ARCH REPORT

Child Tracking: Biometrics in Schools & Mobile Location Devices

During the past five years, developments in Information Technology have created unprecedented opportunities for observing children and young people, for supervising and controlling their activities and for gathering and sharing information about their lives. While awareness has grown of the use of databases to store and share children's personal information, less attention has been paid to the increasing number of commercially-available devices that are used to track children's movements and habits. These range from the routine use of CCTV in schools or webcams in nurseries to devices that purport to reveal the exact location of a child at any given moment. It is now possible for a child to be under near-constant scrutiny throughout each day. Because the expansion in the use of IT has been piecemeal, many commercial technologies are inadequately regulated and there is no overview of the combined effect of the different forms of surveillance on children's development.

Over-confidence in technological solutions and poor standards of information security can threaten the integrity of children's personal information and place children at increased risk of harm. The potential for children to become habituated to accept a far higher level of surveillance than society now tolerates is considerable. Children's rights to privacy, guaranteed by the European Convention on Human Rights and underscored by the UN Convention on the Rights of the Child, are gradually being eroded.

Many different types of surveillance technology are available, each raising important questions about consent, safety and the consequences of treating children as passive objects of adult scrutiny. In this report, we have chosen to focus on the two areas that we believe are in urgent need of regulation: the use of children's biometric data in schools, and the use of GPS and mobile phones to track a child's location.

Biometrics in schools

Since 2001 the use of children's biometric data for school library book issue, lunch systems, registration, vending machines and access to computer networks has been growing steadily. Early experiments in the use of retinal scans were halted because the process was too slow, so currently the type of biometric normally used is a child's thumb or fingerprint.

The fingerprint itself is not stored: a template is created from repeated scans and the identifying characteristics of the print are then reduced to a string of numbers. Each time a child touches the scanner another template is created and run through the database to check for a near match.

Biometric systems are used not only for administrative convenience; they can also monitor children's behaviour. Library systems can create reports of children's reading habits broken down by gender, age and ethnicity.[1] Canteen systems monitor children's individual eating habits and can provide parents with printouts of their child's daily meal choices. Claims have been made that these systems provide solutions to all kinds of popular concerns such as obesity and poor literacy, but there is no evidence to support this. Following a literature review, Dr Sandra Leaton Gray of Cambridge University concluded:

"I have not been able to find a single piece of published research which suggests that the use of biometrics in schools promotes healthy eating or improves reading skills amongst children. I am concerned that these reasons are being given as a justification for fingerprinting children. There is absolutely no evidence for such claims." [2]

Schools may use eLearning credits to subsidise purchase of biometric systems, or they may buy them out of school budgets, with costs ranging from a few hundred pounds for an 'add on' scanner to £25,000 for a biometric lunch system. Under the 'Building Schools for the Future' programme, biometric technologies are being built into refurbished and new build schools. Biometric companies are forming partnerships with PFI bidders so that schools can be biometrically streamlined, utilizing every possible application of the technology.[3]

Children's private data is becoming ever more available to a wide range of people, but there is little awareness of the way in which this can be exploited commercially, nor the personal profiling that it allows. We have already seen the way in which Capita used the

‘Connexions Card’, a now-defunct government incentive card for teenagers, to build consumer profiles of young people based on the pages that they browsed on the Connexions Card website. The profiles were used to target marketing material from other companies.[4] Capita went on to promote the card as proof of age, selling card readers to bars and shops.

Britain is the only country in Europe to use biometric technology extensively in schools. While Ireland has low usage, their data commissioner has issued strict guidance[5] to minimise any possible claims for damages from a student in future.

There are undoubtedly data security implications for the use of biometric systems. Police are able to access school databases to aid in the investigation of crime.[6] Inadequate data cleansing, careless disposal of computer hard drives[7] and the prevalence of theft of IT equipment from schools present serious threats to the future integrity of children’s fingerprints. A fingerprint is for life and, if its integrity is compromised, cannot be replaced as if it were a PIN number. Biometric templates are transferable to other databases. Manufacturers’ assurances that data is encrypted are likely to become meaningless with developments in IT and increased computing speed.

It is not enough to say that a system is relatively secure now: nobody can guarantee that it will remain so. As biometrics are increasingly used for security-critical functions such as passports or ID cards, so will the market develop in illicitly-obtained biometric data. This not only places a heavy responsibility upon adults to guarantee the security of children’s data; it means that we should also be instilling in children a sense of the importance of biometrics and discouraging them from giving them up for low-level purposes.

The Minister for Schools,[8] the Information Commissioner,[9] biometric vendors[10],[11] and schools themselves have repeatedly claimed that fingerprints cannot be reconstructed from templates, but even if this were not open to debate, it is a red herring. If a biometric template can be correlated across systems,[12] then there is no need to reconstruct the fingerprint. Many academics, in any case, disagree that fingerprints cannot be reverse-engineered and have published plausible evidence of the reconstruction of images from templates. [13]

Recent concern has focused on the fact that children's biometrics are taken without parental consent, and sometimes even without their knowledge. In January 2007 the Minister for Schools promised that non-statutory guidance would be produced for schools. After repeated delays, this was placed on the website of the British Educational Communications and Technology Agency (BECTA) in July 2007 [14] to coincide with a House of Commons adjournment debate on the subject. The Information Commissioner issued his own guidance [15] simultaneously, which advises that:

"Where a school cannot be certain that a child understands the implications of giving their fingerprint, the school must fully involve parents to ensure the information is obtained fairly. In circumstances where children are not in a position to understand, failure to inform parents and seek their approval is likely to breach the Data Protection Act."

This does not give schools adequate guidance on the steps necessary for the assessment of each individual child's competence to offer valid consent in their own right, set out in the 1985 House of Lords judgment in *Gillick v. West Norfolk and Wisbech Area Health Authority*. Nor does it mention any positive obligation to ensure that a child can exercise his right under Article 5 of the UN Convention on the Rights of the Child to receive advice from his parents in the exercise of his rights.

No consideration has been given to children's rights to privacy, or to their Article 12 UNCRC rights to have a say in decisions affecting them, as this excerpt from the 'Trustguide' report makes clear:

"In addition, 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 considered why this apathy existed. It seemed that none of the attendees 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." [16]

The whole issue of using children's biometrics urgently needs far closer examination and informed debate. We cannot find any other country in the world other than the US where this technology is being used so extensively in schools. We simply cannot afford to ignore the controversy or to be complacent about the potential dangers.

Mobile phone and GPS tracking

The market in devices to track the physical location of children has been expanding steadily over the past few years. Typically, equipment is promoted as offering parents the 'peace of mind' of knowing exactly where their children are, although in reality a device can only tell you its own location, and not whether it is in the same place as the child being tracked. It is hard to see how child location tracking serves any need that is not already met by a simple mobile phone.

Until quite recently, tracking has been carried out via children's mobile phones by calculating the relative signal strengths at three different mobile communications masts and 'triangulating' the phone's location from these. The accuracy of this system depends upon the number of masts available, and it can be very vague in rural areas. However, developments in Global Positioning System (GPS) technology now allow devices to be located to within 4 metres,[17] and within the past year GPS chips of only 2mm^2 have been created.[18] These can be incorporated into mobile phones, or into small units that can be placed in a child's school bag or pocket.

The largest manufacturer of school uniforms, Trutex, is currently exploring the possibility of producing uniforms that include GPS tracking.[19]

The signal received from the device being tracked is superimposed on to a map that parents can view on a webpage, or regular updates can be sent to their own mobile phones. Additional features allow parents to set boundaries or prescribe routes, and receive an alert if the device leaves the pre-set area.

Currently there is only a voluntary code of practice[20] for providers of mobile phone-based location devices, developed by the mobile telephone industry following consultation with the Home Office

and the Association of Chief Police Officers (ACPO). As yet there is no code of practice governing the tracking of children with GPS.

The code discourages the over-emphasis of 'stranger danger', but it remains a feature of advertising material,[21] giving a false impression of the real risks to children. Abduction by a stranger remains rare. By contrast a child is over 200 times more likely to be killed or injured when walking or cycling down the street, and yet some products are aimed at very young children, implying that it is acceptable for them to be out alone at an age when few would be able to cross a busy road safely. There is a risk that parents may be lulled into a false sense of security.

The voluntary code does not include any requirement that those with access to children's location details have background checks carried out, and an attempt to amend the Safeguarding Vulnerable Groups Act 2006 to cover mobile location services was resisted by government.[22] Also in 2006, Judy Mallaber MP introduced a Private Member's Bill to license mobile location services;[23] although this was dropped before second reading it demonstrated the growing concern about this unregulated market. More recently, Judy Mallaber secured an adjournment debate in Westminster Hall. [24]

The potential for misuse or corrupt disclosure of child location information presents a significant threat to children's safety, particularly in circumstances where it is important that a family's home address is not known, or where information is given to a person who may commit offences against a child.

The need for a statutory licensing regime is urgent, both to regulate those working in the mobile location service industry and to set down clear advertising and data security standards.

October 2007

[1] For example, see: http://www.microlib.co.uk/secondary/sec_contents.aspx?pageID=7

[2] Dr Sandra Leaton Gray, Director of Studies, Sociology of Education, Homerton College, Cambridge, 20 Feb 2007

[3] See: http://pippaking.blogspot.com/search/label/PFI

[4] Students are targets in Connexions selling war: http://www.tes.co.uk/search/story/?story_id=350641

[5] http://www.dataprotection.ie/viewprint.asp?DocID=409&m=f

[6] Parliamentary Questions 50 & 51: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhaff/uc508-i/uc50802.htm

[7] http://www.theregister.co.uk/2005/02/17/hard_drive_data/

[8] http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070723/debtext/70723-0019.htm

[9] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view.pdf

[10] http://www.crbsolutions.co.uk/pdfs/Biometric_Fingerprint_Recognition.pdf

[11] http://www.byamsys.com/right/Brochure.pdf

[12] Kim Cameron, Microsoft's chief architect of identity and access http://www.identityblog.com/?p=741

[13] See eg: Can images be regenerated form biometric templates? Adler 2003

http://www.sce.carleton.ca/faculty/adler/publications/2003/adler-2003-biometrics-conf-regenerate-templates.pdf

Hill C J (2001), Risk of Masquerade Arising from the Storage of Biometrics, B.S. Thesis, Australian National University

http://chris.fornax.net/download/thesis/thesis.pdf

From Template to Image: Reconstructing Fingerprints from Minutiae Points Ross, Shah, Jain (2007)http://biometrics.cse.msu.edu/Publications/SecureBiometrics/RossShahJain_FpImageFromMinutiae_PAMI07.pdf

[14] http://schools.becta.org.uk/upload-dir/downloads/becta_guidance_on_biometric_technologies_in_schools.doc

[15] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view.pdf

[16] *The Trust guide Report, a collaborative research project between BT Group Chief Technology Office Research and Venturing and HP Labs, part funded by the DTI Sciencewise programme.*

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

[17] *http://www.bluetreeservices.co.uk/ourKidsChildSecurityTrackerUK.php4*

[18][*http://www.electronicsweekly.com/products/2007/02/12/1593/sige+claims+smallest+gps+receiver+ic.htm*

[19] *http://www.guardian.co.uk/uk_news/story/0,,2152979,00.html?gusrc=rss&feed=technology*

[20] *Industry Code of Practice:http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf*

[21] *See eg. Childlocate home page: http://www.childlocate.co.uk/*

[22] *Hansard, 23 Oct 2006 : Column 1244*

http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm061023/debtext/61023-0006.htm

[23] *Licensing of Child Location Services Bill www.publications.parliament.uk/pa/cm200506/cmbills/144/2006144.pdf*

[24] *Child Location Services, Hansard 9 Oct 2007 : Column 53WH*

http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm071009/halltext/71009h0009.htm#07100932000521