

Biometrics in school

Sophie McKeand

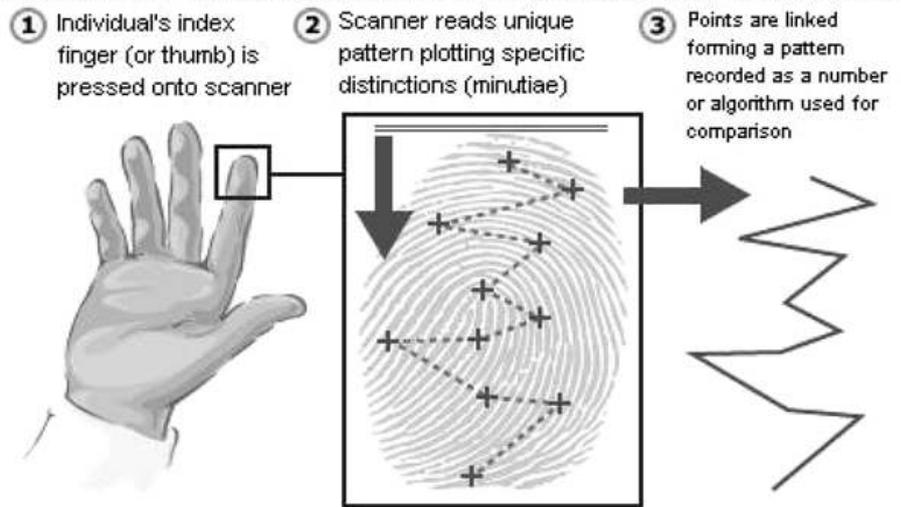
A variety of biometric systems are being installed in schools across the UK at an alarming rate without explicit parental consent.

Children as young as five are being fingerprinted by state schools, and authorities have taken sensitive biometric data from thousands of children without seeking parents' permission. Over two million children have already been fingerprinted by the state and these figures are rising daily. Backed by the government, many schools and local authorities are introducing these supposedly innocuous systems in order to better manage certain school administrative duties such as attendance records, library systems and to improve the efficiency of school dinner queues.

The benefits touted by the manufacturers are apparently many. But who are the people that manufacture and sell these systems in the UK? Research reveals that some of these manufacturers have connections with, or are owned outright by, companies who are more used to tracking 'enemy combatants' than children. *Vericool*, a major supplier of biometric systems in schools, is owned by *Anteon UK*, itself a subsidiary of *General Dynamics* - an organisation that profits directly from war through developing combat systems for the US Government and its allies. See this website: www.generaldynamics.com or perhaps this post on You Tube is more accurate: www.youtube.com/watch?v=7t4IzvPEJw. Do we really trust these organisations with our children's biometric data?

Freedom of Information (FOI) request replies from local councils concerning the introduction of a 'cashless biometric catering system' in schools states that these systems offer wonder cures for problems such as children being bullied for their lunch money and children who have state funded meals being stigmatised by their peers. However, despite numerous FOI requests, neither school nor council are able to offer exact figures concerning the number of children who are affected by these issues. Could it be because there are no cases? When asked if they were bullied for lunch money, or knew of it happening, a number of children who attend one such school replied, "Of

HOW POLICE AND SCHOOL FINGERPRINT SCANNERS RECORD IDENTITIES



www.leavethemkidsalone.com

course not; this isn't some American teen movie!" If bullying is as prevalent in our schools as we are being told, then shouldn't schools have solid 'anti-bullying' policies in place rather than fingerprinting the entire school like criminals?

Shockingly, recent FOI replies from Flintshire County Council's Catering Services Department (which installed a biometric cashless catering system in Mold Alun and Elfyd High Schools) state that the cost of installing the system in just one school is £25,149.46 with annual running costs of £1,967.40 (which you can guarantee is a conservative estimate and will rise!). Now obviously you would expect that before a council department undertakes to spend such a vast amount of public funds (the plan was to roll this system out across ALL schools in Flintshire), then a full 'cost versus benefit' analysis would be carried out in order to ensure that this money was being properly spent. A further FOI request asked for: *ALL cost/benefit analyses that have been completed concerning anything whatsoever to do with implementing these cashless systems in Flintshire schools. Not just for Mold Alun but for all schools in Flintshire... This includes all equipment, maintenance and IT services.*

The astonishingly incompetent reply was that: *the Council holds no information regarding a cost/benefit analysis. The*

commonly perceived benefits, however, are... [followed by the usual corporate nonsense about bullying and healthy eating].

No information? Further investigations reveal that there is no information because no such analysis has been carried out. How, then, can the council assure the public that these systems are beneficial when there is no evidence for these assumed benefits? This smacks of incompetence of the highest order!

Most worrying is the fact that children across the country are being institutionalised to accept disgraceful levels of monitoring by the state at a very young and impressionable age. If children are groomed to hand over sensitive biometric data to the school then they will not question a government that makes such intrusive requests either.

The question of the security of these systems is one that has been raised repeatedly by parents who rightfully object to their innocent children being fingerprinted like criminals. How are local and central government handling these legitimate concerns? By treating those parents who do object like criminals, busybodies and trouble-makers. Parents are told that the systems are safe and that is an end to it, very little evidence is offered to back these assertions, and much of the information given is misleading, can be easily refuted or is simply

Fingerprinting kids without consent

wrong. The manufacturers claim that the child's fingerprint is not stored; a number that correlates to the print is saved which would be useless to anybody else. This is not true; the number is unique to that child's print and so the print can be reconstructed from the stored data - see diagram opposite. A similar system is used by the police in this country to fingerprint criminals and the police are able to identify people from the number they have stored on their databases.

Kim Cameron, Architect of Identity and Access at Microsoft said in 2007: *If you want to find out who owns a fingerprint, just convert the fingerprint to a template and do a search for the template in one of these databases. Call the template a binary number if you want to. The point is that all you need to save in the database is the number. Later, when you come across a 'fingerprint of interest', you just convert it to a number and search for it. Law enforcement can use this information - and so can criminals.*

In addition, government experts have successfully hacked and retrieved fingerprints from a digital scanner such as those currently being installed in schools; how long before criminals can do the same? Identity theft is a hot topic at the moment; can we really rely on this incompetent government or warmongers to safely hold such important biometric data? And if our children's data is stolen, the consequences for them are horrendous. If compromised, a bank account can be closed down or new numbers issued, but it is not possible to change biometric data. Once that is in the wrong hands it can never be rectified. Schools are not able to provide the levels of security needed for such sensitive information, and they should not be asked to squander valuable funds on safeguarding data that they have no right to hold in the first place.

On a local level, in a complete U-turn, Flintshire County Council now states that it has no plans to roll the biometric

cashless catering systems out across any further schools (at present) and a pin number option is available in Mold Alun for parents who object.

Wrexham County Council currently operates a cashless catering system that uses swipe cards or pin numbers; at the time of writing I am not aware of any biometric systems being used. However, it is important to remember that existing systems can be 'updated' to biometrics at any time. Denbighshire council, on the other hand, has taken the draconian measure of getting the systems installed in the blink of an eye without offering parents any option but biometric. In order to eat, the children must be fingerprinted.

For further information or to join the fight against 'kiddyprinting', visit:
www.leavethemkidsalone.com
 email: s.mckeand@btinternet.com
 or call: **07903 775422**



www.bovlomov.com