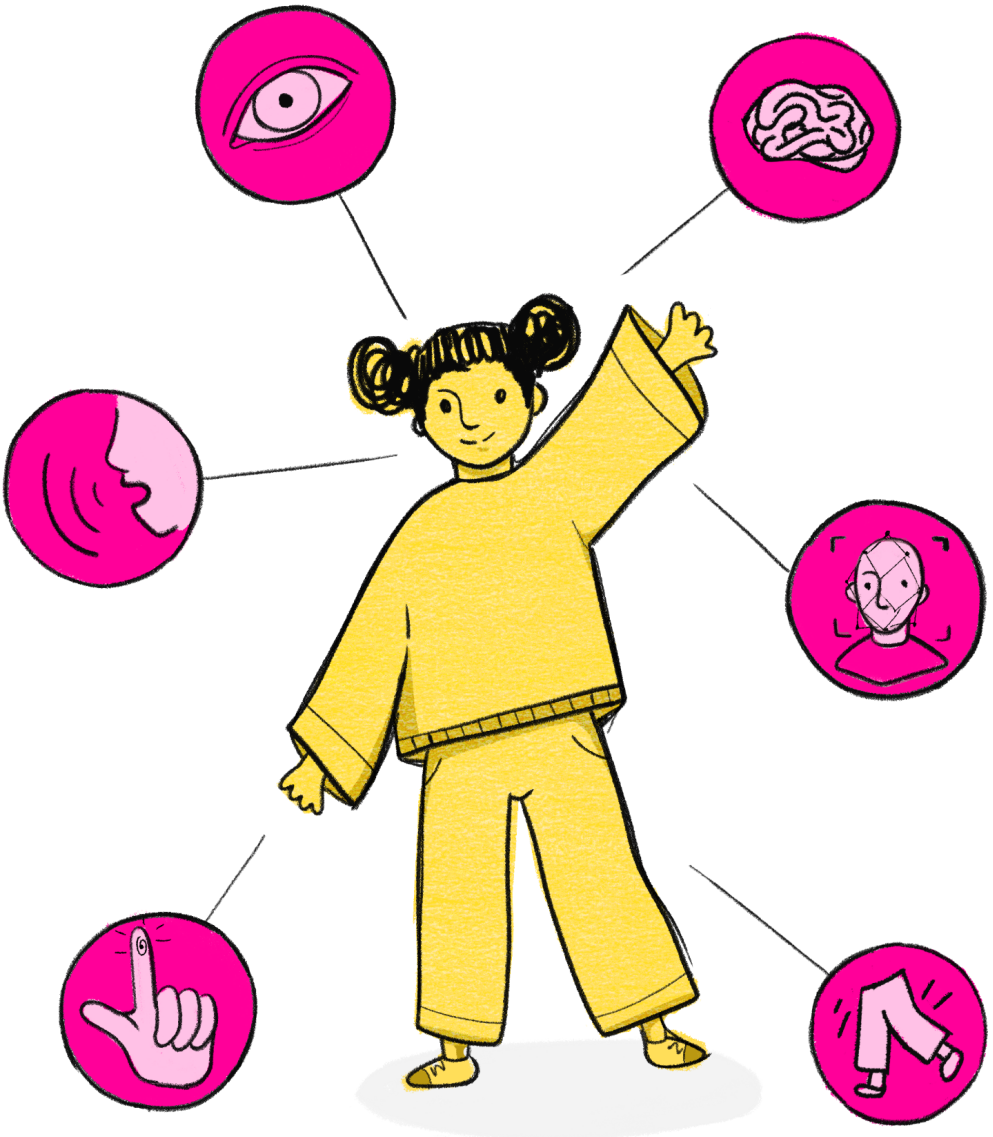
The state of biometrics 2022

a review of policy and practice in UK education



May 2022

defend|digital|me

Authors
Pippa King
Jen Persson

Artwork by
Hannah Mallory

Funded by
the Joseph Rowntree Reform Trust

Citation: The State of Biometrics 2022: a review of policy and practice around biometric data in UK education, defenddigitalme (2022) v1.7

Defend digital me is grateful for contributions and engagement from a wide range of named and unnamed individuals and organisations throughout the report, its research and review, including school FOI officers, academics, teaching union and industry representatives. Note that inclusion does not imply that organisations or individuals have reviewed or endorsed the contents, which reflect the views of the authors.

Any enquiries should be sent to info@defenddigitalme.org
This document is also available from our website at
https://defenddigitalme.org/report/state-biometrics-2022

ISBN 978-1-7396722-0-1

Contents

Foreword

Professor Fraser Sampson

Commissioner for the Retention and Use of Biometric Material and Surveillance Camera Commissioner

My statutory functions as Biometrics and Surveillance Camera Commissioner were introduced by the Protection of Freedoms Act 2012 primarily to cover the use of biometric surveillance by policing and law enforcement. Biometric capabilities that were available only to state intelligence agencies at the time of enactment are now readily available on the open market. In this context the expansion of newly intrusive technologies since the Act was passed, now raises daily questions even when being legitimately used to protect national security and prevent serious harm.

Adoption of those technologies in our schools is certainly no less contentious than it is in law enforcement and in some ways it is more challenging. For example, using technology to predict criminality has been controversial; using it to predict academic results fairly and accurately has proved highly sensitive and hotly disputed.

As the legislation reaches its 10th anniversary several clear trends can be seen. Video analytics have revolutionised surveillance which is no longer about where you put your camera but the purposes to which you're going to put the billions of available images and sounds captured on everybody's camera. Inferential algorithms that purport to identify alertness, emotions and even sincerity are gaining credibility while what to do with facial recognition is the surveillance question that refuses to pass unnoticed.

Biometric surveillance continues to be a fast-moving discipline offering the potential for emancipation and subjugation. In the context of my specific statutory functions, I approach its many facets from three perspectives: the technologically possible (what can be done), the legally permissible (what must/must not be done) and the societally acceptable (what we support being done). While the first two grab the headlines or drive policies, it is in the third area – what people are willing to support or even tolerate – where I believe the future of biometrics is being shaped globally.

Against that backdrop I would offer the following thoughts when considering any proposal for, or discussion of biometric technologies in schools.

1. Who's benefiting? Ask to what extent the best interests of the child are a primary consideration? This is the fundamental requirement in the UN Convention on the Rights of the Child. Parental preference, administrative convenience, cost reduction are all valid considerations, but Art. 3 says that the best interests of the child shall "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, be a primary consideration". It is surprising how often this is overlooked.

2. Who's watching? 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.

3. Whose company are you keeping? Accountable surveillance requires trusted partnership with trusted partners. Some surveillance companies have been clearly associated with human rights abuses of children, depriving them of fundamental rights to education, freedom from economic exploitation, assembly and even family life. Decisions to enter into commercial partnership with such companies therefore have significant due diligence considerations that extend far beyond 'bottom line' issues of cost.

4. Where's the push? Technological development is often characterised as some inexorable and naturally occurring journey, but this is really invention masquerading as evolution. Biometric technology is creationism, pure and simple, and has the DNA of the designer all over it. The proper role for innovative surveillance technology is an important question but it is not a predetermined path.

5. Why the rush? Our enthusiastic adoption of biometric technology needs to balance material risk with measurable benefits, which presupposes we have identified both. Although there are some areas in policing where the adage may not always hold true, the saying "just because you can doesn't mean you should" is still a handy test to apply when balancing the possible with the permissible and the acceptable. Some – including, surprisingly, the Department for Education – appear to have taken the view that bare compliance with Chapter 2 of the Act is all that is required to ensure the lawful, ethical and accountable use of biometric surveillance in schools.

While Chapter 2 addresses one narrow legal issue (that of protecting biometric information of children in schools) and guidance on its practical implementation is vital, I do not believe that this excludes the need to address the many wider technological, legal and societal issues of biometric surveillance generally. If biometric surveillance is to have a legitimate role in places of education, both role and legitimacy will need a much broader approach than this.

I am grateful to have been asked to provide this Foreword and applaud the approach exemplified by Defenddigitalme. As biometric capabilities find their way into every aspect of our lives, keeping focused on a rights-respecting environment, built upon principles of pluralism, universality and ethics will become more important than perhaps even the architects of the Protection of Freedoms Act imagined.

Executive summary

Ten years on, the UK Protection of Freedoms Act 2012 and current UK Data Protection law are not enough to protect children's rights in educational settings. Emerging technology and scope creep have advanced since those laws were written, particularly around the use cases in education that sit outside the narrow definition of biometrics for ID purposes.

The EU AI Act includes as high risk, biometrics, and AI systems intended to be used in ways that have significant impact on children's personal development, including personalised education or cognitive or emotional development.
Will the UK law protect children less?

Recommendations

The ICO should find biometric data processing in educational settings in the UK incompatible with the increased protections in the GDPR and modernised Convention 108 for biometric data and for children. This decision should uphold the principles of necessity and proportionality. It should recognise the failure of consent in educational settings due to the power imbalance between individual and authority. This aligns with court and data protection authorities' decisions in Sweden, France, and Poland since 2019.

All processing of biometric data from children for the purposes of building access, canteen, and library uses in educational settings should end, including fingerprints, and be replaced by using the current non-biometric solutions that must be offered already in parallel, under the Protection of Freedoms Act 2012. The ICO response must be "effective, proportionate and dissuasive" to end all routine use of biometrics through enforcement after a suitable notice period, due to the failures to comply with the principles of the GDPR, the Convention 108, and UK Data Protection Act 2018.

Legislation should expand i.e. to a UK Education and Digital Rights Act, or in the UK Data Protection Act, to protect children at scale from overreach in this sector that do not use bodily data for the unique purposes of identification defined as "biometrics" but use emerging technologies for purposes such as emotion and attentiveness detection, psychometric analytics, gait analysis, or mental health and well being 'prediction'.

Data processing behind the cashless payment systems should be investigated for routine profiling of children's library reading and canteen purchasing habits, in particular those from which the companies or staff, may be able to make inferences about sexual orientation or religion. (i.e. LGBT books and kosher or halal food.)

The Surveillance Camera Commissioner role should incorporate education where biometrics and surveillance camera systems are utilised under Section 29(6) of the Protection of Freedoms Act 2012. (While noting that the Act does not apply in Scotland and Northern Ireland, and the current DCMS proposals to reform the role.)

Background introduction

Biometric technology in UK schools was first introduced around 2000. The first documented evidence of the technology's use comes from the Information Commissioner's Office in a communication in July 2001 to a company, Microlibrarian Systems, for use in primary school libraries:

> *"It is understandable that concerns will be raised over the use of such technology if it is believed that it involves the holding of a database of pupils' fingerprints. However, from what I have understood of our discussions, although theoretically possible to use the information obtained from this system to match fingerprints taken from a scene of a crime, the resources this would require make this highly impractical. In light of this I do not believe that the use of Idenitkit fingerprint technology to identify library members raises any data protection concerns."*
>
> *Letter to MicroLibrarians from Robert Mechan, Senior Case Officer, ICO 4th July 2001*

From then to 2013 schools used a variety of biometrics, often without informing parents. If parents were informed, an 'opt out' rather than an 'opt in' was applied. Biometric technology, at that time, was not in the consumer or commercial marketplace, only used on a daily basis by students in UK schools. Whilst the UK was using biometrics on a regular daily basis in schools, the rest of the world was not routinely using the technology in educational settings. As far as is known the only other country to use biometrics in schools was the USA and their use, which was the fingerprint, wasn't until around 2006.

In 2006 already Wendy Grossman had summed up risks, "*Why does it all matter? Because a password is something you have; a fingerprint is something you are. A password can be reset, reissued, forgotten, copied, written down, or changed. A fingerprint is for life. Like the ID card, as biometric systems pervade society they will be used to secure data of a serious nature. Identity theft will become far more dangerous.*"

Numerous biometric systems have been 'trialled' in UK schools since 2000, including iris scanning in 2002, infrared palm scanning in 2006 and facial recognition in 2010[1]. For cashless catering, library, registration, door access, photocopying, locker access, cashless monetary payments, vending machines and laptop access, the biometric of choice is the fingerprint which has firmly gotten hold of the UK education market.

The Association of School and College

[1] Daily Mail (2010) School installs £9,000 facial recognition cameras to stop students turning up late... and teachers could be next target https://www.dailymail.co.uk/news/article-1317520/School-installs-9k-facial-recognition-cameras-stop-students-turning-late.html

Leaders (ASCL) estimated that about 30% of secondaries in England were using fingerprint data in 2011.[2]

Other biometric technologies were abandoned within a year of their use, seemingly not deemed fit for purpose, until the recent reintroduction of facial recognition in 2020 for cashless catering.

By 2017, concerns with the biometric systems were summarised by researchers in four areas: Pupil resistance, Pupil mistrust, Hygiene, and Parental surveillance. Researchers Leaton Gray and Phippen found that, "*pupils were not inducted into biometric systems in the same way that they had been in 2006 when such systems were relatively novel. There were no talks on the purpose of the system and related data privacy issues (indeed we found that data privacy was not mentioned at all other than in the context of e-Safety*.)"

And while we agree with the assumption that school staff intentions where these technology are employed are benign, we also support their finding that there was no reflection on the potential future impacts,

"staff and pupils are persuaded by the convenience of such systems to a point that they do not reflect on the potential social harms, or related legal issues. Schools did not have effective data protection policy or practice in place to be able to manage data such as biometrics effectively and in a legally compliant manner." "Biometrics may be a great time-saver in the short term, [although unproven] but when it comes with the risk of serious long-term consequences for our students, is it worth it?"

In the 2019 ruling by the French Data Protection Authority, the CNIL also reflected on the wider chilling effect of facial recognition through 'reinforced surveillance' as contributing to its intrusiveness.[3]

Using biometric technology in schools opens up the debate on the necessary and proportionate use of high-risk technology in education when another form of identification, PIN or swipe card, would be enough for low-risk applications such as cashless payments or library card systems.

Where fingerprint readers are used, current law requires schools to offer alternatives such as a touch card, or simply giving their name at the canteen till or to the librarian. For pupils who choose to use the software provided by a leading UK supplier CRB Cunninghams (Constellation Inc.), there are four ID verification methods to choose from within their Fusion cashless system: fingerprints, QR codes, contactless cards, and PINs.[4] Therefore the high bar of necessity for biometrics is already proven not to be met.

Although this provider claimed[5] that around 70 schools had either ordered facial recognition systems, or were using it in October 2021, more may have started using similar systems from different providers that have not yet been identified in our sample of schools we asked via FOI.

We are now starting to see new products emerging in the classroom, beyond canteens and libraries, that challenge the definition of biometrics and are more intrusive than ever on human dignity and affect behaviour. This summary brings us to 2022, ten years after the introduction of the Protection of Freedoms Act 2012.

---

[2] BBC (2012) Biometric data: Schools will need parents' approval https://www.bbc.co.uk/news/education-18073988

[3] Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

[4] CRB Cunninghams https://www.crbcunninghams.co.uk/case-studies/fusion

[5] Sky News (2021) More than 60 schools set to deploy the no-contact payments systehttps://news.sky.com/story/27-schools-in-england-using-facial-recognition-to-take-lunch-payments-12439330

Chapter 1: The Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012

In May 2012, after seven years of campaigning by parents[6] and privacy groups, the Protection of Freedoms Act was passed. Chapter 2 deals with processing children's biometric data in schools in England and Wales and requires consent for educational establishments to process pupils' biometrics. This does not apply to schools in Scotland or Northern Ireland.

- Each parent of the child should be notified by the relevant authority that they are planning to process their child's biometrics and be informed that they are able to object.
- In order for a school to process children's biometrics at least one parent must consent and no parent has withdrawn consent. This must be in writing.
- The child can object to the processing of their biometrics regardless of parental consent. Objection by a parent or the child invalidates consent from the other.
- Schools are also required by the law to offer an alternative solution to using a child's biometric.

Prior to May 2012 other UK laws helped clarify processing of children's biometric data, without parental consent, such as the Data Protection Act, Human Rights Act, Education Act, Freedom of Information Act, the Children Act, and Gillick Competence. The duties of schools in the Protection of Freedoms Act 2012, set out in Department for Education guidance, came into effect from September 1, 2013. Since then the way that schools have asked for consent or not, and offered an alternative or not, has varied across educational settings.

No government department or other bodies monitor whether schools adhere to the Protection of Freedoms Act instructions in Chapter 2, how many schools use biometric technology, how many pupils have their biometrics stored on school or supplier databases, or what schools activities that biometric data is used for. The BSI standard PAS 92:2011 referenced in the DfE 2018 guidance for schools has been withdrawn[7].

In 2018, on our behalf, Survation polled 1,004 parents of children in state schools about their experience of technology in schools. 38% of parents whose children were using biometrics in school, said they had not been offered any choice, and over 50% had not been informed how long the fingerprints or other biometric data is retained for, or when they will be destroyed.

In 2022 we also asked ten unions across the UK with members in teaching and education, but none said they have any Code of Practice on this to assist staff about their own use and rights, or for pupils.

[6] Pippa King (2018) https://pippaking.blogspot.com/2018/08/biometric-consent-for-students-in.html

[7] BSI standard PAS 92:2011 Code of practice for the implementation of a biometric system https://shop.bsigroup.com/products/code-of-practice-for-the-implementation-of-a-biometric-system/standard/preview

Chapter 2: Defining biometric data

What is biometric data?

Biometric data is defined in legislation. To sum up, biometric data is information gathered about a person's physical or behavioural traits that may be used to identify a living person, on its own, or when combined with other personal data of which the data processor is likely to come into possession.

As sensitive data, its processing for "*uniquely identifying a natural person*" is prohibited in UK data protection law based upon the GDPR with exceptions, one of which is consent expressly given in advance. The UK decision to leave the EU does not affect this, although at the time of writing the UK government has signalled its intention to reform the UK Data Protection Act, "to create an ambitious, pro-growth and innovation-friendly data protection regime."[8]

The UK GDPR defines biometric data in Article 4(14):

"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

Convention 108+

Article 6 of the modernised Convention 108+ states that biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law. It sets out that safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject notably a risk of discrimination. The Explanatory Report[9] further notes that biometric data is sensitive data, "Processing of biometric data, that is data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject."

Protection of Freedoms Act 2012 (for schools in England and Wales)

(2) "Biometric information" means information about a person's physical or behavioural characteristics or features which—

[8] Consultation: Data a New Direction https://www.gov.uk/government/consultations/data-a-new-direction

[9] Council of Europe (2018) 'Modernised Convention 108. Convention for the protection of individuals with regard to the processing of personal data'. (Article 6) Explanatory Report pages 21-22. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

(a) is capable of being used in order to establish or verify the identity of the person, and

(b) is obtained or recorded with the intention that it be used for the purposes of a biometric recognition system.

(3) Biometric information may, in particular, include—

(a) information about the skin pattern and other physical characteristics or features of a person's fingers or palms,

(b) information about the features of an iris or any other part of the eye, and

(c) information about a person's voice or handwriting.

In subsection (2) "biometric recognition system" means a system which, by means of equipment operating automatically—

(a) obtains or records information about a person's physical or behavioural characteristics or features, and

(b) compares the information with stored information that has previously been so obtained or recorded, or otherwise processes the information, for the purpose of establishing or verifying the identity of the person, or otherwise determining whether the person is recognised by the system.

Problems with defining biometric data?

We are at grave risk in the digital policy environment of using data rights as a proxy for the entirety of human rights when it comes to challenging infringements of rights in the digital environment. Data laws can find unethical practice compatible with data processing law. The Danish DPA (Datatilsynet) conducted an audit of the IT University of Copenhagen (ITU) and their use of an online proctoring service for one of their online exams, and found it in line with the GDPR and national legislation.

This is inadequate to protect children from the intrusiveness of technology not used for the purposes of their identification, if the classroom teacher already knows who is who, but nonetheless has chilling effects on participation, speaking up, on behaviours, demanding able and competent norms of bodily control that not every child may have.

Perhaps the question should not be whether a tool is 'legal enough' to use in educational settings, but whether it is respectful of human dignity and the aims of education, meeting the full range of human rights; freedom of expression, freedom of thought, and aims of the right to education.

The starting point must be necessity and proportionality whether a tool using biometrics can be lawfully used at all, and only then seek a basis for how the data processing requirements should be met.

Enabling access

Further research is needed into positive exceptions in the use of biometric technology in educational settings for accessibility needs (e.g. eye controls of systems for children with disabilities). We are also continuing to research to assess the discriminatory effect on take up for children eligible for Free School Meals. To date the number of children not using biometrics where it has been introduced is too small to be indicative.

Emerging technologies

Recent developments in the educational sectors use of biometric technology

The urgent need for better protections for children and young people is heightened by the rapid adoption of facial detection coupled with age verification now growing beyond school canteen tills to supermarket tills. But the Westminster government's policy direction is not towards an increase but a reduction in the safeguards on human rights, as outlined in the DCMS consultation on changes to the UK Data Protection regime, *Data: A new direction.*[10]

Facial recognition

Despite being found unlawful and since removed from schools in France, Sweden and parts of the U.S., facial recognition is growing across UK schools.

This despite widespread recognition of research evidence that facial detection, facial recognition and biometric systems are discriminatory. In 2019, researchers for the U.S Department of Commerce National Institute of Standards and Technology (NIST) found, "*elevated false positives in the elderly and in children; the effects were larger in the oldest adults and youngest children, and smallest in middle aged adults.*"

> *"children … are disadvantaged …by being excluded by policy, or by encountering higher false negatives. Age itself is a demographic factor as accuracy in the elderly and the young differ for face recognition (usually) and also for fingerprint authentication. This applies even without significant time lapse between two photographs."*[11]

On gender and race they concluded that Buolamwini and Gebru's 2018 research found some facial analysis algorithms misclassified Black women nearly 35 percent of the time, while nearly always getting it right for white men.

Facial recognition in England

In September 2020 facial recognition was introduced into a secondary school Kingsmeadow Community School in Gateshead, England to use at the point of sale in their canteen. The supplier claims it was one of the first. It was "part of a pilot scheme and "no funds were spent on the system," according to the school.[12] The take up for the system was 904 students out of 909. Since then, the same system supplier has stated that they supply over 70 schools with this kind of technology.

[10] DCMS consultation Data: a new direction (DCMS) September, 2021 https://www.gov.uk/government/consultations/data-a-new-direction

[11] 2019 report for the U.S Department of Commerce National Institute of Standards and Technology (Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[12] Freedom of Information request to Kingsmeadow Community School Gateshead (June 2021) https://www.whatdotheyknow.com/request/facial_recognition_9

Facial recognition in North Ayrshire, Scotland

In October 2021 the ICO intervened in a mass rollout to nine schools—over 8,000 pupils[13]—of this type of biometric technology in North Ayrshire, Scotland[14]. The system was put on hold pending a decision of its use under current legislation. It is unknown how many other schools continue using their technology elsewhere.

An ICO spokesperson told us in May 2022:

> *"Organisations using facial recognition technology ("FRT") must comply with data protection law before, during and after its use. In addition, data protection law provides extra protections for children, and organisations need to carefully consider the necessity and proportionality of collecting biometric data before they do so. Organisations should consider using a different approach if the same goal can be achieved in a less intrusive manner.*
>
> *"We understand that North Ayrshire Council decided to pause using FRT in schools following our initial enquiries. Our aim is to ensure that children's data is protected in line with the law and we will continue engaging with the Council on this issue.*
>
> *"Anyone who feels that their personal data has been processed in a manner that is unlawful can raise a complaint directly with the ICO."*
>
> *"The ICO The ICO guidance on the use of FRT and surveillance is at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/additional-considerations-for-technologies-other-than-cctv/#frt"*

There are over 22,000 schools in the state sector. Without dissuasive enforcement action poor practice will not change. Solving the lack of oversight for educational settings is unlikely to improve without dedicated oversight. The DCMS and Home Office propose moving the role of the Biometrics Commissioner under the ICO. The Commissioner's response[15] in 2021 set out why this would be a backwards step.

Facial recognition Case Study: Stonyhurst College I Suprema

Suprema marketing uses Stonyhurst College as an example of where "staff can now freely come and go through more than 50 doors using convenient Mobile Access and Facial Recognition." But while they claim that the app and FaceStation F2 biometric terminals eliminate the need for cards[16] entirely, we wonder what alternative they are using, since one must be offered by law, and without detriment.

[13] Freedom of Information request to North Ayrshire Council (September 2021) https://www.whatdotheyknow.com/request/biometric_facial_recognition_use

[14] Financial Times, Facial recognition cameras arrive in UK school canteens (2021) https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9

[15] Response by the Biometrics and Surveillance Camera Commissioner to the Department for Digital, Culture, Media and Sport consultation (2021) https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response

[16] Choi, T. (2022) Biometrics Update | Suprema enable UK school to cut back plastic waste from access cards https://www.biometricupdate.com/202204/suprema-face-biometrics-enable-uk-school-to-cut-back-plastic-waste-from-access-cards

Behavioural sensing and monitoring attentiveness

More emerging technology in schools uses children's bodily data but may not be obviously thought of by schools as biometrics in the way that fingerprints or facial recognition is today. Cameras that monitor pupils' engagement in real time during lessons are being used or trialled in some schools and claim to enable teachers and management to see pupil engagement.

ViewSonic Corp., 'a leading global provider of visual solutions', published its partnership with Intel and the Smestow Academy in Wolverhampton in March 2022. It claims it is the first school in the UK to deploy the AI-powered myViewBoard Sens analysis tool in the classroom that can infer and present a variety of data from the ViewBoard, which sits at the front of a classroom, and includes mood and attentiveness, and "indicate the factors that may affect students' focus."[17]

Fig.1 Snapshot of "mood" and behavioural monitoring demonstrated by myViewBoard Sens at the Bett Show 2022

Facial detection and emotional recognition: e-Proctoring

Remote exam invigilation technology is out of scope for the purposes of this report and our research, however emerging technology is growing more widespread and we are already behind in the protection of users from its overly intrusive effects. Essentially, it uses the exam candidate's device camera to monitor the candidates' eye and bodily movements and expressions, the system may assess keystrokes for anomalies, and tabs that are open on the electronic device—all to determine "suspicious' behaviour." Those who move their eyes away too much, have the wrong facial expressions or move their bodies in ways that trigger a flag, may then be penalised. While companies argue that they do not use facial recognition or "biometric analysis", such tools clearly use bodily data such as face detection and gaze detection, and a person may do the ID verification through the tool. The definition here is moot.

University of London moved away from Proctortrack after a change.org petition by students in 2020.[18]

Separately, concerns about data security were realised when ProctorU confirmed a data breach after a database leaked online.[19]

Students around the world, united in protests against e-proctoring, agree that data protection laws are not enough to prevent racial and disability discrimination and protect learners' human dignity.

The BMA has called for a review into the handling of online exams following reports of students being denied toilet breaks and tests abruptly terminated (Tonkin, 2021)[20].

[17] ViewSonic's myViewBoard Sens Brings UK's First AI-powered Classroom to Smestow Academy (March 2022) https://www.prnewswire.com/in/news-releases/viewsonic-s-myviewboard-sens-brings-uk-s-first-ai-powered-classroom-to-smestow-academy-896798309.html

[18] Stop invasive online proctoring petition (2020) https://www.change.org/p/university-of-london-stop-invasive-online-proctoring-at-university-of-london-and-provide-fair-alternative

[19] BleepingComputer (2020) ProctorU confirms data breach after database leaked online https://www.bleepingcomputer.com/news/security/proctoru-confirms-data-breach-after-database-leaked-online/

[20] Tonkin (2021) Call for Review into SJTs: online proctoring. The BMA called for a review into the handling of online exams https://www.bma.org.uk/news-and-opinion/call-for-review-into-sjtshttps://www.bma.org.uk/news-and-opinion/call-for-review-into-sjts

Voice data: Case study | Cameras outside and in | Onvu Lessonvu

We first cited this example in our State of Data 2020 report. The university technical college in Birmingham was the first school in the country to install always-on, 360-degree cameras in all of its 28 classrooms. Aston University Engineering Academy, which caters to just over 600 14- to 19-year-olds, officially launched the equipment at an event at the UTC. ONVU's Lessonvu is described as a

"*non-intrusive classroom video lesson observation system that is controlled by teachers. Its unique technology allows for the complete recording of 360-degree video and audio, giving a comprehensive view of the entire lesson.*"

Lessons are captured using a high definition 360-degree fisheye camera and via high definition microphone. The recording is then converted using ONVU's proprietary software into a more traditional view. By default all recorded material is stored locally on the school's network, and schools can opt to store video clips to the cloud if required while controlling permissions.

Lessonvu's FAQ states, *"Most schools will already have parental approval to photograph students but a school should review its policy on video use. Approval from parents may be required."* In our opinion, this is must, not may, and because this processing is of biometric data such as voice, the law requires a different approach from static photographs. As such processing this personal data from anyone,—children, staff and visitors on film and including their voice data—falls under not only data protection and privacy laws, but the Protection of Freedoms Act 21012 and Chapter 2(26) 'the requirement to notify and obtain consent before processing biometric information'.

That requires active, explicit consent and if either the child or either parent objects, processing must not go ahead. But consent may be irrelevant since other schools perform the public task of teacher improvement without using always-on cameras, therefore we believe that this fails to meet a high bar for sensitive data under the necessity test.

Furthermore, personal data that is processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation) whereas these cameras can be on all the time so collect excessive data. It follows from the GDPR recital 39 that personal data from children may only be processed if the purpose of the processing cannot be achieved in a satisfactory manner using other methods.

"360-degree HD cameras (with studio mics) mean that your teachers will never miss anything. Our cameras are designed to be discreet and always on." (Onvu, 2022)[21].

Does your school treat voice recordings as biometrics within the scope of the Protection of Freedoms Act Chapter 2 (28) (3)(c)?

[21] 'A video capture solution for schools' https://web.archive.org/web/20220305111255/https://www.onvulearning.com/video-lesson-observation-software/

Chapter 3: England

Most of the UK's schools are in England. There are 24,413 schools in England – including 388 nurseries, 16,791 primary schools, 3,458 secondary schools, 2,366 independent schools, 1,005 special schools, 57 non-maintained special schools and 348 pupil referral units (PRUs) (BESA, 2022). The questions asked via FOI to state schools in England was in-effect a pilot of the questions in a small subset of schools which we hope to continue to research. We are still in the process of asking those that did not respond to comply with their FOI obligations and provide answers, to get a more complete picture.

An authoritative estimation would require a larger and more comprehensive research project and complete dataset. However, the data provided points to significant adoption of fingerprint readers in secondary schools and very high uptake where they are in schools.

Data sources

To get this snapshot of the adoption of biometric technology in schools we considered a selection of schools across England: a mix of rural, urban, from the north to the south of England. From the schools that provided data, we analysed the percentage of schools using biometrics technology, and from those, we looked at how many pupils were in each school to get an impression of take-up rate. We asked 144 individual secondary schools plus 12 of the largest Multi Academy Trusts -- a total of 374 schools during 2021 and 2022. Response rates were 41% from individual schools and 50% from the Multi Academy Trusts, but some answered only in part with sufficient comparable data from four MATs.

Within the figures are some small sixth form registration biometric systems which have 100% usage whilst the rest of the schools' age groups do not use it. Some schools indicated they used biometric systems but did not tell us how many pupils were using it, some schools said they had a higher number of people using the biometric system than students on school roll as they included staff. However, these figures were so small they were not significant.

Key findings

From the sample of 142 secondary schools in England using fingerprint readers in school, with 136,293 total pupils on roll, 117,122 pupils use them (85% of all on roll).

Despite the Protection of Freedoms Act 2012 obligations on parental / child consent, some educational settings continue to make biometrics use obligatory for all.[22]

[22] "Children in Nursery do not use the finger scan but have meals recorded manually. Printed statements are available from the Bursary on request. All other pupils, including those entitled to free school meals, will operate the system by using their finger." https://www.whgs-academy.org/parent-info/day-to-day-matters/school-meals

Others appear to discriminate against children in receipt of Free School Meals by making it seem obligatory for pupils who qualify for FSM to be signed up to the biometric system in order to continue to receive their lunch, while others can choose not to use it.[23] Others describe nothing on rights but make the burden on the school seem overwhelming to dissuade opt out despite the legal obligation to offer parallel systems if the school chooses to use biometrics at all.[24] *"Administration of additional systems could create an unnecessary administrative burden and incur additional costs to the School from funds which could be used more effectively elsewhere towards providing your child's education."* If a school wants to have only one system, the answer should instead be to choose the least intrusive tool for children to use.

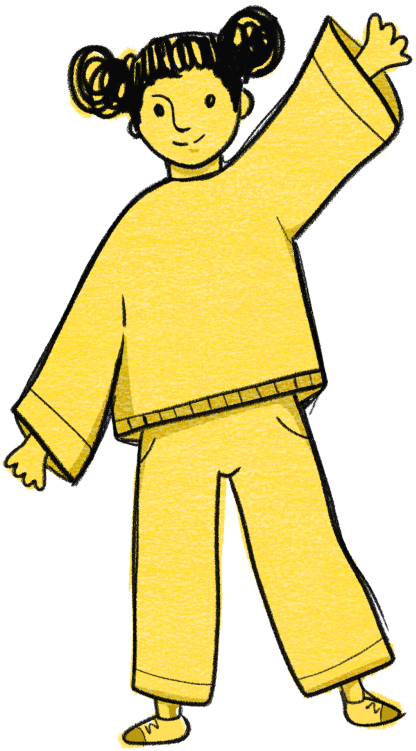
The state of adoption in England

This is information from 374 schools, including nursery, primary, secondary and sixth forms via Freedom of Information requests. None of the MATS that responded had primary schools that use biometric technology. The biometric technology in use is fingerprint based, being used predominantly for canteen use, with a small amount of library, door access, general payment and photocopier access. No schools that responded said they use facial recognition but we know from press and parental complaints that this emerging market is active in secondary schools, just not those that our sample reached.

From 374 nursery, primary, secondary and sixth forms, a total of 216,296 pupils, 142 schools (38%), 118,445 pupils, were using biometric technology (54%).

If the nursery/primary schools figures are *removed*, and we look only at secondary schools and sixth forms (11+), from a total of 189 secondary settings (188,748 pupils) 142 secondary schools responded stating they use biometric technology (75%).

Take up within the 142 secondary schools using biometric technology is 85%. The total pupils on roll in the 142 secondary schools is 136,293 students, of which 117,122 pupils use the biometric system.



[23] *"Accounts must be topped up in advance using the ParentPay system and this can be done either online or via a PayPoint. Students who qualify for FSM will need to be signed up to the biometric system in order to continue to receive their lunch."* archived at https://web.archive.org/web/20220510001253/https://www.buxtonschool.org.uk/542/biometric-system

[24] Lancaster Royal Grammar School | archived at https://web.archive.org/web/20220504195600/https://www.lrgs.org.uk/form/?pid=8&form=99

Chapter 4: Scotland

The state of adoption in Scotland

Scotland has 32 local authorities. From Freedom of Information requests between 2018 and 2021 – fifteen of the LA schools were using biometric technology, fourteen of those LAs are supplied by CRB Cunninghams and one by Civica. Seventeen LA schools are not using biometric technology. The biometric technology actively used in Scotland's schools is fingerprints since facial recognition rollouts were paused. The biometric systems procurement is at LA level, rather than by individual schools which is different from the rest of the UK. Biometric systems in Scottish schools are used for canteen purchases and some have been used in Scottish schools since 2000.

The total number of pupils on roll in the 15 LA secondary schools using biometric systems is 49,700 with 41,000 pupils using the biometric system. In those secondary schools that are using biometric technology the take up within those schools is 83%, near to the 85% take up rate in schools in England.

Recent developments

Biometric facial recognition technology was briefly introduced in North Ayrshire Local Authority secondary schools with West Lothian Local Authority planning to use the same facial recognition system for canteen point of sale transactions. North Ayrshire schools, approx 8,000 secondary pupils, started using facial recognition in October 2021 for around a week, then suspended the system due to adverse public reactions, discussion in the Scottish Parliament and at the local council meeting, and subsequent intervention from the Information Commissioner's Office. To date the ICO has not ruled whether or not the facial recognition technology use is lawful under the GDPR and UK data protection law. North Ayrshire put its rollout on pause, on October 22nd, 2021.

West Lothian Council have also put their project on hold[25]. The council had, "begun to consider cashless catering in secondary schools using facial recognition, but this has not been progressed."

Data sources

Figures are taken from Freedom of Information requests made in 2018 and 2021 to all Scottish Local Authorities. The Freedom of Information response rate was over 95%.

[25] FOI request to West Lothian Council (January 2022) https://www.whatdotheyknow.com/request/biometric_facial_recognition_use_2#incoming-1947239

Chapter 5: Wales

Data sources

These schools were asked about adoption in 2018 and the response rate was 50%. We are pending responses from 2021-22 and will update this information in the published report online, once available.

There are 1,553 schools in Wales – including 9 nursery schools, 1,219 primary schools, 23 middle schools, 182 secondary schools, 80 independent schools and 40 special schools. (BESA, 2022)

The State of adoption in Wales

In 2008 Caldicott Comprehensive School in Newport, Wales, saw one of the first protests from parents about fingerprint systems, who had not been consulted about its rollout.

In 2018 we made 24 FOI requests to secondary schools in Wales and we found that those that responded used fingerprints for canteen services. The 12 responses indicated that 7 schools used biometrics and 5 did not.

Non-statutory guidance for schools was last updated in Wales in 2021.[26] There are no circumstances in which a school or college can lawfully process a learner's biometric data, without having notified each parent of a child and received the necessary consent.

Since May 2014, the Welsh Ministers must, when exercising any of their functions, have due regard to the requirements of the UNCRC. Under the UNCRC Article 16: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy." As per Article 16(2), "The child has the right to the protection of the law against such interference."

We believe that facial recognition for the purpose of payment is in violation of the Human Rights Act 1998, where the law states that the privacy invasion must be proportionate to the threat, and a potential infringement of rights under the UNCRC and the ECHR.

Furthermore, the UNCRC Committee on the Rights of the Child General comment No.16 (2013) para B(1)(27) says that States should not invest public finances and other resources in business activities that violate children's rights. In order to meet this standard, we suggest that a human rights impact assessment is required.

[26] Non-statutory guidance for schools in Wales https://gov.wales/protection-biometric-information-schools-and-colleges-html

Chapter 6: N. Ireland

The state of adoption in Northern Ireland

There are 1,123 schools in Northern Ireland, including 94 nursery schools, 784 primary schools, 192 secondary schools, 39 special schools and 14 independent schools. (BESA, 2022)

Requests for information ("FOIR") were sent to 26 secondary schools in 2022 and data was received from only 6 schools. Four of those schools were not using biometric technology and two schools were. From the data received, the total roll of pupils from the 6 schools is 4,905. The two schools are using fingerprint biometrics for canteen services with a total on roll 1,333 pupils, of whom 1,323 were pupils using biometrics. Take up rate in schools based on these figures is over 99%.

Due to the limited nature of the data from these recent requests we looked back at previous requests to the same schools in 2018, when the response rate was higher, revealing different data from 2022 replies.

From 14 responses (48% FOIR response rate) 8 schools were using biometrics and 6 were not. All use was fingerprint for canteen use. Based on those response figures from 2018 it showed that 58% of secondary schools were using biometric systems, with a near 100% take up within those schools.

Figures are taken from Freedom of Information requests sent in 2022 and 2018.

Chapter 7: Company data

Whose company are you keeping? asked Fraser Sampson in the foreword. Our research from a total of 550 schools covering a quarter of a million pupils, sets out some of the commercial background of biometrics in schools.

Twenty years ago, in the early days of companies commonly supplying biometric systems to schools there were 14 names, largely independent UK companies. However, the biometric supply market to schools, still with some of the same names, has changed considerably since then. Larger multinational companies have bought out smaller entities and significant UK school biometric providers are now also owned in the US, Canada, and Israel.

Fig. 2 Supplier information to England, Wales and Northern Ireland from the individual schools and MATs that replied to FOI and confirmed they are using fingerprint technology. 'Other' include Vericool, Spie, Sharp and Infineer. 'Paysystems' includes ParentPay and WisePay and suggests a poor understanding of schools between suppliers that provide only cashless payment systems and / or the linked biometric technology.

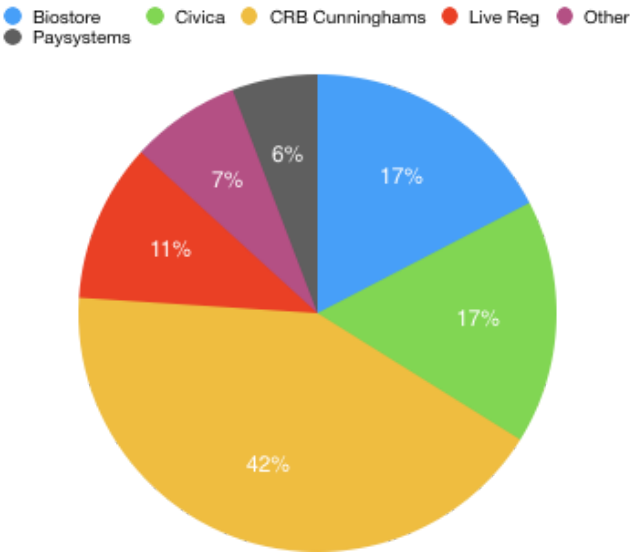
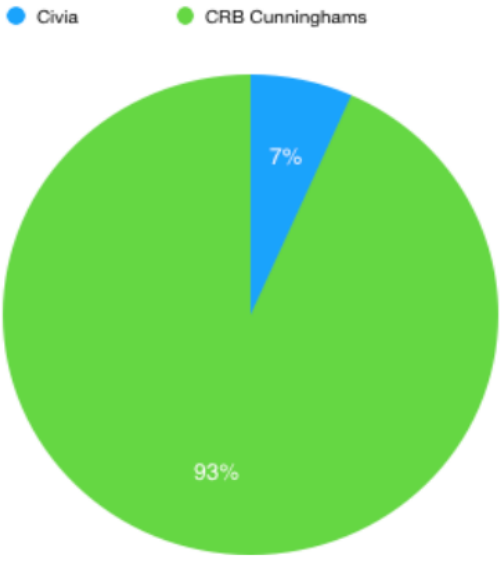


Fig. 3 Data for Scottish suppliers of the market. Data by Local Authority. Fourteen out of fifteen Local Authorities in Scotland (all LAs using biometrics out of the total 32) are supplied by the same company.



The biometric technology

FIngerprint

The fingerprint reader two decades ago was not an 'off the shelf' purchase as it is today and UK schools were the forerunners in the global education sector to use biometric fingerprint readers.

The companies supplying biometric systems to schools are evenly split between long established companies supplying point-of-sale (POS) for over twenty years, to newer companies set up since 2000 to supply the biometric schools market. The companies that supply the schools market specialise in POS delivery in the form of cards, PIN,ID management tills, stock inventory, accounts, and other services. They did not initially develop biometric hardware and software.

In the early days of biometrics being supplied to schools the vendors were transparent about where the technology had come from, essentially originally developed for military uses. Where exactly the biometric tech comes from today, is largely unpublished.

We can look at Vericool's introduction of fingerprint readers in the 2000s, part developed by Anteon UK (of which Vericool was a trademark) as described on Vericool's website from 2008:

> *"VeriCool biometric software utilises the Digital Persona U r U 4000B optical scanner in conjunction with the Neurotechnolojica and Anteon (UK) developed biometric software application. The algorithm used by Digital Persona is unique to them."*

The Digital Persona fingerprint reader was the technology used by Micro Librarian Systems in the early 2000s. Micro Librarian Systems was later acquired by Education Software Solutions ("ESS") of Capita plc. It was reported in 2021[27] that a leading European private equity firm, had agreed to acquire the Education Software Solutions business ("ESS") and also agreed to invest in the ParentPay Group ("ParentPay").

Such commercial decisions and any vertical market integration, open up a range of questions for the implications for control of pupil images and personal data held in core information management systems and their use in biometric systems, and whether there are Chinese Walls between data uses within company groups or systems. This would be another area for further research.

Facial Recognition

With the emergence of facial recognition, and the sophistication of the recent addition that CRB Cunninghams is supplying to schools[28], again it is unclear to parents from published information online who is supplying CRB Cunninghams with this particular facial recognition technology. This type of technology seems new or unique in the way the company describes it as it learns "updated every 3 months" from a changing child's face, continually updating the facial recognition templates to accommodate the growing, changing face.

> "*...algorithm grows with the child*", "*the system will manage… by constantly evolving the algorithm to match the child's growth and change of appearance*".

[27] https://www.ess-sims.co.uk/

[28] ESS (2021) Montagu to acquire ESS business and invest in ParentPay Group | Education Software Solutions. https://www.educationsoftwaresolutions.co.uk/resources/article/montagu-acquire-ess-business-and-invest-parentpay-group

They talk about the first template being scanned from the school MIS system. The second template is being taken to "improve the score associated with the registration." And the "third template is taken at the point of sale… a change in hairstyle, they begin wearing glasses, the algorithm grows with the child." **We believe this suggests the product is still being developed if it 'learns' as it is used and uses the children's personal data (their faces) to do so.**[29]

We asked the ICO whether they were aware where else this type of facial recognition software is used (that rescans the child's face every 3 months for the algorithm to 'learn'), outside CRB Cunninghams use in the UK, with children.

The ICO responded that they don't hold information regarding facial recognition software used on children that specially rescans a child's face every 3 months. And they also said that, *"We can also advise that the software provided by CRB Cunningham's to North Ayrshire Council didn't use facial templates to train its algorithms."*

(From email exchanged between the ICO and Pippa King 9th February 2022)

There appears to be a difference between what the supplier suggests their product does on an ongoing basis in its training for schools, and what the UK regulator understands. We will research this further.

Whose company is our children's biometric data keeping is a good question for school governors and parents to ask of schools.

Major suppliers in the UK market today

Supplier:	Parent Company:	Based:
CRB Cunninghams	Constellation Software	Canada
Gladstone	"	
AMI	"	
Biostore	Iris Software Group	UK
Civica	The Civica Group	UK
National Retail Systems	"	
Live Register	Live Register	UK
Vericool	General Dynamics	USA
Synel	Synel MLL PayWaY Gp	Israel

[29] From 15:20 https://vimeo.com/570313423 or https://marketing.crbcunninghams.co.uk/acton/fs/blocks/showLandingPage/a/35817/p/p-00da/t/page/fm/0

Chapter 8: Points of view

Scottish Parliament, October 2021

The MSP for North East Fife, **Willie Rennie,** asked what the Scottish government position is on facial recognition in schools on October 28th in the Scottish Parliament. The First Minister, **Nicola Sturgeon**, responded that she felt the technologies do not appear to be proportionate or necessary.

House of Lords: Biometric Technologies in Schools, November 4, 2021

Lord Scriven

"If we leave it to individual schools, the unintended consequences and problems that will arise will be not just technical but deeply ethical and societal. There must be a balanced debate within this Parliament and legislation must be brought forward. We have seen the unintended consequences in live facial recognition use by the police when the marketing teams and the technology gets ahead of the legislation. We talk then about the lack of regulation, rather than first talking about where it is acceptable and unacceptable and we start seeing that, as the technology leads, people's rights are trampled on and we try to play catch-up."

"This debate is very fundamental. It is a debate about where we, as a society, draw the line in the use of technology—not about what we do once it is deployed but what the limitations of it are before we start talking about how it is regulated. Where do we draw the line? This cannot be left to individual schools or councils. It is for this Parliament to legislate and to decide where we draw that line."

Lord Clement-Jones

"From the surveys and evidence given to the Ada Lovelace Institute, which has the ongoing Ryder review of the governance of biometric data, it is clear that the public already have strong concerns about the use of this technology. Yet we seem to be conditioning society to accept biometric and surveillance technologies in areas that have nothing to do with national security or crime prevention and detection."

Lord Strasburger

"Will the Government bring forward legislation to impose an urgent moratorium on public authorities' use of live facial recognition technology in order to give Parliament an opportunity to properly assess it before any further harm is done?

Baroness Chisholm of Owlpen

"I cannot believe it will not be discussed at great length as far as legislation is concerned. All the concerns brought up today are very live and important and need a great deal of thought. I will take this back to the Department for Education, but it is the Department for Digital, Culture, Media and Sport which really needs to get involved in this. I think everyone is almost wondering what is coming next."

Children and young people's voices

Young people from Hull and Hackney, shared their views on the question: "What are your thoughts on facial recognition and fingerprints in schools? Should they be used?" (April 2022)

Andi (17)
"The option for me was either you get the biometrics [taken] and I'm able to go to the school, and can participate and can get into the school, you had use your thumbprint to unlock the door, or you just couldn't go to the school...and you could bring your own packed lunch [instead of using fingerprints in the cashless payments system, also for FSM children] but you'd be at more of a disadvantage from everyone else."

Adam (22)
*"Students should be more informed about it so they can make a choice if they want to use it or use other methods like cash or card. What's wrong with just using cards? Fob cards work fine and don't have my unique biometric data attached. Cards and other methods could end up being cancelled (*as a result of moving to biometric scanning in schools*). If fingerprint scanning/ facial recognition is used, children should be educated about how they are used."*

Cyrus (16)
"I don't know..it's cool so I think we should."

Becky (23)
"I think that we should be given the option to decide. We should have more choice…a unique code or number."

Alicia (19)
"I don't think we should be using fingerprint scanning or facial recognition in schools. We had fingerprint scanning at our school for storing lunch money, but for sixth formers they had a separate lanyard/swipe card for their associated documents and information to be stored on, which could also be used to pay for things instead of fingerprint scanning. If you were younger than sixteen they didn't really tell you much about consenting to fingerprints or storing your data. Sixth formers at my school were trusted to use swipe cards. Younger students were not given this trust or choice. College aged young people can give informed consent but the younger children can't if they don't understand it. Children will just say yes cause it sounds cool."

Nadine (17)
"How do we know that catering companies don't sell that information to people or give it away, like to the police? We should have a better voice for the student body before schools bring it in."

Cynthia (25)
"As a newly qualified teacher I resisted my fingerprint being required in my first job but you needed it to use the school printer. I gave in after two weeks."

Looking back before and after the Protection of Freedoms Act 2012

Baroness Walmsley, 2007[30]

"is [the Minister] aware that the practice of fingerprinting in schools has been banned in China as being too intrusive and an infringement of children's rights? Here, it is widespread."

Baroness Carnegy of Lour (2007)

"My Lords, the Minister usually displays a great understanding and sympathy of what it is to be a child. Is he not concerned about the impression that children will get of what it is to live in a free country and what it is to be British if, in order to get the right school meals and other things, they can have their fingerprints taken? That seems completely astonishing to me. I suggest that the Government think hard about this and change their minds."

Dr Julian Huppert (MP for Cambridge in 2012, comment given to authors for this report)

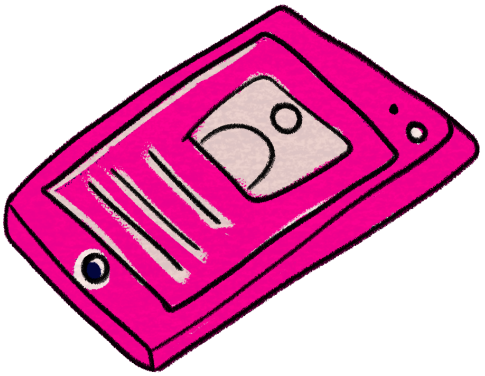
"There is a constant pressure for governments to increase the power they have over their citizens. If unchecked, this leads to increasingly totalitarian states.

"When the Lib Dems entered into the Coalition in 2012, we wanted to unwind some of the unneeded powers that had crept it – and so we insisted on a Protection of Freedoms Act. Originally intended as the first of a series, this took at least some steps to reverse the excessive powers of the state. One of the many good things there were some constraints on the use of biometrics in schools.

"In hindsight, we should have insisted on being bigger and bolder, both in terms of the scope of the Act (the list of items for PoFA II never made progress) and in terms of ensuring proper enforcement. Too often, people have found ways around the protections provided."

Baroness Featherstone (Parliamentary Under-Secretary of State for the Home Department in 2012, comment given to authors for this report)

"I suppose I would say now, 'Thank goodness for the protections' but whoever thought we would have an education system where they are necessary!"



[30] The Houses of Parliament (March 2007) Schools: Biometric Data debate https://publications.parliament.uk/pa/ld200607/ldhansrd/text/70319-0002.htm#0703193000078

Chapter 9: Children's and family rights

Children and parents have rights set out in law that go beyond the Protection of Freedoms Act 2012 and data protection laws.

The rights-protecting articles in the UN Children's Convention on the Rights of the Child are sometimes described grouped under three categories, often known as the "three Ps" – participation, protection and provision.

Cashless payment systems

There is evidence of discrimination of provision and respect for rights through the imposition of cashless payment systems with obligatory use of biometrics upon children in receipt of free school meals.[31] However, it remains for us to research the extent of these issues.

Children and families are deprived of participation, agency and voice in this debate, which means their own views and rights are under-represented in procurement decision-making and consent is almost impossible to be freely given, especially when collected during the school admissions process. Cashless payment providers are well established in the UK. Parentpay alone, for example, claims that "*11,000 UK schools rely on us for best-in-class cashless payments*".

They can work with a variety of verification tools at the canteen checkout including the PIN number / card systems offered alongside fingerprints. Cashless payment systems are also being used increasingly alongside facial recognition. Some companies provide this integrated as part of the cashless payment services, others may be chosen by schools from entirely separate companies.

Cashless payment systems are normalising the expectations and financial norms of online banking, the processes are controlled by companies and not schools. Any associated costs, both monetary and in time, are borne by families which may be

[31] "Accounts must be topped up in advance using the ParentPay system and this can be done either online or via a PayPoint. *Students who qualify for FSM will need to be signed up to the biometric system in order to continue to receive their lunch*." (London) and (Cheshire) https://www.weaverhamhighschool.com/wp-content/uploads/2019/10/Biometrics-Policy-2019.pdf https://www.buxtonschool.org.uk/542/biometric-system

convenient for some, but disadvantages those who cannot afford the Internet access to do so. This creates the potential for social stigma or burden on families that few talk about, perhaps no longer seen in the school lunch queue, but pushed outside of schools instead. Parents may need to use PayPoints[32] in shops instead of paying into the cashless payment system online from home. This removed step makes recourse for redress for mistakes harder to manage, by involving third parties and removing the accountability of the school. We believe that cashless payment systems, all tied into digital systems, widens the gap in the everyday school experience of fair provision of services, between the haves and have-nots but while the digital divide has been analysed in other sectors (Baker et al, 2020) it has not been assessed in such school administration systems as far as we know.

Since the systems are private and proprietary, we are unable to ascertain how many parents use in-shop paypoint systems instead of their own devices. We have contacted IRIS Software Group Ltd, ParentPay, Squid, Tucasi, and WisePay to ask questions on this, and will update the information in this report online, if and when we receive any answers.

Questions over the digital divide, discrimination and ability to exercise rights in families with children in receipt of Pupil Premium or Free School Meals, remain to be explored for the next of stage of this research.

[32] PayPoint Barcodes for Cashless Catering https://parentmail.zendesk.com/hc/en-us/articles/360010494099

The right to privacy

Article 16 of the UNCRC makes clear that children have a specific human right to protection in law from, *"arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation*". These standards imply that children should be given the same levels of protection in their right to privacy as adults.

The right to be heard

Institutional decision-making at school level when it comes to technology rarely involves children, or even families. Despite the UNCRC Article 12 right to express their views, *especially in justice and administrative matters,* the Committee on the Rights of the Child, recognised in 2013[33] that children are often politically voi*celess and…have little influence, to have their rights realised. This makes it hard for them to have a say in decisions regarding laws and policies that impact their rights."*

The UK Office for Statistics Regulation conducted a review of a selection of the key published data available on children and young people during the COVID-19 pandemic. They used the lens of 3V's on vulnerability, visibility, and voice; and concluded that children are rarely heard on data about them, or adequately represented in UK data (The Office for Statistics Regulation, 2022)**.**

There is rarely a route for everyday families to be democratically included in decisions that affect their school procurement such as cashless catering systems or consultation on the controversial installation of CCTV in school bathrooms. The education sector today has no consistent social contract to

[33] Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf

enable and enforce expectations between schools and families or any advocate on behalf of parents at national level.

To enable views to be expressed on data management for example in the NHS, there is a code system to express consent where it is required for repurposing data beyond your GP or hospital records beyond direct care. Today the need to enable a process for the right to object is simply ignored by schools and the Department for Education. Personal data is repurposed for secondary uses beyond a child's own education at local, regional and national levels, that few parents understand. (Survation, 2018)

Parental rights

How children's rights can be exercised must also take *the rights and duties* of parents into consideration, as supported in principle by Articles 5, 18 and the second part of Article 3 in the UNCRC.

In the educational context, parents have a prior right to choose the kind of education that shall be given to their children, grafted onto the child's right to education in the Universal Declaration of Human Rights, and in the European Convention on Human Rights.

This intersection of the rights of the child and rights of the parent in the educational environment needs particular consideration and mechanisms for decisions to be explained, challenged and exercised like opt-in, consent management, and objections.

Withdraw consent

If you or your child agree to use biometrics in schools, consent is valid until such time as it is withdrawn, or when the child leaves the school if agreed in the initial school sign up terms. However, it can be overridden at any time if one parent/legal guardian or the child objects to the processing.

A child can withdraw consent to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after their biometric data has been obtained and is being used as part of a biometric recognition system. If a pupil objects, the school or college must not start to process his or her biometric data or, if they are already doing so, must stop. The child is not obliged to object in writing, although it may be useful. We suggest wording below that one might use in email or in print to withdraw consent. Only a parent/guardian withdrawal of consent must be made in writing, for example asking like this:

WITHDRAWAL OF CONSENT FOR BIOMETRIC DATA PROCESSING IN SCHOOL

_____

I hereby withdraw consent from the school and any data processors for the biometrics of my child (please print name and form/year group).

Child's name .....

Form/year Group .....

Name of Parent .....

Signature .....

Date.....

Chapter 10: Myths and mistakes

When schools deal with the term biometric data in communications to parents or children, claims are made that ‘we are not storing a fingerprint / face’, ‘it is a long number string’. In fact it is a number string that is specific to a child’s unique bodily information, ‘bio’ - life ‘metric’ - measure.

The stored number is unique to the child and relates to their biometric data for the time it is stored and processed on a school or supplier company database. Comparison can be made to the fact a digital photograph is not an actual photograph but a series of coloured pixels, informing the user what the accumulated data is. True for an image - or a number string biometric identifier.

No claims made from industry or school have ever been shown to have been substantiated by independent evidence that using a biometric system improves school services, stops bullying or theft of cash/cards and that healthy eating is encouraged by children using their biometric data. There might possibly be an ease of administrative services if lost cards do not need to be replaced but this potential problem could be solved by implementing a PIN system.

A school’s communication to parents can often be misleading and defend digital me has received complaints from parents when they feel home-school communications are lacking or give a leading suggestion how to “consent” which is not freely given.

Common claims on “Why use biometrics”

- *Convenient way of paying for school meals. No more looking for change every morning*
- *Discourages the misuse of school dinner money through spending in shops outside of the school grounds*
- *Alleviates many of the associated problems with the use of cash in schools. i.e.: Loss, theft and bullying*
- *Specific food allergy ingredients can be barred automatically in the cashless payment system*

- *Healthy eating is encouraged*
- *Queuing times are reduced through increased speed of service*

Claims from suppliers:

Fingerprints - "*Enable and revoke user permissions instantly, implement flexible permissions dependent on individual requirements, including offices, classrooms and lockers, monitor and report on user behaviour"*[34]

Fingerprints and facial recognition claims - *"...eliminate the occurrences of lost cards and security system complications in an example of how biometrics can reduce plastic pollution as well as increase efficiency."*[35]

Facial recognition claims- *"Facial Recognition is fast! In addition to offering a truly contactless solution, one of the main benefits to UK schools is an increased speed of service, with the average serve time currently at 5 seconds per pupil! This truly contactless identification method allows catering teams to safely increase the speed of service by simplifying the payment process for students who no longer need to carry any form of identification such as a card or even enter a PIN."*[36]

We made a FOI request to North Ayrshire Council in autumn 2021 on their use of facial recognition[37]:

Please provide the cost benefit analysis of the new facial recognition system, in other words:

i) time it took on the previous catering system to process children through the lunch line
ii) what that system used i.e. PIN, swipe card
iii) the time it is thought to take with the new facial recognition system
vi) costs saved by each school or by North Ayrshire Council, (annually or monthly) and any plans to incorporate that time to benefit children in school, I.e lunch club extensions, etc.

Response received : ***No cost benefit analysis completed, as the speed of processing was not deemed a deciding factor.***

[34] Iris Software Group https://www.iris.co.uk/solutions/area/biometrics/
[35]Biometric Update (2022) https://www.biometricupdate.com/202204/suprema-face-biometrics-enable-uk-school-to-cut-back-plastic-waste-from-access-cards
[36] CRB Cunninghams https://www.crbcunninghams.co.uk/news/crb-cunninghams-launch-facial-recognition-to-uk-schools

[37]FOI request to North Ayrshire Council, Scotland https://www.whatdotheyknow.com/request/800701/response/1914635/attach/html/3/Response%20101003991085.docx.html

Conclusion

Our key findings from enquiries to schools with over a quarter of a million pupils in total, suggests that around 75% of secondary schools are using fingerprint technology (or other biometrics), and where used, uptake is routinely as high as 85% or more where use is restricted to only certain year groups. Use is still being made obligatory despite the law.

In line with recent decisions on facial recognition in France and Sweden, and fingerprints in Poland, as well as various parts of the U.S. it is time to ban the broad use of biometrics in UK schools, from facial recognition and fingerprints in canteens to AI using bodily data to make inferences of emotional detection and attentiveness through articulated human pose estimation.

Harm is already very real from discrimination and infringement on human dignity in e-proctoring to the imposition of biometrics policy on disadvantaged children in receipt of free school meals. Further risks to the rights and freedoms, and full and free development of the child, may not be fully realised yet. The normalisation and chilling effects of surveillance are already seen in trials. The effects of undermining the importance of biometrics for later in life, in security and identity theft, are foreseeable.

The UK Regulator, the ICO must step in to better protect children's rights and freedoms as recognised under the GDPR, the UK Data Protection Act 2018 and Convention 108. These tools rarely meet the high bar of necessity and proportionality required, since other tools can be used to achieve their aims in less intrusive ways. That should have been a barrier to routine use which consent could have permitted in exceptional circumstances. The intentions of the 2012 Protection of Freedoms Act were strong and should have been a vehicle to drive the increased protection of children's rights in educational settings. But in practice in the ten years since, consent in data protection terms has failed to protect children's rights.

Consent fails (1) as a lawful basis in data protection law for biometric data processing due to the coercive imbalance of power between the child, the family and school authority, affecting its freely given nature. (2) Consent fails where biometrics used in the school or learning environment is not optional, made compulsory through home-school agreements, where choosing 'no' is made more difficult, or with a cost,[38] again making consent invalid, even where parents tick 'agree'. And (3) Tools using biometrics such as facial detection in e-proctoring or emotions detection can infringe upon human rights and human dignity, which data laws fail to adequately address.

The failure to address rights in the field of biometrics in schools is part of a larger failure to understand and implement duty bearers' obligations in the wider application of technology in schools. This must be addressed in initial teacher training and children's digital citizenship curricula as well as in quality standards for school procurement. Stoilova et al concluded in 2020, that, "*since the complexity of the digital environment challenges teachers' capacity to address children's knowledge gaps, businesses, educators, parents and the state must exercise a shared responsibility to create a legible, transparent and privacy-respecting digital environment in which children can exercise genuine choice and agency*".

We first propose a moratorium on all biometric technology and use of bodily data in schools until September 2023 or until the ICO carries out an assessment of the use of children's data across UK educational settings, whichever occurs later. (Face, fingerprints, eye scans, brain, vein and palm patterns, gait, pose and emotional detection and processing.)

[38] "These cards will have to be purchased and administered by the school and it is our intention to pass these costs on to the families". https://web.archive.org/web/20220509235117/https://www.weaverhamhighschool.com/wp-content/uploads/2019/10/Biometrics-Policy-2019.pdf

Appendix A: other FOIR

Date asked	Authority	Response	Reference
28/07/2021	The Department of Education (Westminster)	The DfE does not hold any information on **standards or specifications of any hardware or software of biometric technology used in UK schools.**	https://www.whatdotheyknow.com/request/biometric_technology_in_schools#incoming-1843851
28/07/2021	The Department of Education (Westminster)	The DfE **does not hold any information about suppliers** that provide biometric technology to schools.	https://www.whatdotheyknow.com/request/biometric_technology_in_schools#incoming-1843851
28/07/2021	The Department of Education (Westminster)	The DfE **does not hold any information about the types of biometrics that are used in schools**. i.e. fingerprints, facial recognition, palm, vein or iris scanning.	https://www.whatdotheyknow.com/request/biometric_technology_in_schools#incoming-1843851
17/9/21	The Department of Education (Westminster)	Nor do we provide advice to providers of such [facial recognition] technology. The department's publication [1]Protection of children's biometric information in schools explains the legal duties schools and colleges have if they wish to use biometric information about pupils. (But fails to mention this is long out of date). 2) Please provide your advice to companies which are providers to schools and schools/ educational establishments wishing to use facial recognition technology. (This would include advice ref GDPR and Data Protection Act 2018). 3) Please advise if you have been approached by any companies wishing to supply facial recognition to schools and provide all communications you have had with them, this includes all communications, i.e. minutes of meetings, letters, emails, video calls, etc	https://www.whatdotheyknow.com/request/facial_recognition_use_in_educat#incoming-1878017 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf The above 'Protection of Children's Biometric Information in schools' is out of date. Last update was March 2018 and cites the DPA 1998 4 times, no update on DPA 2018 and GDPR. Needs updating.
2/9/21 Due Back 4th Nov 2021	Information Commissioner's Office (ICO)	• Advice to companies • Working with companies • Facial recognition hardware and software standards to be used in educational establishments?	https://www.whatdotheyknow.com/request/facial_recognition_in_education#outgoing-1198010
8/9/21	Education Scotland	Government does not have the information [on facial recognition in schools] you have requested.	https://www.whatdotheyknow.com/request/facial_recognition_use_in_educat_2#incoming-1871933

Appendix B: Parent views

Survation poll (2018)

Personal Data in School Poll
Prepared on behalf of Defend Digital Me

Table 21
Q21. Regarding the use of the following, has the school offered a choice of whether to use this system for the school's purposes or not? Fingerprints, retinal scans, palm scans, or facial image recognition (any biometric technology)
Base: Respondents whose child's school use Fingerprints, retinal scans, palm scans, or facial image recognition (any biometric technology)

	Total	Gender of Parent		Age of Parent			Gender of Child		Age of Child				Region				School Level				Type of School		
		Male	Female	18-34	35-44	45+	Male	Female	5-8	9-11	12-15	16-18	London	Midlands	North	South	Primary	Secondary	Further education	Higher education	Community school	Academy school	Other
Unweighted Total	252	75	177	78	98	76	154	98	46	52	119	35	52	56	81	63	79	162	9	2	94	96	62
Yes, the school has offered a choice	155 61.5%	52 69.3%	103 58.2%	59 75.6%	54 55.1%	42 55.3%	97 63.0%	58 59.2%	32 69.6%	33 63.5%	73 61.3%	17 48.6%	39 75.0%	31 55.4%	51 63.0%	34 54.0%	56 70.9%	93 57.4%	5 55.6%	1 50.0%	55 58.5%	55 57.3%	45 72.6%
No, the school has not offered a choice	97 38.5%	23 30.7%	74 41.8%	19 24.4%	44 44.9%	34 44.7%	57 37.0%	40 40.8%	14 30.4%	19 36.5%	46 38.7%	18 51.4%	13 25.0%	25 44.6%	30 37.0%	29 46.0%	23 29.1%	69 42.6%	4 44.4%	1 50.0%	39 41.5%	41 42.7%	17 27.4%
SIGMA	252 100.0%	75 100.0%	177 100.0%	78 100.0%	98 100.0%	76 100.0%	154 100.0%	98 100.0%	46 100.0%	52 100.0%	119 100.0%	35 100.0%	52 100.0%	56 100.0%	81 100.0%	63 100.0%	79 100.0%	162 100.0%	9 100.0%	2 100.0%	94 100.0%	96 100.0%	62 100.0%

Personal Data in School Poll
Prepared on behalf of Defend Digital Me

Table 23
Q23. You said your child's school offered a choice to use fingerprints, retinal scans, palm scans or facial image recognition (any biometric technology). Did either you or your child allow these being taken or did you or your child refuse?

Base: Respondents school has offered a choice of Fingerprints, retinal scans, palm scans, or facial image recognition (any biometric technology)

	Total	Gender of Parent		Age of Parent			Gender of Child		Age of Child				Region				School Level				Type of School		
		Male	Female	18-34	35-44	45+	Male	Female	5-8	9-11	12-15	16-18	London	Midlands	North	South	Primary	Secondary	Further education	Higher education	Community school	Academy school	Other
Unweighted Total	155	52	103	59	54	42	97	58	32	33	73	17	39	31	51	34	56	93	5	1	55	55	45
I/my child allowed these being taken	116 74.8%	36 69.2%	80 77.7%	37 62.7%	41 75.9%	38 90.5%	74 76.3%	42 72.4%	16 50.0%	23 69.7%	63 86.3%	14 82.4%	29 74.4%	22 71.0%	44 86.3%	21 61.8%	31 55.4%	79 84.9%	5 100.0%	1 100.0%	40 72.7%	41 74.5%	35 77.8%
I/my child refused these being taken	39 25.2%	16 30.8%	23 22.3%	22 37.3%	13 24.1%	4 9.5%	23 23.7%	16 27.6%	16 50.0%	10 30.3%	10 13.7%	3 17.6%	10 25.6%	9 29.0%	7 13.7%	13 38.2%	25 44.6%	14 15.1%	- -	- -	15 27.3%	14 25.5%	10 22.2%
SIGMA	155 100.0%	52 100.0%	103 100.0%	59 100.0%	54 100.0%	42 100.0%	97 100.0%	58 100.0%	32 100.0%	33 100.0%	73 100.0%	17 100.0%	39 100.0%	31 100.0%	51 100.0%	34 100.0%	56 100.0%	93 100.0%	5 100.0%	1 100.0%	55 100.0%	55 100.0%	45 100.0%

Personal Data in School Poll
Prepared on behalf of Defend Digital Me

Table 24
Q24. Were you informed of how long the fingerprint, retinal scan, palm scan or facial image recognition data (any biometric technology) are kept by either the school or the company that provides the service?

Base: Respondents whose child's school use Fingerprints, retinal scans, palm scans, or facial image recognition (any biometric technology)

	Total	Gender of Parent		Age of Parent			Gender of Child		Age of Child				Region				School Level				Type of School		
		Male	Female	18-34	35-44	45+	Male	Female	5-8	9-11	12-15	16-18	London	Midlands	North	South	Primary	Secondary	Further education	Higher education	Community school	Academy school	Other
Unweighted Total	252	75	177	78	98	76	154	98	46	52	119	35	52	56	81	63	79	162	9	2	94	96	62
Yes, I was informed of how long the data are kept for	127 50.4%	43 57.3%	84 47.5%	46 59.0%	43 43.9%	38 50.0%	74 48.1%	53 54.1%	31 67.4%	25 48.1%	54 45.4%	17 48.6%	32 61.5%	25 44.6%	40 49.4%	30 47.6%	47 59.5%	73 45.1%	6 66.7%	1 50.0%	46 48.9%	51 53.1%	30 48.4%
No, I was not informed of how long the data is kept for	125 49.6%	32 42.7%	93 52.5%	32 41.0%	55 56.1%	38 50.0%	80 51.9%	45 45.9%	15 32.6%	27 51.9%	65 54.6%	18 51.4%	20 38.5%	31 55.4%	41 50.6%	33 52.4%	32 40.5%	89 54.9%	3 33.3%	1 50.0%	48 51.1%	45 46.9%	32 51.6%
SIGMA	252 100.0%	75 100.0%	177 100.0%	78 100.0%	98 100.0%	76 100.0%	154 100.0%	98 100.0%	46 100.0%	52 100.0%	119 100.0%	35 100.0%	52 100.0%	56 100.0%	81 100.0%	63 100.0%	79 100.0%	162 100.0%	9 100.0%	2 100.0%	94 100.0%	96 100.0%	62 100.0%

Survation (2018) poll on behalf of defenddigitalme in February 2018 of 1,004 parents with children aged 5-18 in state schools

https://defenddigitalme.com/2018/03/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/

Full survey and response tables
https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

Appendix C: Biometrics around the world

Poland

In February 2020, the President of the Personal Data Protection Office of Poland (PUODO) imposed a fine of PLN 20,000 (EUR 4,700) on a Primary School in Gdańsk for unlawful processing of children's biometric data when using the school canteen. In this case the UODO found that the consent given by the parents was not valid in particular because of the imbalance of power between the parties, hence the processing of biometric data did not have a valid legal basis. It also stressed that the identification of the students could have been achieved through less intrusive means. For the mentioned reasons, the UODO ordered the primary school to delete the biometric data concerned, and to cease the collection.
Poland: Fingerprint

Elsewhere in Europe

France: Facial Recognition 2019 "*...on proportionality and data minimization. It was concluded that the goals the facial-recognition program would help reach could "be achieved by much less intrusive means in terms of privacy and individual freedoms." "In this context, and in the presence of less intrusive alternative means, such as badge control, the use of a facial recognition device to control access to a high school appears disproportionate.*
Such a device cannot therefore be legally implemented and it is now up to the region and the high schools concerned, responsible for the planned device, to draw the consequences."

Sweden: Facial Recognition 2019 The Swedish DPA fined a municipality 200 000 SEK (approximately 20 000 euros) for using facial recognition technology to monitor the attendance of students in school. "*...the Swedish DPA considers that consent was not a valid legal basis given the clear imbalance between the data subject and the controller.*"

Bulgaria: Facial Recognition - "*It should be noted that consent in the hierarchical relationship between employer and employee, by analogy between principal and student, is an inappropriate ground for suspicion that it is not freely given." "Consent can only be valid if the data subject is able to make a real choice and there is no risk of fraud, intimidation, coercion or significant negative consequences (e.g. significant additional costs, non-admission to the workplace, etc.), if the person does not agree."*

The EDPB and EDPS joint opinion on the European Commission's Proposal for a Regulation laying down harmonised rules on artificial intelligence (AI). *"Taking into account the extremely high risks posed by remote biometric identification of individuals in publicly accessible spaces, the EDPB and the EDPS call for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context."*

USA

In the USA schools use fingerprint, infrared palm scanning and facial recognition technology, the latter not without controversy. Out of the 50 states in America there are only 6 states that have legislation with regards to biometric technology in schools, 3 states dealing with consent and one, Florida, banning the use of biometric technology completely.New York State issued a moratorium on all biometric technology in schools from 2019 until July 2022 after a consideration consultation period with a variety of public and private bodies.

US legislation on biometric technology use in schools includes

New York Assembly Bill A6787D March 2019

Governor Cuomo signed AB A6787D which, among other things, prohibited the use of biometric identifying technology in schools at least until July 1, 2022.

a. "biometric identifying technology" shall mean any tool using an automated or semi-automated process that assists in verifying a person's identity based on a person's biometric information.

b. "biometric information" shall mean any measurable physical, physiological or behavioral characteristics that are attributable to a person, including but not limited to facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but are not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry.

c. "facial recognition" shall mean any tool using an automated or semi-automated process that assists in uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's face.

Michigan Legal Opinion No. 7069 December 2000. The Child Identification and Protection Act prohibits a school district from using electronic fingerprinting technology to identify a child for school-related purposes. The Child Identification and Protection Act (Act), 1985 AN ACT to safeguard the privacy of children by regulating the fingerprinting of children." With some limited exceptions [...] the Act provides that "a governmental unit shall not fingerprint a child." Section 3. The Act defines "[c]hild" to be a person under 17 years of age.

Illinois SB 1702 2007. Sets forth conditions for collecting and using the information including written consent if using biometric technology in schools.

Florida SB188 April 2014. Banning the use of biometrics in schools. Schools "*may not: (a) Collect, obtain, or retain information on the...biometric information of a student*" this includes physical and behavioural traits.

The New York State Senate Assembly Bill A6787D - March 2019. "Public and nonpublic elementary and secondary schools, including charter schools, shall be prohibited from purchasing or utilising biometric identifying technology for any purpose, including school security, until July 1st 2022 or until the Commissioner authorises such purchase or utilisation as provided in subdivision 3 or this section, whichever occurs later."

Methodology

The data used in this report has been obtained under Freedom of Information Act requests to schools over the past 10 years first in 2010 during pre-legislative discussion for the Protection of Freedoms Bill. Following this a second set of FOI asked similar questions in 2018, and the most recent round was made to the same schools in 2021-22, as well as addressing FOI to twelve of the largest Multi-Academy Trusts (MATs).

The structure of the education system in England has changed considerably over this time period as the result of academisation which changes the nature of the legal entity of the school and its reporting structure. This makes public scrutiny and accountability through FOI requests more difficult because Local Authorities no longer have oversight or responsibility for academies and can no longer be asked for information on all schools within their region.

We are alert to the challenges of obtaining quality data in this subject area. The returns per country / devolved nation reflect poor response rates despite their public sector obligations under the FOI Act and at the same time, in the COVID-19 pandemic we are alert to the unique challenges that schools and the education sector have faced in recent months. It is difficult to make assertions of trends or shares of schools using biometrics with absolute certainty, due to the closed nature of the data but any opinions in the report reflect the nature of the available data and expertise of the authors to give as good a picture as possible of the current situation.

Next steps

We are keen to continue to research three main areas of work in this subject.

(1) positive exceptions in the use of biometric technology in educational settings for accessibility needs (e.g. eye controls of systems for children with disabilities).

(2) to assess the discriminatory effect on take up for children eligible for Free School Meals and the effects of cashless payment systems on families in disadvantaged areas.

(3) The commercial infrastructure of the industry and its changing ownership through mergers and acquisitions, in particular vertical takeovers, is of significance to the future stability of the provision of school services and deserves more attention.

We intend to continue this work and welcome questions or ideas for collaboration.

References

Baker, C. et al. (2020) COVID-19 and the digital divide. UK Parliament briefing. https://post.parliament.uk/covid-19-and-the-digital-divide/

BESA (2022) Key UK education statistics. https://www.besa.org.uk/key-uk-education-statistics/

Bulgarian data protection authority (2020) Opinion on the unlawfulness of facial recognition in schools https://www.cpdp.bg/?p=element_view&aid=2261

Council of Europe (2018) Modernised Convention 108. Convention for the protection of individuals with regard to the processing of personal data. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Council of Europe (2020) Guidelines for the protection of personal data in educational settings. Committee on Convention 108. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Department for Education (2018) Protection of children's biometric information https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Department for Education (2022) Schools, pupils and their characteristics 2020/21 https://explore-education-statistics.service.gov.uk/find-statistics/school-pupils-and-their-characteristics

European Data Protection Board (2019) Facial recognition, Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en

European Data Protection Board (EDPB) and EDPS (2021) Call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

House of Lords November 4 Biometric Recognition Technologies in Schools Hansard, Volume 815 https://hansard.parliament.uk/lords/2021-11-04/debates/26FB2DF4-8D5A-456B-AFDA-73501D1CCBD3/BiometricRecognitionTechnologiesInSchools

ICO (2021) What is special category data? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

Scottish Parliament (28 Oct 2021) Facial Recognition Technology (Schools) https://archive2021.parliament.scot/parliamentarybusiness/report.aspx?r=13373&mode=html#iob_121339

Stoilova, M., Livingstone, S. and Nandagiri, R. (2020) 'Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy', *Media and Communication*, 8(4), pp. 197–207. doi:10.17645/mac.v8i4.3407.

Survation (2018) Poll on behalf of defenddigitalme in February 2018 https://defenddigitalme.com/2018/03/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/ Full tables https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

Comments contributed by the French Data Protection Authority, the CNIL, in relation to the facial recognition programs carried out at the entrance of high schools as response to the PACA regional Council (October 2019):

"The CNIL considers that facial recognition devices in high schools, insofar as this kind of processing is particularly intrusive and entails major risks of infringing the privacy and individual freedoms of minors, is contrary to the main principles of proportionality and minimization of data provided by the GDPR.

Indeed, the objectives of securing and streamlining entrances to these high schools can be achieved by means that are much less intrusive in terms of privacy and individual freedoms, such as badge control, for example. Such devices cannot therefore be legally implemented, even though the students gave their consent to the processing".

Arguments outlined by French regional court in its decision published in 2020:

"If the processing is based on consent as legal basis, given the imbalance of power between the data subject and the heads of the public schools/ educational establishments concerned, the data controller must provide appropriate safeguards to obtain from high school students or their legal guardians that consent is given for the collection of their personal data in a free and informed manner.

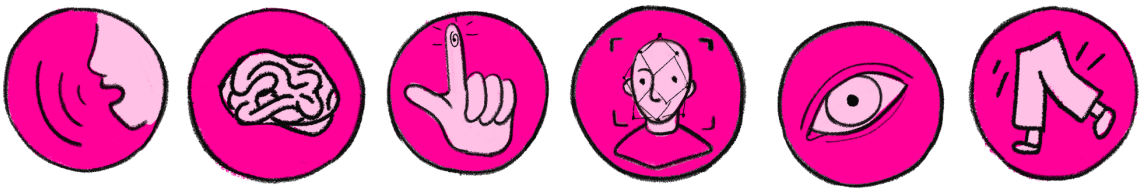
The data controller must establish and assert that the intended purpose of making access control at the entrance of the high schools more flexible and secure is carried out in a public interest and that these objectives could not be achieved in a sufficiently effective way by means of badge controls, supported, where appropriate, by the use of CCTV."

"As parents you should be very worried and angry that private companies are seeking to make a profit from your child's face, fingers, eyes and other personal characteristics while trying to pretend that it is to aid their educational attainment. It's time that as law makers in Parliament we stood up and say as a matter of principle that this isn't required. Children's faces and other biometrics shouldn't be used as a gatekeeper to access the full education services in our schools."

Lord Paul Scriven

"At a time when intrusive surveillance and data hoarding is rapidly expanding across Britain's schools, this report is a milestone in defenddigitalme's vital work illuminating serious legal and policy issues in order to protect children's rights for today and the future."

Silkie Carlo, Director, Big Brother Watch



defenddigitalme.org
May 2022