BIG BROTHER WATCH

General Election Briefing: 2024

1) Protect rights from facial recognition surveillance

1.1) Ban live facial recognition for generalised surveillance of public spaces

1.2) Strictly regulate retrospective facial recognition

2) No bank spying

2.1) Commit to reject mass bank spying for welfare or other purposes

2.2) Prevent mandatory invasive CBDCs

3) No censorship

3.1) Commission an independent inquiry into the government's counter disinformation units

4) No 2 ID

4.1) Commit to never propose mandatory ID or digital ID

5) Privacy for all

5.1) Protect workers from excessive employer surveillance

5.2) Build up data protection standards, not water down

5.3) Protect the Human Rights Act 1998

1) Protect rights from facial recognition surveillance

1.1) Ban live facial recognition for generalised surveillance of public spaces

1.2) Strictly regulate retrospective facial recognition

1.1) Live facial recognition (LFR) cameras biometrically scan the faces of every person that walks within the view of the camera – turning our streets into police line-ups. Police have increased their use of LFR by 1,000% in London, and high street retailers have started rolling out LFR with secret, non-police blacklists resulting in intrusion, discrimination and serious injustice.

A black community worker was recently misidentified by LFR and wrongly interrogated by the Met Police; whilst a teenager of Bangladeshi heritage was wrongly searched, publicly accused of being a thief and thrown out of a Home Bargains store after a LFR error. Both victims are now pursuing legal action.[1]

LFR is seriously ineffective and dangerously inaccurate, with particular issues identifying women and people of colour. 77% of all police LFR flags in the UK have been inaccurate[2] and only 0.03% scans resulted in an arrest. The £55m[3] of taxpayers' money planned for LFR would be better spent on traditional, targeted policing and crime prevention.

Whilst the EU AI Act significantly restricts uses of LFR to serious and targeted cases and requires primary legislation, judicial authorisation and oversight, the words "facial recognition" are not in a single Act of Parliament in the UK. The Equality and Human Rights Commission[4] and 130 rights groups[5], including Amnesty and Human Rights Watch, have called for a stop to LFR in the UK.

1.2) Retrospective Facial Recognition [RFR] biometrically compares still images or video recordings taken in the past. Police have created a giant, national facial recognition database by the backdoor, turning the population's passport photos into mugshots for biometric searches[6] – although, unlike DNA, fingerprints and other biometrics, there is no parliamentary or specific legal authority. If police make the case that RFR is a necessary forensic tool, parliament must legislate to limit searches to those strictly necessary where less intrusive methods fail and limit databases to serious crime and national security as per DNA.

2) No bank spying

2.1) Commit to reject mass bank spying for welfare or other purposes

2.2) Prevent mandatory invasive CBDCs

2.1) The Government attempted but failed to introduce powers to snoop on the nation's bank accounts, without suspicion, under the premise of tackling fraud and error in the welfare system in the Data Protection and Digital Information Bill. The

measures were a monumental threat to financial privacy, reversed the presumption of innocence, and put vulnerable people at risk. The plans met strong cross-party opposition including from the Information Commissioner, the Equality and Human Rights Commission, and UK Finance; over 40 privacy, equality, disability rights groups; and 270,000 petition signers who called on the Government to drop the powers[7]. The next government must reject bank spying.

2.2) Another threat to financial privacy is the development of a UK Central Bank Digital Currency (CBDC), which the Sunak government planned to pilot by 2025. CBDCs, which are typically linked to digital identities, can be incredibly invasive and exploited for intrusive surveillance by the state and Big Tech. CBDCs could also be 'programmable' meaning the potential for direct state control over the public's spending. Parliament's Economic Affairs Committee called the plan "a solution in search of a problem" and warned that digitising such national critical infrastructure would introduce serious security risks. 50,000 members of the public responded to the Government's consultation, raising privacy and inequality concerns.[8] If a UK digital pound is introduced it must not be mandatory and must be at least as privacy-preserving as cash.

3) No censorship

3.1) Commission an independent inquiry into the government's counter disinformation units

Disinformation is a problem - but it's also a term at risk of political exploitation. Big Brother Watch revealed that the UK government's secretive Counter "Disinformation" Unit (CDU) monitored opposition to government policies on social media - recording MPs, journalists, academics, and rights campaigners in secret "disinformation reports"[9]. The Unit flagged lawful speech to social media companies to be suppressed or censored. The government has been forced to apologise for some of its unlawful activity which it admitted was "not impartial".

Despite the Intelligence and Security Committee complaining of an "erosion of oversight"[10] over this and the Culture, Media and Sport Committee urging an independent review of the unit In April 2024,[11] the unit, now rebranded as the 'National Security and Online Information Team', is monitoring and flagging speech in the 2024 general election. Given the Unit has previously included MPs from all parties in its so-called 'disinformation reports', the ongoing lack of oversight into the work of this government body raises serious concerns.

4) No 2 ID

4.1) Commit to never propose mandatory ID or digital ID

Mandatory ID systems raise significant privacy and civil liberties concerns such as increased surveillance and tracking of individuals, abuse of people's private information, and restrictions on individual freedoms. Such systems could disproportionately affect marginalised communities, exacerbating inequalities. In light of the increasing emphasis upon digital ID and proving identity online, it is essential that individuals are not coerced into relying on digital ID and are able to access offline alternatives. In situations where proving identity is truly necessary, people must always have the choice of how they do so. The next Government must never propose mandatory ID cards, digital or otherwise.

5) Privacy for all

5.1) Protect workers from excessive employer surveillance

5.2) Build up data protection standards, not water down

5.3) Protect the Human Rights Act 1998

5.1) The TUC has warned of a huge lack of transparency over the use of AI at work; whilst automated decision making is increasingly being used in shift allocation, recruitment, line management, performance ratings, and deciding who is disciplined or made redundant. The majority of workers (60%) believe they have been subject to surveillance at their most recent job (Britain Thinks); and over half reported stress, anxiety and considered having to resign as a result (UNISON Scotland). The Post Office scandal shows that worker monitoring tech must be approached critically and with strong safeguards, to prevent intrusion and injustice. Unions and privacy groups agree that safeguards are missing – the next government must protect workers from excessive employer surveillance.

5.2) At a time when concern is rising about the threats of AI our data protection laws are more important than ever - but the last Parliament also saw these protections come under attack. The next Government must build our data protection standards up not water them down.

5.3) The last Parliament saw legal protections for our rights come under attack. The Human Rights Act formally enshrined the rights to free speech and privacy in UK law. Any attempt to tear up the HRA would undermine human rights in the UK.

1 https://bigbrotherwatch.org.uk/press-releases/landmark-legal-challenges-launched-against-facial-recognition-after-police-and-retailer-misidentifications/
2 See Metropolitan Police and South Wales Police live facial recognition deployment statistics.
3 https://www.theguardian.com/business/2024/apr/10/shoplifting-crackdown-to-include-55m-for-facial-recognition-tools-in-england-and-wales
4 https://www.equalityhumanrights.com/sites/default/files/2021/civil-and-political-rights-in-great-britain-march-2020.pdf, p.89
5 https://bigbrotherwatch.org.uk/press-releases/180-tech-experts-call-for-global-stop-to-facial-recognition-surveillance/
6 https://libertyinvestigates.org.uk/articles/police-secretly-conducting-facial-recognition-searches-of-passport-database/
7 https://www.theguardian.com/society/2024/mar/04/ministers-urged-to-scrap-plans-for-surveillance-of-benefit-claimants-bank-accounts
8 https://bigbrotherwatch.org.uk/press-coverage/the-telegraph-50000-people-respond-to-the-government-consultation-on-a-uk-cbdc/
9 https://bigbrotherwatch.org.uk/wp-content/uploads/2023/01/Ministry-of-Truth-Big-Brother-Watch-290123.pdf
10 https://isc.independent.gov.uk/wp-content/uploads/2023/12/ISC-Annual-Report-2022-2023-Press-Release.pdf
11 Trusted voices, House of Commons Culture, Media and Sport Committee Sixth Report of Session 2023–24, 26 March 2024, https://committees.parliament.uk/publications/44146/documents/219482/default/

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

Email: mark.johnson@bigbrotherwatch.org.uk