BIG BROTHER WATCH

Big Brother Watch briefing on 'Biometric data in schools' for the Welsh Senedd

March 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 Members of Senedd ahead of a debate on 8th March on the use of biometric data in schools.

We are concerned that schools across the UK, including in Wales, are **rolling out the use of intrusive new forms of biometric surveillance, with limited understanding of the data protection and privacy issues engaged by these technologies.**

The increasing use of biometric technologies threatens the privacy of children and young people as they develop. It creates greater opportunities to track an individual pupil's activity across multiple areas, from the library books they take out to the food they eat. Many of these technologies also have serious problems with accuracy and bias, and normalise the collection and retention of deeply sensitive data at a young age.

FAILURE TO MEET LEGAL OBLIGATIONS

Schools and local authorities are vulnerable to the sales pitches of technology companies, who promise that their products will lead to increased efficiency and cost savings. **In our engagement with schools around their use of biometric technologies, we have found that they are often unaware of their obligations under data protection law, and have failed to adequately inform pupils and parents of their data rights.**

The Protection of Freedoms Act 2012 sets out the requirements for processing children's biometric data in schools in England and Wales. Critically, the Act requires written consent from a parent or carer in order for schools to process pupils' biometric data. Schools must also provide an alternate means of accessing the service that does not require the processing of biometric data.

However, a Survation poll conducted in 2018 on behalf of Defend Digital Me found that of parents whose children's schools were using biometric technology, **38% said they had not been offered any choice, and over 50% had not been informed how long the fingerprints or other biometric data were retained for,** or when they will be destroyed.[1] Additionally, Defend Digital Me has found examples of schools where the use of biometric technologies is mandatory for all pupils, or where pupils who qualify for Free School Meals are required to use a biometric system in order to receive their lunch, while other pupils can choose not to use it.[2]

1 The state of biometrics 2022: A review of policy and practice in UK education – Defend Digital Me, May 2022: https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf

2 The state of biometrics 2022: A review of policy and practice in UK education – Defend Digital Me, May 2022: https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf

These basic failings are extremely concerning, and betray a lack of understanding from schools about their responsibility to safeguard children's data rights.

Biometric data is considered special category data under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018), meaning it is subject to additional protections. This is due to the deeply personal nature of biometric data, and the risks inherent in its processing. **While a password or pin code can be changed, or a access card replaced, biometric data such as a fingerprint is permanent. The impact of a data breach, hack or improperly stored data could have lifelong consequences for children.**

Under the DPA 2018 and UK GDPR, schools must have a lawful basis in order to process special category data. Schools have typically relied on the consent of parents and/or pupils as the lawful basis. Children's data rights campaigners have noted that schools approach to obtaining "meaningful consent seems cursory at best" and that schools often fail to explain to pupils and parents that biometric systems are voluntary.[3]

In both Sweden and France, courts have found that consent was an inadequate basis for the use of facial recognition in schools, given the intrusive nature of the technology. Critically, the Commission Nationale de l'Informatique et des Libertés (CNIL) in France found that even if fully informed, freely given consent is given by student, **the inherent power asymmetry in the school environment means consent cannot be used as a lawful basis for facial recognition technology in schools under the GDPR.**

The Biometrics and Surveillance Camera Commissioner, Professor Fraser Sampson, has warned that the use of biometric surveillance in schools requires careful consideration and oversight, beyond just ensuring that the technology is compliant with the Data Protection Act 2018:

> "*Somewhat ironically, biometric surveillance requires constant vigilance. To ensure its proper governance, avoid mission creep and irreversible erosion of freedoms this area calls for careful recognition – and anyone who believes it is simply about data protection hasn't been paying attention*."[4]

RISK TO PRIVACY

The use of biometrics data in schools poses a risk to pupils' right to privacy and

3 27 schools in England using facial recognition to take lunch payments – Alexander Martin, Sky News, 20th October 2021: https://news.sky.com/story/27-schools-in-england-using-facial-recognition-to-take-lunch-payments-12439330

4 The state of biometrics 2022: A review of policy and practice in UK education – Defend Digital Me, May 2022: https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf

normalises, at a young age, intrusive data collection for everyday activities. We are aware that schools are purchasing technologies which are capable of collecting children's fingerprints, iris and palm scans, face prints, temperature readings, as well as undertaking object and behavioural analysis.

The increasingly mundane purposes of biometric systems, such as paying for lunches, photocopying, locker access or taking out library books, raises questions as to the necessity and proportionality of such systems. Schools should consider whether less privacy-intrusive means of undertaking basic tasks would be more appropriate. **It highly unlikely that schools *need* to collect sensitive biometric data in order to carry out their educational and safeguarding duties. Less intrusive means, such as passes or pin codes, are more proportionate and privacy preserving and must remain the default option for schools.**

FACIAL RECOGNITION

We are particularly concerned by the increasing use of facial recognition. We welcome the Welsh government's decision to "strongly discourage the use of this technology" in schools.[5] Facial recognition has no place in schools.

Facial recognition technology involves the creation of a faceprint, which is biometric data as sensitive as a fingerprint, of individuals who pass in front of a camera. This faceprint is compared against a database of known faces, in order to find a match. **The technology is notoriously inaccurate**, with the Metropolitan Police force's use of the technology wrongfully flagging individuals in 81% of cases.[6]

The technolgy carries additional privacy risks, as unlike fingerprint, iris or palm scanning, it can be utilised without an individual's knowledge. There is no central register of which schools are using facial recognition, although one major UK supplier of the technology states that over 70 schools use their technology, meaning the actual number could be considerably higher.[7] The Welsh government states that it is not aware of any schools in Wales using the technology, although it is not clear how it has come to this conclusion.[8]

In Scotland, the Information Commissioner's Office (ICO) was forced to intervene when journalists revealed that several schools in North Ayrshire were using live facial

5 Protection of biometric information in schools and colleges – Gov.Wales, 4th July 2022: https://www.gov.wales/protection-biometric-information-schools-and-colleges-html#section-81641
6 Big Brother Watch analysis based on data from 2016-2022. See our campaign page for details: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-uk
7 27 schools in England using facial recognition to take lunch payments – Alexander Martin, Sky News, 20th October 2021: https://news.sky.com/story/27-schools-in-england-using-facial-recognition-to-take-lunch-payments-12439330
8 Protection of biometric information in schools and colleges – Gov.Wales, 4th July 2022: https://www.gov.wales/protection-biometric-information-schools-and-colleges-html#section-81641

recognition technology as part of a 'cashless catering' system.[9] After an investigation, the ICO concluded that "the processing carried out by NAC [North Ayrshire Council] is likely not to have been in compliance with data protection law".[10] NAC had failed to consider the risks of bias and discrimination and that they had failed to explain to children "the risks and consequences of the processing as well as the safeguards put in place to minimise these risks". The council had also failed to obtain the meaningful consent of parents and children, and failed to obtain any consent from children between the age of 12-14. **This litany of failures should act as a stark warning to other local authorities who may be considering the introduction of facial recognition technology.**

Although we welcome the ICO's intervention in this case, more must be done to safeguard children from the use of facial recognition in schools. **Big Brother Watch is calling for live facial recognition to be banned in the UK, due to the considerable risk it poses to privacy.**

CONCLUSION

The use of biometric data in schools poses a serious risk to the privacy and data rights of children in Wales. Many schools are failing to adequately inform or seek the consent of parents and children over the use of these intrusive new technologies. The Welsh government must ensure that biometric data is collected and processed in accordance with the law and the children's rights are meaningfully upheld and enforced.

9 ICO to step in after schools use facial recognition to speed up lunch queue – Sally Weale, the Guardian, 18th October 2021: https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk

10 North Ayrshire Council's use of Facial Recognition Technology in its schools – Infromation Commissioner's Office. 31st January 2023: https://ico.org.uk/media/action-weve-taken/4023847/ico-letter-to-nac-appendix.pdf