Strathprints Institutional Repository

Bryce, T.G.K., Nellis, M., Corrigan, A., Gallagher, H., Lee, P. & Sercombe, H. (2010) Biometric Surveillance in Schools: Cause for concern or case for curriculum?, *Scottish Educational Review,* 42 (1), 3-22.

Biometric Surveillance in Schools: Cause for concern or case for curriculum?

Tom Bryce, Mike Nellis, Amanda Corrigan, Hugh Gallagher, Peter Lee and Howard Sercombe

University of Strathclyde

ABSTRACT

This article critically examines the draft consultation paper issued by the Scottish Government to local authorities on the use of biometric technologies in schools in September 2008 (see http://www.scotland.gov.uk/Publications/2008/09/08135019/0). Coming at a time when a number of schools are considering using biometric systems to register and confirm the identity of pupils in a number of settings (cashless catering systems, automated registration of pupils' arrival in school and school library automation), this guidance is undoubtedly welcome. The present focus seems to be on using fingerprints, but as the guidance acknowledges, the debate in future may encompass iris prints, voice prints and facial recognition systems, which are already in use in non-educational settings. The article notes broader developments in school surveillance in Scotland and in the rest of the UK and argues that serious attention must be given to the educational considerations which arise. Schools must prepare pupils for life in the newly emergent 'surveillance society', not by uncritically habituating them to the surveillance systems installed in their schools, but by critically engaging them in thought about the way surveillance technologies work in the wider world, the various rationales given to them, and the implications - in terms of privacy, safety and inclusion - of being a 'surveilled subject'.

INTRODUCTION

> What was then being formed was a policy of coercions that act upon the body, a calculated manipulation of its elements, its gestures, its behaviour. The human body was entering a machinery of power that explores it, breaks it down and rearranges it. A 'political anatomy', which was also a 'mechanics of power', was being born; it defined how one may have a hold over others' bodies, not only so that they may do what one wishes, but so that they may operate as one wishes, with the techniques, the speed and the efficiency that one determines. Thus discipline produces subjected and practised bodies, 'docile' bodies (Foucault 1978: 138).

The Report on The Surveillance Society, published in England by the Information Commissioner's Office (ICO) in 2006, contains a number of speculative vignettes describing how surveillance might impact on various areas of social life - transport, shopping, workplaces, criminal justice, etc., - by 2017. Schooling is alluded to, but not developed as well as the other areas. The

following vignette (a concise means of concretising certain social possibilities, written for the purposes of this article) specifically addresses schooling and extrapolates from contemporary developments in surveillance technology, particularly those incorporating biometrics (fingerprinting, iris patterns, etc…). It complements the vignettes in the Information Commissioner's report (ICO 2006) and sets the scene for the issues which are analysed in this article.

> *Keeping Track of Caitlin: Schools and Surveillance - a scenario for 2017*
> It is not inconceivable that in the near future a secondary school pupil somewhere in the UK – let's call her Caitlin, aged 16 - might register their arrival at school by passing a radio frequency identification (RFID) chipped card across a scanner at the entrance to the main building, having already been filmed by CCTV cameras coming though the school gate. An autotext is sent to her mother's mobile phone, letting her know Caitlin has arrived. Internal CCTV cameras follow her down the main corridor - images are recorded digitally for security purposes; no one is actually watching in 'real-time'. She arrives at her first class, where she hands in written work on a CD, to be scanned by plagiarism software. Later in the morning she takes two books out of the library, using a fingerprint scanner installed several years before the RFID registration system was introduced (otherwise the same card could be used in the library). Unknown to her, or to any pupil, the senior school administrator takes five minutes to do an 'online headcount' just before lunch - the position of every chipped identity card on site (and the person assumed to be carrying it) is graphically displayed on a screen in his office, colour-coded to show if any pupil is not in the classroom they are supposed to be in at that time of the day. All seems well, but the movement sensors installed in the school lavatories - so much less intrusive than webcams - indicate that two pupils have remained there for longer than might be considered necessary.
>
> At 1pm Caitlin does use her RFID card on the canteen scanner to debit her lunch account. In the afternoon she travels to a further education college, entering the premises using a fingerprint registration system because the college has not yet upgraded to an RFID system, despite being twinned with her school. She logs on to her college computer using the same fingerprint scanning system, grateful that she does not have to remember a password, as (she has been told) pupils did in the old days. Between classes she is invited to join a cluster of pupils as they walk through a police-manned 'search arch', recently installed in the college to deter knife-carrying after a 'serious incident' outside the college gates. At the end of the school day she leaves the building, de-registering her presence there using the fingerprint scanner.
>
> At home, fifteen minutes later, Caitlin's mother goes online to check her daughter's whereabouts by locating her GPS-enabled mobile phone, using the latest 'kidtracka' software. She assures herself that her daughter is on the way home, glad that she does not have to raise her daughter's anxiety by actually phoning her. She wishes that the college had an autotext system which notified her phone when Caitlin 'clocked-out', just as the school's registration system did when she 'clocked-in' in the morning. She still worried that Caitlin would lose her RFID card, and preferred the scanning system at her younger son's primary school, where the RFID chip was sensibly sewn into the lapel of his blazer, un-losable. She remembers that she has a letter from the school, inviting her to a PTA meeting to discuss the implications of their latest privacy impact assessment, but she knows she will be too busy to go. She is confident that

> there will be no problems with it, and that the minority of parents who always seem to criticise the safeguarding systems will not get their way. She is happy that in an uncertain world her children are so well looked after by their schools.

When one reflects carefully on what is already happening in Britain in respect of surveillance, as the ICO has done, this is not as implausible a scenario for a decade hence (or less) as it may at first seem, for some if not for all schools. Whilst anecdotes abound in the press, however, little systematic knowledge has been gathered about surveillance in schools in Britain (or indeed, worldwide[1]). Andrew Hope's work on CCTV in British schools makes a start (see Hope 2009), and a recent collection by Monahan & Torres (2009) significantly illuminates developments in North America. By way of creating a context for our own observations, we will nonetheless begin with the anecdotes. The examples below are drawn from a random trawl of newspapers, TV news reports and internet news sites since 2000, with all the methodological limitations that this implies. They relate more to England than Scotland. They may well be merely transient-but-newsworthy incidents, or early signs of imminent, ongoing or as yet inchoate trends: no-one knows. While they do not in themselves, even in aggregate, indicate the prevalence or depth of surveillance in British schools, they do suggest that closer attention be given to the issue than it has received to date. Our scrutiny of press coverage has of course been influenced by the ICO report itself, for it provides, if not a framework for surveillance-related issues in contemporary society, then a wide range of headings under which fall topics of prospective interest to researchers in this field. Together with matters raised in the Scottish Government Consultation Paper (discussed in detail in the section following this), we used these headings to identify where journalists were noting matters of public concern regarding surveillance.

SIGNS OF SURVEILLANCE IN BRITISH SCHOOLS

In public discourse "surveillance" remains a word with mostly sinister connotations, evoking Orwell's Big Brother and the spectre of insidious totalitarian controls, but in recent years attempts have been made by academics to define it more neutrally, so as to better understand the multiplicity of data gathering practices in contemporary global society, the range of reasons given for their use and the diversity of their consequences, hidden and overt, intended and unintended, good and bad, or both. David Lyon's widely accepted definition will be used here:

> [Surveillance] is the focussed, systematic and routine attention to personal details, for purposes of influence, management, protection or direction. Surveillance in the end directs its attention to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture). …. This attention to personal details is not random, occasional or spontaneous: it is deliberate and depends on certain

[1] International developments are beyond the scope of this paper but Nellis *et al.* (2008) refer to instances of school surveillance in the USA, Japan and Sweden. The use of electronic "tagging" technology for truancy reduction in the USA is discussed in Michel (2009).

> protocols and techniques. ….. it occurs as a "normal' part of everyday life in all societies that depend on bureaucratic administration and some kinds of information technology. Everyday surveillance is endemic to modern societies (Lyon 2007: 14).

In terms of this definition, which encompasses watching, monitoring movement and the routinised authentication of identities, all of the following are examples of surveillance used in, or in relation to, schools. They are not exclusive or exhaustive, but putative instances of the ways in which children in contemporary society are being subject to surveillance for both welfare and control reasons (Fotel & Thomsen 2004; Penna & Kirby 2009). They signify, between them, a newly emergent reality which warrants deeper and more detailed analysis.

Visual Surveillance

CCTV is in widespread use in schools in Britain, for a range of different purposes – the prevention of vandalism, the monitoring of access at the school perimeter, the maintenance of order in classrooms and corridors and as a means of protecting school staff from allegations of mistreating pupils (*Scotland on Sunday,* 12th October 2008). Tragedies like the Dunblane murders in 1996 gave easy legitimacy to some uses of CCTV, but other uses, such as their use in toilets to combat vandalism, smoking and drug-taking, have occasionally antagonized parents – although the school concerned still sought to defend the practice (*The Guardian,* September 17th 2005). In some nurseries and pre-schools, internet-linked webcams enable parents to 'look in on' their child at various points during the day. The National Day Nurseries Association is opposed to them on both privacy and security grounds, as well as fearing that staff–child interaction will be disrupted. The Professional Association of Nursery Nurses sees it as unwarranted 'workplace surveillance' rather than a means of enhancing childcare; in reality it may function as both simultaneously.

Electronic Registration

Increasing numbers of schools use electronic registration to improve efficiency, security, and child protection (automatically notifying parents by phone or text of their child's safe arrival in school) - and to reduce truancy (Lewis 2004). Some use fingerprint scanners - twice daily pupils scan themselves in as they pass various sensors, and their presence is immediately recorded on a computer (Hammersley 2004). Trutex, a long-established English school uniform maker, has expressed interest in using tracking technology, linked to a tiny signaling device embedded in school clothing (*The Guardian,* 21st August 2007), and Hungerhill High School in Doncaster began testing RFID tracking equipment with 19 pupils, using "smart threads" embroidered into uniform jumpers and scanning devices fastened to doors (to monitor entrances and exits from classrooms). Doors can be programmed to allow access for certain people at certain times, and to deny it at others (*Doncaster Today*, 18th October 2007).

Library Management and Cashless Catering

The most ostensibly innocuous surveillance systems in schools are arguably fingerprint scanning technologies for issuing books from school libraries, and/or

enabling cashless catering at lunchtimes and breaks (which will be the main focus of this article below) (*The Guardian,* 30th March 2006). Some schools have claimed that this is no different from giving children individualized passwords to access computers, although this seems not to grasp that all biometric information is more personal and intimate than a password. They are usually introduced on efficiency grounds - smartcards may so easily be lost - but parents have sometimes found them controversial and the ICO has commented on them. Cashless catering can segue into the monitoring of pupils' eating habits. At least one school extended cashless catering to promote healthy eating by recording on the same computer pupils' choices of food and awarding points and eventually prizes to those who made the healthiest choices. More recently, Todholm Primary School, Renfrewshire has developed this further, using 'a system based on the infrared light detection of vein patterns on pupils' hands', which tells catering staff if a child has any food allergies, and informs parents on what their children are eating (Renfrew Council 2009).

Crime Prevention

Some school surveillance takes place to monitor drug use – using periodic, unannounced visits by sniffer dogs - and is operated in conjunction with local police forces; in England these do tend to have the support of parents (*The Guardian,*21st April 2005). Metal detector 'search arches' of the kind used in airports (and some railway stations) have been set up in some English schools to deter knife carrying. Children are not required to empty their pockets before they pass through the search arches, which represents a limited form of privacy protection - but to avoid allegations of discrimination, all pupils rather than just 'suspect categories' of pupil, are periodically required to pass through them. *The Observer* (20th January 2008) noted 'teachers unions have welcomed them because of the dangers caused by manually frisking pupils'.

Assessment and Examination

John Gilliom (2010) provocatively suggests that the ancient, core school tasks of assessment and testing can be illuminated via the lens of surveillance theory, and new technologies do make this possible in a variety of ways. Anti-plagiarism software (which compares a pupil's submitted written work with online databases) is increasingly being used to scan essays, literally monitoring the words used. More mundanely, perhaps, the (English) Examination Officers Association may use CCTV and fingerprint scanners in some of its centres to deter and detect cheating (e.g. proxy candidates being sent, pens fitted with voice recorders), and to protect invigilators from complaints from pupils – which are apparently rising (*The Daily Telegraph,* 12th April 2008).

Catchment Control

Dorset County Council has used the Regulation of Investigatory Powers Act (RIPA) 2000 (enacted to deal with serious crimes and terrorism) to ascertain whether or not families who had applied to send their children to particular schools were in fact living in the catchment area. The council used covert physical surveillance, arguing that this protected the rights of genuinely local

parents. Alarmingly, the Home Office did not object to this (*The Guardian,* 11th April 2008).

Certain elements recur in the above news stories (which are detailed more fully in Nellis *et al.* 2008). Firstly, specific incidents of harm to pupils (including murder), coupled with the fear of further incidents, have clearly played a part in triggering or consolidating the use of visual surveillance, electronic registration and search arches. Secondly, in a number of instances it is clear that commercial organisations are actively promoting these technologies and/or working in partnership with schools, and the role of such organizations certainly warrants greater scrutiny. Writing in an American context, Monahan (2006) sees the growth of surveillance in schools as an expression, in microcosm, of a distinctly "neoliberal" approach to the creation of social order, a position also taken (but critiqued) in Cory Doctorow's (2008) California-set school surveillance novel, *Little Brother*. In Britain it is true that "efficiency" vies with "security" as the main stated rationale for their introduction but whether these are the real "causes" of the new developments, or merely discourses which legitimate them, is unclear. Empirical research into the development of surveillance practices in schools, the meanings they have to those involved with them and the consequences (intended and unintended) they have for the life of the institution would need to be undertaken before they could be theorised with confidence, given the divergent trajectories of recent surveillance theory (Lyon 2006). As the text which heads this paper reminds us, however, the shadow of Michel Foucault's prescient critique of discipline, biopower and panopticism falls still across all contemporary surveillance practices (Monahan & Torres 2010). While it is indeed not difficult to anticipate dangers posed by these technologies – our vignette deliberately plays into them – we cannot rule out the occurrence of benign or indifferent consequences, the advent of viable ethical and legal constraints or even the emergence of resistance by teachers and pupils, or both. While we believe that making surveillance in schools "a case for curriculum" will offset some of the dangers posed, by sensitising teachers and pupils alike to the issues involved, we are also, like Hope (2009: 903), mindful of the "possible moral cost" of allowing these technologies to become embedded without adequate reflection, beyond the point at which danger can be averted. The following brief analysis of a recent consultation exercise in Scotland on biometrics will shed some light on the emerging issues.

THE SCOTTISH GOVERNMENT CONSULTATION PAPER

The Scottish Government issued its consultation paper on biometrics in schools in September 2008 (see Scottish Government 2008). Drafted by the Schools Directorate, it tapped expertise from three sources: the pre-existing Principles Expert Group[2], established the same month to advise more generally on the

[2] The Principles Expert Group was established to undertake a review of identity management and privacy principles. It met between October 2008 and March 2009, and its report (Scottish Government 2009c) went out to consultation between 1st September and 23rd November 2009. The members were Jerry Fishenden, Lead Technology Adviser, Microsoft UK; Gus Hosein, Privacy International; Rosemary Jay, partner at Pinsent Mason LLP; Alan Kirkwood, chair of

protocols which should underpin identity management and privacy in Scottish public services in an era of e-government; the British Educational Communications and Technology Agency (BECTA), which advises schools on all aspects of ICT implementation); and the Information Commissioner's Office[3], which had already concluded, for example, that biometric technologies in schools were not illegal, even when introduced without parental consultation.

The very fact that guidance on biometrics was thought necessary by the Scottish Government is itself a sign of changing times. The paper recognized that some Scottish schools are already using, or contemplating the use of, biometric systems to register and verify the identity of pupils in a number of settings[4]. Cashless catering systems, automated registration of pupils' arrival in school and school library automation were the three mentioned, but potentially there are others, as the above overview indicates. The government's focus seemed to be on fingerprints and palmprints (which work as identifiers because of unique vein patterns in the hands), but as their guidelines acknowledged, the debate in future may encompass iris prints, voiceprints and facial recognition systems, which are already used in non-educational settings.

Contemporary biometrics – literally, the measurement of the body – entails the use of technologies to authenticate individual identity, by integrating unique data gathered from peoples' bodies into electronic systems and databases. This data can then be used to authorize access to places and services, at borders or in organizations – and in the case of DNA (the most publicized of biometrics), to identify, incriminate or exonerate (Zureik & Hindle 2004). As an aspect of surveillance, biometrics are increasing in prominence: 'in a world of identity politics and risk management, surveillance is turning decisively to the body as a document for identification, and as a means of prediction' (Lyon 2001: 72). Irma van der Ploeg, (1999; 2003) sees the 'informatisation of the body'- the translation of physical qualities into digital code - as something which may eventually enlarge our sense of what our bodies are for, as machine-readable objects which can place and trace us. As noted above, commercial organizations have sensed (and perhaps created) a market here, promoting the view that biometric technology is constantly improving, although as Lyon (2009) points out, evidence of biometrics' decisive value in achieving stated organizational goals is very variable. Given biometrics' expansion in the wider world, it was perhaps inevitable that schools would eventually be affected by these developments, for better or worse, as the Scottish Government's consultation now confirms.

A number of initial observations about the consultation paper might usefully be made. Whilst, as noted, research in this area remains limited, schools are

---

SocITM Scotland; Ken MacDonald, Assistant Information Commissioner for Scotland; Duncan McNiven, Registrar General for Scotland and Charles Raab, Professor Emeritus and Honorary Fellow, University of Edinburgh. (Scottish Government, News Release 31st August 2009).

[3] The Information Commissioner's Office is the UK-wide regulatory body for the Data Protection Act 1998. Its guidance on fingerprints in schools can be found at www.ico.gov.uk. BECTA's material is available at http://industry.becta.org.uk/

[4] The guidance (para 8.2) implies that the Schools (Health Promotion and Nutrition) (Scotland) Act 2007 has given schools an incentive to adopt biometrics in respect of catering arrangements.

showing an interest in biometric systems (and perhaps surveillance systems more generally) ostensibly because of concerns about *efficiency* (switching to time-saving systems which don't require pupils to carry smart cards, which may easily be lost), *security* (creating safe learning environments by restricting or denying access to unapproved/unregistered people) and *accountability* (in respect of school attendance and the prevention of harm to pupils). These concerns are widespread in contemporary society, and biometric solutions to them are only one among several surveillance technologies that have been, or are being, developed to address them. The draft guidance did not in fact use the word 'surveillance' to describe biometric technologies. This may have reflected the sense that, as noted earlier, the term 'surveillance" is so freighted with negative connotations that it may impede a fair appraisal of measures which may well be benign and constructive. Nonetheless, for three reasons, the term should be used in the context of the biometrics debate generally, and in respect of the consultation document in particular, specifically:

i) The Information Commissioner's Office, on whose views the guidance built, openly uses the term 'surveillance' and has invited open debate on what it means to live in a 'surveillance society' in which people's behaviour is monitored, for good or ill, far more extensively than in the past. This debate is both valuable in itself, and an important backcloth to any debate on the introduction of biometric technologies in schools.

ii) The draft guidance rightly emphasised the importance of consultation with parents and pupils, and it is unlikely that in any dialogue between schools and parents the broader question of surveillance would not be raised, however inchoately. By not using the 'S-word', the guidance looks as though it is avoiding the obvious, which may seem suspicious to people whose sensibilities may already have registered, however simplistically, the state's capacity to surveil them.

iii) Acknowledging the *general* term 'surveillance' highlights the fact that biometrics are only one technology among several that can (at least in principle) be used to increase safety, security and accountability in the world at large and in schools in particular - CCTV, webcams, RFID chips, searchable databases, metal detectors, plagiarism-detecting software, and so forth. It seems important to acknowledge *the broader context* into which school biometrics may be introduced, and that in the course of consultations with parents and pupils, such technologies are not discussed as if they operate in isolation.

The actual uses of biometric systems in Scottish schools - as far as they can be ascertained - have a tentative and experimental feel about them. They seem not to be extensively used - a *Sunday Herald* (October 7th 2007) survey indicated that 14 of the 32 Scottish authorities were using biometrics (although not in every school) - a Paisley primary school having been the first, in 2006. Interest in the potential of biometrics in schools is probably being shown, as it is in wider society, for the reasons given above - they seemingly offer solutions to perceived problems of efficiency, security and accountability. There are

increasing numbers of commercial organizations which market their products in these terms[5]. To some extent they are exploiting fear and anxiety about staff and pupil safety, as well as a latent desire to be modern and technocratic - but there is no doubt, at root, that these concerns are sometimes felt keenly in schools themselves, and that technical solutions are being sought (Lloyd & Ching 2003).

INTERPRETING THE DRAFT GUIDANCE

In tone, discursively, the draft guidance was in fact tilted towards *discouraging* local education authorities from adopting biometric technologies, implying that they were probably not a good thing. It questioned the proportionality of such systems – were they really necessary, were there alternatives? (para 8:1) – and suggested that biometric solutions to the problem of identifying pupils in receipt of free school meals in non-stigmatising ways 'probably cannot be justified purely as a response' to recent Scottish legislation on school nutrition. Furthermore, it said, designing opt-out systems for pupils and parents who did not wish to enrol in biometric systems (para 8.1), would be administratively cumbersome.

Recognising nonetheless that Scottish schools may well adopt biometric technology regardless, the guidance identified issues that warranted attention. In respect of security, they insisted that biometric data must be encrypted, that access to it would be limited to authorised personnel and that it would be destroyed when the pupil left the school. It is indeed essential that school-based biometrics are self-contained within a given school, not only that they are not "hackable" but also that they are not "interoperable", i.e. deliberately linked to other computerised databases which can be accessed by a range of agencies. Their legitimacy in the eyes of most stakeholders depends on their being secure in themselves, and their data unsharable. Public confidence in the security of data held by government and corporations has been dented by large scale losses of personal data (by accident, human error or crime) such that, in respect of schools, regular (annual?) reviews of technical and administrative systems should be undertaken to ensure that they have not become vulnerable to abuse.

In respect of legislation, the guidance wisely insisted that while no prevailing legislation *required* parental or pupil consent to the introduction of biometric measures, consultation with parents should always be undertaken (paras 9.1.2, and 4). Worryingly however, it said nothing about requiring consultation with teaching staff or support staff on the introduction of biometric systems, not least in respect of the workload and training implications, implying that this was

[5] The number of commercial organisations involved in making surveillance technologies for the schools market, and related markets, can only be guessed at. Most CCTV manufacturers can supply schools, but Classwatch, which (according to its brochure) "provides clear real-time, high-quality digital and audio recording with unobtrusive vandal-proof cameras and secure recorders with removable hard drive", caters specifically to them. Some identity verification companies, like Biostore Ltd, are subsidiaries of larger organisations, while others are created specifically: Darnbro was set up (by former teachers) in England to patent and pilot the RFID tracking in Doncaster schools.

perhaps a decision for senior school managers only, and that other staff's consent does not matter. Even in respect of parental consent, the issue was fudged. The guidance did not explicitly say that schools MUST seek informed consent from parents, although in allowing non-consenting pupils and parents to opt-out, it at least implied that consent must be given. Even paragraph 9.4, emphatic as it was, left ambiguous the relationship between consultation (which is required) and consent (which is not, at least legally).

The draft guidance did not give sufficient attention to relevant differences in introducing biometric systems in primary and secondary schools, and to their implications for the primary/secondary interface. Small rural primary schools may not find it particularly attractive to go down the biometric route, even for efficiency reasons. In such relatively intimate communities, face-to-face knowledge makes it fairly easy to keep track of pupil attendance, library loans and individualised catering arrangements. (At the same time, some automated surveillance systems make possible a welcome anonymity, and reduced stigma, in intimate communities where perhaps too much is potentially, and unavoidably, known about individual members). In addition, liaisons between primary and secondary schools vary in their complexity, ranging from a small number of primaries being associated with a local secondary, to very large numbers of primaries having, in practice, no linkages (other than the transmission of some paperwork) with a distant popular secondary. It will need to be assumed that databases generated by biometric identification and allocation systems should be treated as separate and discreet entities, and play no part in the primary/secondary transition. To a degree, this runs counter to the prevailing (and still deepening) ethos of interoperability/data sharing in the interests of children's welfare, as in England's ContactPoint[6] system: schools will have to reconcile these dissonant mentalities.

Quite apart from the question of where, and with whom, back-up biometric data might be stored, the sharing of such data in some contexts may in fact be unavoidable. Partnerships between secondary schools and further education colleges (increasing as more Skills for Work courses come on-stream – see HMIe 2009) raise the problem of institutional identity and affiliation: pupils may pursue their education in a complex network of linked but spatially separate institutions, rather than a single school campus. In practice, it would seem that each component of the partnership would need common systems for appraising biometric identifiers. This would probably make the management and safeguarding tasks referred to above more complex still.

[6] ContactPoint - launched in England in 2009 at a cost of £224m, as a response to several child protection scandals - is a nationwide database accessible by authorised public sector personnel to add and gather information which, it is officially claimed, will help them to support and safeguard children. It has been criticised by privacy advocates for its surveillance dimensions, and by Overtis Systems, a computer security firm, for its vulnerability to viruses and spyware (*Daily Telegraph* 3rd August 2009).

SCHOOLS AND THE SURVEILLANCE SOCIETY

The ICO's (2006) *Report on The Surveillance Society* (launched in Scotland in 2007) is somewhat weaker in its analysis of how surveillance might impact in schools in 2017 than in any other area of social life, whether the workplace, the shopping mall, transport systems, or criminal justice institutions. It also says nothing about the place or function of schools in surveillance society. Whatever the merit of speculative extrapolations (as in the vignette at the start of this article), the ICO is nonetheless clear that the surveillance society is here now; it is not something that yet awaits us, although surveillance in the future may well extend, mutate and intensify to meet shifting perceptions of, or demands for, convenience, security and accountability. Schools arguably have a responsibility to prepare and educate pupils about life in the surveillance society. There seem to be two emerging views as to how schools might do this, which are in some tension with each other:

i) As schools themselves become more surveilled environments, some privacy activists fear that they will habituate pupils into accepting the forms of surveillance they will encounter in workplaces and public space as adults, indeed which they already encounter as young people outside school. Schools, in this view, will prepare pupils for the surveillance society, but in an uncritical way, simply by normalising surveillance within its own structures and administrative processes. One solution - which the draft guidance seemingly tilted towards - is to stop schools becoming surveilled environments, presumably as part of a more general attempt to roll-back the presence of surveillance technologies in other areas of life. This "traditionally liberal" position may, given the pervasiveness of broader surveillance developments, be Canute-like.

ii) Schools should prepare pupils for the surveillance society by critically engaging pupils with its realities and prospects. This seems to be the implied position of the ICO and several academic commentators on surveillance. It is premised on a belief that, through informed understanding, the worst excesses of the over-surveilled society may yet be avoided; but also on a recognition that we are already immersed in a web of surveillance, that we find it useful or innocuous, that it will not easily be rolled-back and that what liberty, autonomy and privacy mean in this new world must be worked out anew. Some pupils will doubtless work this out by resistance (Doctorow 2008; Weiss 2010; Hope 2010), but this cannot be left to chance. Schools themselves must turn surveillance-in-schools into a pedagogical issue, not just a technical, administrative or management issue, as part of a wider curricular strategy for educating pupils about the changed environment in which they are growing up.

The prospective introduction of biometric surveillance technologies - or indeed any surveillance technologies - into a school does need to be effectively addressed as an administrative task (the focus of the draft guidance), and as an aspect of "workplace surveillance", which affects teachers themselves, but it also provides a pretext for more explicitly educational discussions with pupils (secondary pupils, at least), and indeed with parents. The draft guidance did not

cover “workplace” or “educational” concerns, and while it may not have been thought appropriate to raise pedagogical issues, it could usefully have outlined the intellectual/educational issues that warrant exploration in consultation, above and beyond the merely technical and administrative issues. It is possible that unless teachers themselves take the “surveilled workplace” issue seriously, the subject will not be prioritised with pupils; equally, it may enter the curricula of some schools regardless of whether teachers (and their unions) address it systematically.

Consultation with parents should always entail more than a letter to the home. Inadequate literacy among some parents, and the technical nature of biometrics, makes full understanding unlikely from merely written notification. Only in a face-to-face dialogue with teachers and the anticipated administrators of the new system, where parents can test the technology, is the level of understanding necessary for truly informed consent - a consciously articulated “yes” - likely to be generated.

Consultation with pupils, especially primary school pupils, will require careful thought. In eliciting responses from young people, it will probably be difficult with this topic for schools to distinguish between naiveté (which is likely to mean that pupils will regard biometric technologies as ‘cool’ and futuristic, and be uncritically enthusiastic about them), and immaturity (which means they do not have the life experience to make good judgements of the pros and cons). Perhaps the only way to alleviate this is to address surveillance in the curriculum.

It would not be difficult to address biometrics and, more sensibly, the surveillance society in general within the secondary school curriculum. Alert, enterprising teachers may already be doing this – this is something else we do not know. The very nature of the topic certainly makes it amenable to curricular inserts and cross-curricular approaches. Both would afford study in the sciences and technology, in social subjects/modern studies, in literature and media studies, and in social education. This, above and beyond consultation with pupils about the introduction of specific biometric systems within their particular school, would help prepare them - critically, one hopes - for life in the surveillance society. In the Scottish context, the incoming (2010) Curriculum for Excellence guidelines in the area of Technologies would permit the inclusion of material on biometrics (Pupils should ‘develop an understanding of the role and impact of technologies in changing and influencing societies’;...; they should ‘become an informed consumer and producer who has an appreciation of the merits and impacts of products and services…’ (see LTS 2009).

PRIVACY, PROPORTIONALITY AND INTRUSIVENESS

Biometrics raise important new questions about privacy and bodily integrity, some common to all surveillance technologies, some distinct. In settings where different sorts of technology can operate simultaneously, interact with each other and perhaps generate aggregated data, it is arguably limiting to discuss biometric technologies in isolation, particularly in respect of privacy impact

assessments[7]. Any such assessment that failed to explore *all forms* of surveillance technology operating, or anticipated, in a given school would be incomplete, and would say little, in human or institutional terms, about the privacy issues that were actually at stake. Pupils, after all, experience school as a total environment, not in separate administrative segments, and it is surely preferable to heighten their consciousness of being 'data subjects'[8] in the round, not just in relation to particular technical systems.

Concerns about proportionality and intrusiveness were rightly central to the draft guidelines, and were seemingly part of what tilted the government against biometrics, but they need to be explored in relation to changing sensibilities. What people experience as proportional and intrusive can alter within and across generations, and while that does not obviate a need for setting standards, attention to people's - including children's - actual subjectivity in respect of surveillance matters if we are to treat them fairly, and if we are to recognize the benefits which benign technologies might offer. Objectively, it might well be argued that biometrics are simply not a proportionate response to mere problems of efficiency in a school when other solutions are available. Whether they are *felt* by users to be disproportionate is, however, another matter; they may, for better or worse, be sensed as nothing more than innocuous 'functional equivalents of other forms of informal controls that [previously] operated' (Feeley 2003: 118). Following Aas (2004) and Parton (2008), a more critical analysis may well suggest that biometrics in general exemplify a broader, potentially dehumanizing, shift from "social" to "informational" ways of authoritative knowing, from reliance on rich "narrative accounts" about people to shallow "database profiles" - but subject populations' own vocabularies for understanding this transition still need to be grasped, all the more so if they have little inkling of its significance for their lives.

To many contemporary adults, biometrics - especially fingerprinting - has indelible associations with policing and criminal justice, and, nowadays, border control. They have 'connotations' of suspicion, incrimination and exclusion which one would not sensibly wish to see carried over into school settings, where their very presence may well engender feelings, not of reassurance, but of insecurity and paranoia. To younger people – whose engagement with social networking sites such as Facebook suggests a more attenuated commitment to informational privacy than their parents had (Boyd 2008) – they may not seem quite so stigmatizing. In any case, as van der Ploeg (2003: 60) argues, the

[7] Privacy Impact Assessments (PIAs), often seen by organisations as a means of "risk management", but just as important for civil liberties, are becoming the tool of choice to assess surveilled environments. An online handbook describing how to construct and conduct them is available from the ICO, and they are now strongly encouraged by the Scottish Government (2009b). For a broad and accessible discussion of contemporary privacy issues, see O'Hara & Shadbolt (2008).

[8] Examining what it means to be a "surveilled subject" entails understanding both an individual's subjective experience of surveillance, and also the way which *profiles* about him/her (variously called "data doubles" or "digital selves") can be built up on databases, retained for years despite inaccuracies, and used to affect decisions about them – minor or major - perhaps without their knowing (see Lyon 2001; 2007; 2009).

'exclusive association [of fingerprinting] with criminality is rapidly becoming obsolete', and biometric identity verification is now being used to confirm status and privilege 'for the respectable client, the cardholder or club member'- fast-tracking them through airports, for example, or facilitating entry to, and mobility around, Disneyworld, Florida. If, as a result of their normalization in the wider world, biometrics come to be seen in more mundane and/or more positive terms, the question of their proportionality and intrusiveness in school settings may well be revised.

Echoing van der Ploeg (2003), the Scottish Government (2008: para 4.2) stated openly that "biometric systems can be perceived as more intrusive than other systems". True enough: they use parts of the body as personal identifiers, in a way that other access and registration systems do not. The 'bodyparts' in question, however, are minute and complex patterns on skin and in vein systems of which their 'owners' themselves may barely be aware, and which are (probably) not integral to people's subjective identities or sense of uniqueness. Using technology to make these patterns 'visible' and 'machine-readable' at selected service-access points is arguably less threatening to privacy and dignity than, say, scanning systems which reveal the naked body (now used in some airports), or manual searches which require "frisking". Not all surveillance systems "intrude" in the same way, or to the same degree; biometric systems are not "panoptic" in any literal sense, but in the way that they can sort and code individuals at access points, they can isolate and exclude in a way that systems which "merely watch" cannot. Cashless catering systems can be adapted to identify pupils in receipt of free school meals without the potential embarrassment entailed by showing a special card or saying aloud that they are such recipients. In that sense an automated biometric scanning system may be experienced as less stigmatising than the gaze of another human being. In the longer term, however, the routine use of our body as a "password" (Lyon 2009: 113) may well add subtle new dimensions to our experience of embodiment and sense of self, particularly if digitized body data is used to enforce the spatial exclusion or denial of significant services to vulnerable people, in ways unimaginable to present generations.

For now, the question of whether pupils experience biometrics in school as intrusive is partly a question (for better or worse) of what they might over time get used to, of the meanings they bring to the experience of being scanned and the perceived losses and gains entailed - as against the alternatives. Some pupils, particularly those of secondary age, are used to electronic gadgets in their lives, and may perceive certain aspects of surveillance as 'cool' (much media representation treats it thus) - but little is known about their actual responses to these emerging new realities. Above all, at the present time, both pupils' and parents' perspectives on biometrics is – as Hope (2009) suggests in relation to school CCTV systems – a question for research because, without it, it is difficult to know which theoretical tack to take, what level of anxiety to muster. It is difficult, for example, to envisage how meaningful privacy impact assessments could be undertaken in this area without research-based data on the kinds of privacy people care about, and the trade-offs that, rightly or

wrongly, they may be willing to make for the sake of security, or just to have more electronically "connected" lives (O'Hara & Shadbolt 2008).

THE RESPONSE TO THE CONSULTATION

The Scottish Government received 23 responses to the draft guidelines, publishing them on their website on 7th January 2009. There were 13 from local councils; 2 from teacher associations; 1 from a parent-teacher association; 1 from a primary school, and 1 from NO2ID (a pressure group opposed to the expansion of surveillance). In addition, there were responses from Biostore Ltd (which manufactures biometric technology), the ICO; and Clydebank Women's Aid, as well as our own response from the University of Strathclyde. One individual citizen made a private submission. What follows is not a comprehensive review of the responses – which can be found at Scottish Government 2009a – but a selection of key points that support or extend the same debate that we ourselves wish to stimulate. The Scottish Government (2009b) in fact issued its own analysis of the responses in February 2009; our emphases are somewhat different from theirs.

The responses from the councils were wide-ranging in content and format, the majority simply commenting on the perceived clarity or otherwise of the draft guidelines. Glasgow and Inverclyde seemed to take pride in saying that they did not use biometric technologies and had no plans to do so, whilst commending the clarity of the guidance in the event of ever needing them. Overall, the guidance was seen as flagging up the right issues and as being fair-minded, but several agreed that the omission of advice on how to handle the media (who were perceived as unduly interested in surveillance in schools) needed to be rectified. Concerns about data security were legion, and some councils recognized the roles that schools might inadvertently play in acclimatizing young people to the surveillance society. Those using biometric systems, e.g. Renfrewshire, did not report difficulties with families who opted out. Several councils reported using other registration and authentication systems that did not rely on biometrics, Highland Council, for example, linking theirs to the roll out of the National Entitlement Card[9]. Edinburgh City Council questioned the wisdom (and cost) of biometric systems *not* being interoperable, and linked to existing "school management information systems", while the board of Wester Cleddens Primary School stated that it was "vehemently opposed" to the introduction of any "Orwellian" biometric technology in school.

The Educational Institute of Scotland took a sombre view of the prospect, doubting their necessity as a means of making schools safer or more efficient,

[9] The National Entitlement Card (NEC) is an electronic smartcard available for 11-26 year olds in Scotland, which enables them to give proof of age and to access a range of services, including travel and library/leisure membership, sometimes at a discount. The intended linking of the NEC to school-based identity verification systems shows clearly how debates on biometrics in schools mirror broader debates on identity authentication in wider society, in particular ID cards (see Lyon 2009). In 2006 the then Scottish Executive considered incorporating Scottish Candidate Numbers, which had hitherto been given only to secondary school pupils in the third year and above, as part of electronic registration systems in schools (*Glasgow Evening Times* 23rd February 2006).

and fearing that if the technologies were applied to the pupils they would sooner or later be applied to the workforce as well, "to record timekeeping, attendance and other behaviours". It opposed this. The Scottish Secondary Teachers' Association anticipated simple practical problems: "There would be a potentially serious problem with overcrowding if every pupil in a large secondary school had to record their palm or fingerprint at one of a small number of machines every day" – delay at the scanners would give some pupils the perfect excuse for late attendance. Perth and Kinross Council echoed this point, noting also that scanning protocols "in emergency situations such as building evacuations [are] not addressed". The Scottish Parent Teacher Council accepted that biometric systems could be made secure, insisting that "it is important not to overstate the dangers of using biometric systems".

Clydebank Women's Aid worried about the "containment of information" on the databases associated with electronic/biometric registration systems, suggesting furthermore that inclusion on them sometimes accentuated domestic violence victims' pervasive sense of vulnerability, of being at the mercy of a "totality of power". Responding simply as an individual, Jackie Marshall, a mother, opposed the introduction of biometric surveillance technologies into schools because of the climate of mistrust and suspicion she felt they created, plus the difficulties that would exist (in terms of stigma and inconvenience) for any child or parent who opted out of such schemes. She then made a novel point:

> I have a thirteen year old daughter who is learning to handle money and the last thing I wish to do as a parent is to engender a culture of mistrust on how she chose to spend her lunch money. The State should not be trying to undermine parental responsibility and I believe this policy, should it be successful, will do just that. ….. What are we saying to our young people when we are scanning their palms, fingerprints and not trusting them to handle money?

Many of the responses, NO2ID's most emphatically, questioned the easy reassurance in the draft guidance that school-based biometric technologies were not interoperable and wanted more safeguards. As if in anticipation of this reaction, Biostore Ltd's response emphasized the security, reliability and versatility of the various technologies that were already being used in schools, and those which might be used in the future. The company has been in existence for 2 years - it was a subsidiary of Softlink Europe Ltd – to provide "authentication software" for the schools market. Its emergence was premised on "a rapid and understandable trend towards integration of identification across a range of applications, allowing vital information to be available instantly across a number of databases, without the need for rekeying of data, or 'manual' transfer of files". It acknowledged that "in this fast moving sector, technology is advancing quickly, and for the next few years is likely to be implemented well in advance of up-to-date guidelines being laid down by any governing authority". It claimed to have "product…. in use in over 600 schools throughout the UK", indicating its openness to using biometrics alongside other forms of identify authentication – smartcards, barcodes, PINs and passwords - in a range of

applications, library management, cashless catering, access control, print and copy management, computer log-on [and] lesson registration."

CONCLUSIONS

Surveillance practices, in a variety of forms and for a range of reasons, are becoming a more commonplace feature of schools in Scotland and elsewhere. The precise reasons why this is occurring are improperly understood, and warrant research, both national and comparative, in order to theorise their full social and political complexity. The Scottish Government's publication of guidance on the introduction of biometric technologies in Scottish schools, and the subsequent consultation, created a useful opportunity to examine one small aspect of these developments, but more comprehensive investigations are needed, which look at the combined impact of multiple surveillance technologies in schools, and theorise them in the context of the emerging "surveillance society".

In September 2008, the Scottish Government's draft guidance seemingly recognised the pressures on schools - centred on improving the security and safety of children and staff and the need for ever more efficient administrative systems - to see surveillance technologies as credible means of addressing real and anticipated difficulties. In a risk-averse, cost-conscious culture, schools may well be accused of not doing enough to improve safety and efficiency if available technologies are not adopted - although in the coming age of public sector austerity even the start-up costs of biometric systems may be prohibitive. Final guidance will not be issued until after the completion of the Scottish Government's (2009c) consultation on identity management in the public sector more generally (in November 2009)[10], and it remains to be seen if the Government's position on biometrics remains as it was in the original draft guidance. The new consultation document makes only brief mention of biometrics, but is very strong on consultation with affected parties, and indeed, public and professional education about the underlying technical and ethical issues.

The draft guidance arguably underplayed the potentially positive aspects of biometrics as enhancers of convenience (ease of access at checkpoints) and justice (eliminating the stigma of welfare recipients). The public association of biometrics with policing and border controls may well crumble as more innocuous uses of them develop in the wider world; the lingering suspicion that they are inherently disproportionate and intrusive for use in schools may (for better or worse) dissipate. The guidance unhelpfully fudged issues of

[10] At the time of the final revisions to this paper (February 2010) the Scottish Government was planning to issue final guidance on biometrics in schools – informed by the consultation on identity management and privacy - in March 2010. (Personal communication, Laura Miekle, Scottish Government, 1st February 2010.)

consultation and consent in respect of parents, pupils and teachers, in ways that would curtail rather than encourage necessary dialogue. It was somewhat complacent in respect of data security. Alongside privacy impact statements, regular technology reviews are essential, to demonstrate and signal to others that systems remain secure over time - or not – and to ensure their continued legitimacy in the eyes of various stakeholders.

The crucial issue – overlooked in the initial guidance – is that schools must prepare pupils for life in the newly emergent 'surveillance society', not by uncritically habituating them to surveillance systems used in schools, but by critically engaging them in thought about the way surveillance technologies work in the wider world, the various rationales given to them, and the implications - in terms of privacy, accountability, safety and inclusion - of being a 'surveilled subject'. The introduction of biometric identification systems - or any surveillance system - in schools creates a pretext for this, but a far wider range of issues could - and should - be addressed in the curriculum. The subtitle to this article was in the form of a question – Is biometric surveillance in schools a 'cause for concern or case for curriculum?' Our answer is most certainly: 'Both'. And, it is interesting that Biostore Ltd, in its submission to the consultation, came close to endorsing this view:

> It is vital that questions about the management of identity take on a high profile within education, as data loss and identify theft becomes more significant in this age of vast databases and an excess of stored information. Students need to be very aware of how their data can be compromised. Issues to be discussed must range from revealing personal data on social networking sites, to protecting how biometrics are recorded and used.

This is a welcome admission, attuned to contemporary realities, but – despite our agnosticism about the precise theoretical tack to take in this paper – it arguably does not go far enough. The near future of surveillance in British schools may not resemble those of their US counterparts (Monahan & Torres 2010) or be as grim as novelist Cory Doctorow (2008) envisages in *Little Brother*. The results of future research, and the depiction and dissemination of dystopian futures now (like the vignette with which we began) may well work to make such futures less likely. Nonetheless, the very existence of Biostore Ltd, and organisations like it, signal the quiet and unexamined emergence of a market in school surveillance technology, and while this alone does not warrant a necessarily sinister interpretation of all surveillance-in-school developments it undoubtedly justifies the close analytical attention to the issues which we have provided in this paper.

REFERENCES

Aas, K.F. (2004) From Narrative to Database: technological change and penal culture, *Punishment and Society,* 6 (4), 379-93.

Boyd, D. (2008) Facebook's Privacy Trainwreck: exposure, invasion and social convergence, *Convergence,* 14 (1), 13-20.

Doctorow, C. (2008) *Little Brother,* London: Harper/Voyager.

Feeley, M. (2003) Crime, social order and the rise of neo-Conservative politics, *Theoretical Criminology,* 7 (1), 111-130.

Fotel, T. & Thomsen, T. U. (2004) The Surveillance of Children's Mobility, *Surveillance and Society,* 1 (4), 535- 554.
Foucault, M. (1978) *Discipline and Punish: The birth of the prison,* London: Penguin Books.
Gilliom, J. (2010) Lying, Cheating and Teaching to the Test: the politics of surveillance under no child left behind. In T. Monahan & R. D. Torres (Eds.) *Schools under Surveillance: Cultures of control in public education,* London: Rutgers University Press.
Hammersley, B. (2004) Thumbs do the Talking, *The Guardian,* 25th November 2004.
HMIe (2009) Working Out: A report on work-related learning for Scottish secondary school pupils, Edinburgh: HMIe. Available at http://www.hmie.gov.uk/Publications.aspx
Hope, A. (2009) CCTV, school surveillance and social control, *British Educational Research Journal,* 35 (6), 891-907.
Hope, A. (2010) Seductions of Risk, Social Control and Resistance to School Surveillance. In T. Monahan and R.D. Torres (Eds.) *Schools under Surveillance: Cultures of control in public education,* London: Rutgers University Press.
ICO (2006) A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network. Full report. September 2006. Online at www.ico.gov.uk/
Lewis, I. (2004) Technology Tackling Truancy: e-registration a success, Government IT February 2004, 70-71.
Lloyd, R. & Ching, C. (2003) School Security Concerns, *Research Report RR419*, Nottingham: Department for Education and Skills.
LTS (2009) Curriculum for Excellence guidelines on Technologies. Online at http://www.ltscotland.org.uk/Images/technologies_experiences_outcomes_tcm4-539894.pdf
Lyon, D. (2001) *Surveillance Society: monitoring everyday life,* London: Routledge.
Lyon, D. (Ed.) (2006) *Theorising Surveillance: the panopticon and beyond,* Cullompton: Willan.
Lyon, D. (2007) *Surveillance Studies: an overview,* Cambridge: Polity Press.
Lyon, D. (2009) *Identifying Citizens: ID cards as surveillance,* Cambridge: Polity Press.
Michel, P. A. (2009) Truancy Reduction: an emerging application for electronic monitoring, *The Journal of Offender Monitoring*, 21(2), 16-19.
Monahan, T. (2006) The Surveillance Curriculum: risk management and social control in the neoliberal school. In Monahan, T. (Ed) *Surveillance and Security: technological politics and power in everyday life,* London: Routledge.
Monahan, T. & Torres, R.D. (2010) (Eds.) *Schools under surveillance: Cultures of control in public education,* New Brunswick, NJ: Rutgers University Press.
Nellis, M., Bryce, T.G.K., Corrigan, A., Gallagher, H. *et al..* (2008) Biometric Technologies in Schools: Draft Guidance for Education Authorities. A response to the consultation from the Surveillance and Education Group, Faculty of Education, University of Strathclyde.
O'Hara, K. & Shadbolt, N. (2008) *The Spy in the Coffee Machine: the end of privacy as we know it,* Oxford: Oneworld.
Parton, N. (2008) Changes in the Form of Knowledge in Social Work: from the "social" to the "informational", *British Journal of Social Work,* 38, 253-269.
Penna, S. & Kirby, S. (2009) Children and the "New Biopolitics of Control": identification, identity and social order, *Youth Justice,* 9(2), 143-156.
Renfrew Council (2009) Todholm Primary School. Cashless catering system. Online at http://www.renfrewshire.gov.uk/ilwwcm/publishing.nsf/Content/ce-gm-todholm
Scottish Government (2008) Biometric Technologies in Schools. Draft Guidance for Education Authorities. 9.9.2008. Online at http://www.scotland.gov.uk/Publications/2008/09/08135019/0
Scottish Government (2009a) Biometric Technologies in Schools. Draft Guidance for Education Authorities - Consultation Responses. 7.1.2009. Online at http://www.scotland.gov.uk/Publications/2008/12/30090717/0
Scottish Government (2009b) Biometric Technologies in Schools. Draft Guidance for Education Authorities: Consultation Analysis Report. Edinburgh: Scottish Government.
Scottish Government (2009c) Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles. Edinburgh: Public Service Reform Directorate, Scottish Government.
van der Ploeg, I. (1999) Written on the Body: biometrics and identity. In C. Norris and D. Wilson (Eds.) (2006) *Surveillance, Crime and Social Control,* Aldershot: Ashgate.

van der Ploeg, I. (2003) Biometrics and the Body as Information: normative issues of the sociotechnical coding of the body. In Lyon, D. (Ed.) *Surveillance as Social Sorting: privacy, risk and digital discrimination,* London: Routledge.
Weiss, J. (2010) Scan This: examining student resistance to school surveillance. In T. Monahan and R.D. Torres (Eds.) *Schools under Surveillance: Cultures of control in public education,* London: Rutgers University Press.
Zureik, E. & Hindle, K. (2004) Governance, Security and Technology: the case of biometrics. In Norris, C. & Wilson, D. (Eds.) (2006) *Surveillance, Crime and Social Control,* Aldershot: Ashgate.