

Biometrics in schools

Oversight of schools' ICT policy has, for the past decade, been delegated to the British Educational Computing and Technology Agency (BECTA), a Non-Departmental Public Body of the Department for Children, Schools and Families. BECTA has now been abolished and the return of responsibility to the Department of Education is welcome. For several years our attempts to engage the DCSF on issues involving ICT in schools, particularly on the use of biometrics and on data security, have been frustrated as we were repeatedly referred back to BECTA, which had no power to enforce the guidance that it issued. In consequence, effective governance of ICT in schools has, in our view, been extremely poor.

From small beginnings, biometric usage in schools has increased rapidly in the last few years. In 2001, a company called Microlibrarian systems (MLS) approached the UK Information Commissioner's Office (ICO) to ask for comments on the company's plans to incorporate biometric fingerprint readers into school library systems, replacing the use of cards. The ICO raised no objections and in fact supplied MLS with a letter endorsing the use of fingerprints. MLS then approached the DfES (as it then was) with this letter, and the use of biometrics was approved.

By 2007, it had become clear that increasing numbers of schools were installing biometric technology. A councillor¹ in Enfield, for example, found that 15 of the 92 schools in Edmonton were already using it, while MLS estimated that approximately 30% of schools had bought its library system. At that time we estimated that more than two million children were regularly using biometric systems and undoubtedly the numbers have since increased. There are now at least 34 companies selling biometric systems, and their use has gradually expanded from school libraries to schools meals, school lockers, zone control and registration. PFI schemes and the 'Building Schools for the Future' programme have led to the incorporation of biometric systems into the fabric of some schools.

Primarily the biometric data that children currently give in UK schools are fingerprints. Retinal scanning was trialled in 2004 at the Venerable Bede Church of England School in Ryhope, Sunderland, but the experiment was not successful². Palm-vein systems were first trialled in a primary school in Scotland in 2007. By the time of the 2010 BETT exhibition in January, the biometrics systems on offer to schools included infra-red face recognition³, finger vein scanners⁴ and fingerprint scanners.

¹ <http://pippaking.blogspot.com/2007/08/how-many-children.html>

² <http://news.bbc.co.uk/1/hi/england/tyne/3652638.stm>

³ <http://www.bettshow.com/page.cfm/Action=Exhib/ExhibID=1010>

⁴ <http://www.bettshow.com/page.cfm/Action=Press/PressID=373>

It has proved difficult to obtain figures for the number of biometric systems in use, and the total cost to the public purse. Biometric systems are generally incorporated into larger 'cashless catering' packages, or into the purchase of library, locker and registration systems, either under an annual licence fee or sold as an 'add on'. DCSF and BECTA have never held information about the amount spent by schools on these systems. FOI requests to schools show that funding comes from a variety of sources including local authority grants; e-learning credits and Primary Care Trusts.

Schools in the UK do not report whether or not they hold children's biometric data to their local authority or to the Department of Education. Some do register the retention of the data with the Information Commissioner but this is sporadic and inconsistent. Trying to gather accurate figures for the numbers of children using biometrics systems in schools has thus involved the laborious process of making FOI requests to each individual school, but this has been hampered by schools' poor understanding of their responsibilities under FOIA.

In 2006, we asked more than 600 schools about their use of biometrics, but the response rate was only 19%. We subsequently held discussions with ICO staff, who undertook to improve the guidance given to schools. However, this clearly had only a limited effect: FOI requests to over 500 schools in March 2010 have resulted in replies from 43% of them. The ICO has now agreed to adopt a more vigorous approach, but in the meantime the means of collecting accurate figures of biometric usage within schools remain elusive, and until the situation improves, figures can only be extrapolated from whatever data is available.

There has been no specific research into the effects of school biometric systems upon the subsequent development of children's attitudes to their biometric data. As the systems are not widely used outside school, there are few opportunities for children to consider the pros and cons. They may not even discuss the issue: schools do not always inform parents/carers that the systems are in place and if the taking of fingerprints is treated as merely a routine procedure, it may not occur to a child to mention it at home.

Schools themselves appear to rely upon BECTA and on those selling the systems for their information. A series of FOI requests and PQs in 2007 established that neither the DCSF nor BECTA had ever commissioned any independent research into the efficacy or security of the systems used in schools. In other words they, too, were relying upon manufacturers' assurances and on the fact that the Information Commissioner had 'endorsed' use of the product (although this appears to have been without any investigation of manufacturers' claims).

It has become clear that aggressive marketing tactics are used to promote systems. On several occasions, parents have told us that they have been invited to a single consultation meeting at which the system supplier and head teacher have waxed lyrical about the benefits, but criticism and difficult questions have quickly been silenced. Some companies have engaged PR firms in order to promote their systems. Livewire PR, for example, were engaged by 'Vericool' to provide 'crisis management' for its registration system and describes its tactics as follows:

- *Ensured that all news releases included implementation advice from the Department for Children Schools and Families (DCSF) – a guideline developed in association with VeriCool.*
- *Used 'superfan schools' to highlight the positive benefits of biometrics in education.*

- Secured coverage on new school installations within the local media in a drive to educate parents about biometrics and dispel any myths surrounding fingertip technology.
- Commenced executive profiling programme for VeriCool spokespeople to educate teachers and parents about the benefits of biometrics.⁵

Suppliers of biometric systems – and BECTA – have claimed that using biometric technology frees up teaching time by shortening registration; it improves the rate at which library books are issued; it encourages healthy eating habits and it reduces the cost of replacing lost swipe cards. These claims have yet to be proven.

“Such systems can save considerable staff time and effort in taking registers”⁶

“There is reduced opportunity for bullying and theft”⁷

Schools using biometric systems may find that there are administrative benefits by comparison with manual systems, but whether the same advantages apply when biometric systems are compared to less invasive pin number or swipe card systems is unknown.

Some useful research has been carried out into children’s knowledge of the potential disadvantages of biometric systems. The Trustguide⁸ report, published in October 2006, was the result of a collaborative research project between BT Group and HP Labs, partly funded by the DTI’s Sciencewise programme. During this project, children using the technology were interviewed and researchers reported:

“...in some of the groups we discovered that their school used fingerprinting to take books out of the library. Once again, there seemed to be little consideration for the potential infringement to privacy or civil rights this posed.

We asked children how long the school kept their fingerprint records and found that most [school children] had not even considered this question and showed little concern:

We considered why this apathy existed. It seemed that none of the attendees [school children] were thinking beyond the immediate scenario or what they had been told from ‘trusted’ sources (i.e. their parents, their teachers, or the community policeman). They felt that they could not challenge this viewpoint, or present any alternative views.”

From these observations it seems that a child using this technology, even at an age when they might understand the concept, is simply not receiving sufficient information or opportunity to consider the importance of biometric data. This increases our concern that the repeated, routine use of biometrics for trivial purposes may serve to desensitise children to the significant, irreplaceable nature of their biometric data, and allow the development of a casual attitude that has long-term implications for its security.

⁵ <http://www.livewirepr.com/clients/case-studies/vericool-crisis-management.html>

⁶ http://schools.becta.org.uk/upload-dir/downloads/becta_guidance_on_biometric_technologies_in_schools.doc

⁷ http://schools.becta.org.uk/upload-dir/downloads/becta_guidance_on_biometric_technologies_in_schools.doc

⁸ <http://www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf>

Until 2007, there was no guidance to schools relating to the practice of the use of biometric systems with children until, in response to persistent campaigning, BECTA and the Information Commissioner both issued guidance in July 2007. Subsequent FOI requests to DCSF, BECTA and the ICO established that they had not carried out any consultation in the course of preparing this.

It is a source of concern that no apparent control has been exercised over the expansion in the use of biometric systems. Figures are not collected centrally; the amount of public money involved has not been monitored, and neither government nor the ICO has commissioned any research whatsoever into the security and implications of the systems that they are so readily endorsing.

It is perhaps unsurprising that parents, children and teachers have so little knowledge of biometric systems when a hierarchy of ignorance has been established, beginning with those whose judgment the public might reasonably be entitled to trust. In reality, the ICO and the government appear to have based their endorsements entirely upon the assurances of biometric system suppliers. In turn, head teachers and school governors rely upon these endorsements; parents and children in turn rely upon school staff and thus an ill-informed and somewhat gullible chain of consumers has been created in UK schools

This reckless approach to biometric technologies creates the further danger that schools may be providing a captive test-bed for new systems, without the protection of the ethical standards that normally govern research with children.

The systems are undoubtedly costing a great deal of public money, but whether they are necessary or provide good value is highly debatable. Many of the technologies have been transferred from the defence arena, but there is a considerable difference between the authentication requirements of a national defence programme and the needs of a primary school canteen. If biometrics are to retain any integrity in situations where security is critical, it seems foolhardy to encourage children in the idea that they can routinely be given up for trivial purposes.

The Government's commitment to introduce consent into the process of taking children's biometric data is very welcome. However, simply to request consent is not enough: in order to be valid, it must be properly informed. This requires independent research into the claims of biometric system suppliers so that authoritative material can be produced to inform the decisions of parents and young people.

There is also the question of how the gaining of consent will be policed to ensure that it is properly valid: that is, informed and voluntary consent from a person who has the capacity to offer it. In addition, will consent be revisited for those whose biometric data has already been collected? The whole issue of consent – and oversight – presents a considerable challenge.