dahua cannot be considered to be anything like normal private business companies operating in a free-market economy. Both not only receive generous subsidies from the Chinese state but under Article 7 of China's national intelligence law they are expected to work hand in glove with the state.*"[17]

Article 7 of China's National Intelligence Law states, "Any organisation or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work."

Further, Article 28 of China's Cybersecurity Law states, "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."

Article 11 of China's National Security Law states, "All citizens of the People's Republic of China .... shall have the responsibility and obligation to maintain national security."

As Lord Blencathra warned:

14 *Who's Watching You? The dominance of Chinese state-owned surveillance in the UK* – Big Brother Watch, 7th February 2022, p. 8-9: https://bigbrotherwatch.org.uk/wp-content/uploads/2022/02/Whos-Watching-You_The-dominance-of-Chinese-state-owned-CCTV-in-the-UK-17746.pdf
15 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col.1816
16 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col.1817
17 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1821-1823

> "*In effect, these companies are not only required by China's national intelligence law to help assist with national intelligence work, but they are bound to secrecy not to reveal the extent of their collaboration with Chinese intelligence services.*"[18]

It is vital that such companies, clearly linked to human rights abuses overseas and security risks domestically, should be debarred from our procurement supply chains.

The threats posed by the Chinese government to the UK and the international community are well recognised. The Prime Minister Rishi Sunak recently stated:

> "*China unequivocally poses a systemic threat – well, a systemic challenge – to our values, and our interests, and is undoubtedly the biggest state-based threat to our economic security (...) That's why it's important that we take the powers that we need to defend ourselves against that.*"[19]

The national security risks posed by Chinese state-owned technology companies in particular have also been recognised and acted on in several jurisdictions, including recently in the UK. However, action in the UK has been inadequate.

What limited action has been taken in the UK, and how does it compare to other nations?

On 24th November 2022, the Government announced it will be removing surveillance equipment manufactured by Chinese state-owned companies from "sensitive sites" within Government departments, in recognition of the risk they pose to national security.[20] This is an important step, but the entirety of the public sector must be afforded the same protections. The national security risk posed by these companies, which has been acknowledged, also applies to the police stations, hospitals, council buildings and schools, where their technologies are widely used.

As Lord Coaker said during Report Stage in the House of Lords:

> "*(...) what about all the other cameras within local authorities, such as street cameras and cameras in hospitals? Do they not pose a security risk? If they do in a government department, I cannot see why they do not when they are outside one but happen to be run by Westminster council. This is ludicrous and illogical, and the Government need to take account of it. That is why [Clause 65] is so*

18 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1821-1823
19 Rishi Sunak calls China 'systemic challenge' - Jessica Elgot, the Guardian, 15 November 2022
20 Security Update on Surveillance Equipment – Written Statement, 24th November 2022, UIN HCWS386: https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386

important. (...) Everybody in your Lordships' House agrees with that; no one is opposed it."[21]

The Scottish Government has committed to "phasing out" Hikvision cameras,[22] while Edinburgh City Council plans to remove existing cameras.[23]

The US has already banned Hikvision and Dahua due to national security concerns.[24]

Additionally, the European Parliament has voted to remove Hikvision cameras from its buildings, citing "an unacceptable risk that Hikvision, through its operations in Xinjiang, is contributing to serious human rights abuses".[25]

In Denmark, the Capital Region Hovedstaden has discontinued the use of Hikvision cameras.[26]

High ethical and security standards are paramount when sourcing technology and surveillance equipment, given the potential impacts on security and human rights. The Government has announced its intention to be one of "the toughest regimes in the world for telecoms security" and has already taken important steps to ensure this, through the removal of Chinese state-owned firm Huawei from 5G networks.[27] However, there has been inadequate Government action against Chinese state-owned surveillance companies to date and in the Procurement Bill.

How could the Procurement Bill deal with these companies?

There was no simple mechanism by which suppliers linked with serious human rights violations such as Hikvision could be rejected under this Bill until the House of Lords' amendment, introducing Clause 65.

The Minister Baroness Neville-Rolfe rejected the amendment (now Clause 65), on the basis that the Procurement Bill introduces an exclusion ground on the basis of national security ground.[28] However, this is a discretionary exclusion ground (Schedule 7,

21 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1825
22 'Dangerous' Chinese CCTV cameras to be phased out in Scotland – Marck McLaughlin, the Times, 21st November 2022: https://www.thetimes.co.uk/article/dangerous-chinese-cctv-cameras-to-be-phased-out-in-scotland-ntnh29m96
23 Edinburgh council to tear down CCTV cameras linked to Chinese human rights abuse – Jacob Farr, Edinburgh Live, 28th October 2022: https://www.edinburghlive.co.uk/news/edinburgh-news/edinburgh-council-tear-down-cctv-25381201
24 Congress passes bill banning new FCC equipment authorizations for Hikvision, Dahua and others – Joel Griffin, Security Info 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
25 EU Parliament Removes Hikvision, Citing Human Rights Abuses – Charles Rollet, IPVM, 29th April 2021: https://ipvm.com/reports/hik-eu
26 Danish Capital Region Bans Hikvision Purchases, Calls "Critical Threat To Security" – Charles Rollet, IPVM, 28th September 2022: https://ipvm.com/reports/danish-capital?code=1
27 Huawei to be removed from UK 5G networks by 2027 – GOV.UK, 14th July 2020: https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027
28 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1827

paragraph 14). Furthermore, Clause 65 deals with companies involved in human rights atrocities – although it is likely that, relatedly, such companies will pose a security threat to the UK, it is not the sole or primary purpose for which companies could be debarred under Clause 65.

Indeed, despite the action taken by individual ministers to remove Hikvision cameras from their own departments,[29] it would appear that the Government does not intend to take the necessary action to remove Chinese state-owned companies' products from across the government estate. Another reason for which Baroness Neville-Rolfe rejected Clause 65 is the claim that it "seeks to interfere directly with security arrangements":

> "*In mandating a timeline for the removal of existing physical technology or surveillance equipment from the Government's supply chain, the amendment seeks to interfere directly with security arrangements on the government estate*."[30]

However, in light of the Government's own admission that Chinese state-owned surveillance companies pose a risk to British interests and the decision to remove such technology from sensitive sites, the effect of Clause 65 is to apply the same logic and afford a minimum level of security across the public sector. This is not an interference by Parliament, but a reflection of its duty to protect the British public.

Lord Alton stated during Report Stage in the House of Lords,

> "*I welcome the leadership that Ministers have shown recently in banning the use of Hikvision and Dahua cameras in government departments, but I urge them to consider applying that same leadership to the rest of the procurement supply chain*."[31]

Parliament and the public rightly expect that the Procurement Bill will offer a route by which to debar Chinese state-owned surveillance companies from the UK. The Government has previously stated:

> "*The forthcoming Public Procurement Bill will further strengthen the ability of public sector bodies to disqualify suppliers from bidding for contracts where they have a history of misconduct, including forced labour or modern slavery*"

29 DWP announces decision to remove Hikvision cameras – Big Brother Watch, 26th June 2022: https://bigbrotherwatch.org.uk/2022/06/the-telegraph-dwp-announces-decision-to-remove-hikvision-cameras/
30 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1827
31 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1815-1818

and that the Government was working to

> "*enable commercial teams to more effectively exercise their discretion to exclude suppliers linked with modern slavery and human rights violations.*"

This statement was repeated in response to a written parliamentary question on the use of "Chinese-made surveillance cameras" in the public sector in February 2022.[32] However, whilst modern slavery is referenced in the Procurement Bill, other serious human rights violations were not – until the House of Lords introduced Clause 65.

Is the Procurement Bill the right vehicle for measures to remove rights-abusive companies from existing and future procurement supply chains?

Opposing the amendment to introduce Clause 65, Minister Baroness Neville-Rolfe said that "The Bill is not concerned with existing equipment or kit which has already been installed, or with the termination of existing contracts by central government."[33] However, the amendment would require the Government to set out a timeline for removal of relevant companies from the supply chain; it does not necessitate the termination of contracts per se (although that may be advisable).

The wider question is whether the Procurement Bill is the right vehicle by which to set these basic ethical standards. Big Brother Watch supports the view of the majority of the House of Lords that the Procurement Bill is the right legislative vehicle by which to remove companies linked to the most serious human rights abuses from existing and future contracts.

The Procurement Bill is the vehicle by which the UK is setting values and principles to guide procurement for the future. In the Green Paper 'Transforming Public Procurement', the Government set out key principles for public procurement in the UK: value for money, public good, transparency, integrity, equal treatment and non-discrimination.[34] In particular, the Green Paper stated that 'public good' should support the delivery of strategic national security priorities, public safety and ethics. Consistent with international practice, the Green Paper further emphasised that "public procurement is regularly leveraged to achieve social and environmental value beyond the primary benefit of the specific goods, services and capital". Accordingly, Big Brother Watch believes that the Procurement Bill is a key opportunity to ensure

32 Written question: Lord Alton to Baroness Trafford, answered 22nd February 2022, UIN HL6066: https://questions-statements.parliament.uk/written-questions/detail/2022-02-08/hl6066
33 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1826
34 Green Paper: Transforming public procurement – GOV.UK, 6th December 2021: https://www.gov.uk/government/consultations/green-paper-transforming-public-procurement

that public sector procurement promotes at least the basic standard of rejecting companies involved in the most serious human rights abuses, as per Clause 65.

In the Report Stage debate in the House of Lords, Shadow Minister Lord Coaker said:

> "*Legislatively, we should say that we, as a UK Government and Parliament, believe these things are so important that they should be put in the Bill, that we hold to these international values, and that we will set an example for other countries to do the same and that our procurement policy will reflect this*."[35]

Agreeing on the importance of encoding procurement values into the Bill, Lord Hunt said:

> "*(...) this is a Procurement Bill, setting the regime for government procurement for a number of years ahead. Where better to place values—not just the issue of the lowest common denominator price—than in this Bill, which sets the parameters under which billions of pounds are going to be spent by government and government agencies over the next decade?*"[36]

CONCLUSION

Clause 65 represents a vital step towards ensuring that the procurement of technology meets high ethical standards. It seeks to target companies involved in the most serious violations of rights – those that should have no place in the UK's public sector.

The Procurement Bill is a key opportunity to remove Hikvision and Dahua from the public sector, where they pose significant ethical and security concerns. We urge Members of Parliament to use this opportunity by supporting Clause 65 to protect security and human rights in the UK.

35 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col.1824-25
36 Procurement Bill, Report Stage in the House of Lords, 30th November 2022, vol. 825, col. 1831