Overlooking children: an experiment with consequences

Terri Dowty

Abstract Since 2001 there has been a proliferation of commercially-available devices that observe children, track their movements and gather data about the routine choices that they make. At the same time, a growing number of databases in education, social care, health and youth justice store detailed information about children and facilitate its sharing between agencies. Some of this data is derived from in-depth personal assessment tools that are believed to 'predict' poor life outcomes such as criminality or social exclusion. These developments are often presented as a means of keeping children safe or of intervening to deal with problems promptly, but they leave children with little privacy and create a new set of ethical and practical difficulties. There are dangers that overloading an already stretched social care service with low-level concerns will damage effective child protection work, while any insecurity in the systems potentially puts all children at increased risk of harm. Issues around consent to data-sharing have not been adequately addressed, but the reduction in confidentiality brought about by routine inter-agency information-sharing may deter children and their families from accessing services at all. We risk habituating children to a very high level of surveillance, and yet the possible effect of such widespread data-gathering on their personal development and future lives has not been considered. This paper lists some of the systems now in use or being planned, and outlines the potential risks that they pose to children's safety and development.

Keywords Children · Privacy · Information technology

T. Dowty (✉)
Action on Rights for Children, c/o 62 Wallwood Road, London E11 1AZ, UK
e-mail: terri@arch-ed.org

Introduction

Children unquestionably have a right to a private life. This is guaranteed by Article 8 of the European Convention on Human Rights and underlined by Article 16 of the UN Convention on the Rights of the Child, ratified by the UK in 1991. Although other rights to life, health and development may sometimes weigh more heavily in the balance, privacy is still as fundamental to children as it is to adults. The right to privacy encapsulates the knowledge of its importance for individual identity and mental health.

Developments in the use of Information Technology threaten to destroy children's privacy. When technology is combined with an adult-centric view of children as human beings in-the-making rather than subjects of rights in the present, it threatens to create a society in which children no longer have private lives at all. We risk habituating children to a very high level of surveillance, but the ethical issues that this raises, the new difficulties it creates and the potential effects of monitoring, data-gathering and information sharing on children's personal development and future lives have not been considered. A zero-privacy approach to child-rearing is likely to have unintended consequences that will exacerbate the very problems that gadgetry and databases are apparently designed to solve.

More than a decade ago, the cultural historian Marina Warner observed in the Reith Lectures:

> Childhood placed at a tangent to adulthood, perceived as special and magical, precious and dangerous at once, has turned into some volatile stuff—hydrogen, or mercury, which has to be contained. The separate condition of the child has never been so bounded by thinking, so established in law as it is today. (Warner 1994: 30)

It is this otherness of children that allows adults to objectify them. Their perceived 'preciousness and dangerousness' create an atmosphere in which we believe that children must be watched closely in order to curb the monsters that may prey upon them, or those that lie in wait within children themselves, and that sacrificing children's privacy rights is a fair price to pay.

We fear that children will be abducted, harmed, corrupted or bullied. That they will get fat, play truant, watch too much television and never so much as look at a book. We worry that they will fail to get jobs and will grow up to be criminals. In fact, given children's capacity to live up to adults' expectations, it's surprising that so many survive our doomsday prognoses for them.

These popular anxieties provide a fruitful sales pitch for anything that adults believe will help in their quest to steer children past the lurking dangers. Whether it be a parenting manual, monitoring and surveillance gadget, or a system that collates information and promises to nip problems in the bud, a product or initiative needs only the tag of child protection, education or the prevention of delinquency in order to find a receptive market.

Consequently, developments in a wide range of arenas are having a cumulative effect on children's privacy and their interactions with adults. In this article, I shall outline the innovations taking place in the use of technology to watch and regulate children, beginning with its use by parents to monitor their own children, by teachers

to control their behaviour at school, and by the State to watch their development and screen for early signs of trouble.

CCTV and Webcams

Recently, a head teacher in Manchester justified his decision to install CCTV cameras throughout his school (including in the toilets) as follows:

> They've definitely proved their worth because pupils know they're being watched 24 hours a day. There are cameras on the corridors, in all the communal spaces and outside on the playground. (Manchester Evening News 2007)

There seems to be no room here for doubt that children need intensive surveillance and, while the 24-h claim may be an obvious exaggeration, it is nonetheless true that if the full range of available devices were used on any particular child, she could be under constant physical surveillance.

It is not only schools in which CCTV cameras are proliferating. There is a growing trend towards the use of webcams in pre-school settings. Parents, and others nominated by them, are able to log on to a dedicated website at any time in order to watch their toddler at play. Since the camera covers the entire room, all observers see every child and adult present. While advertising material focuses on webcams as a way of fostering parental involvement in their children's lives, a Danish study of the use of nursery webcams concludes that they are a useful means of bridging the gap between 'traditional society' and 'radicalised modernity' and could help parents who experience: 'difficulties accepting the decreasing importance of the family in the socialization of the child.' (Jørgensen 2004)

Webcams are thus seen as important for parents, and in promoting a political agenda, but children are, paradoxically, invisible. No attention is paid to the potential problems of allowing large numbers of people to observe the daily lives of children too young to offer consent. Quite apart from any child protection implications, there is no apparent recognition that webcams undermine the dignity of a baby or toddler. Moreover, the assertion that they permit 'parental involvement' is simply misleading: one-sided observation cannot constitute a reciprocal relationship; it merely reinforces the idea of a child as a passive object of adult scrutiny. One can only imagine the confusion a small child might feel were his parents to comment on the events of his day when they had not actually been present.

Mobile location

There is another growing market in mobile phones with which parents can track the whereabouts of their children. Some include a feature that allows parents to set a physical boundary or key in a regular route, and receive an alert if the child deviates from this. Typically, the advertising appeals to parental perceptions of 'stranger danger' and suggests that the product can bring parents 'peace of mind', but this is illusory: all that parents can know is the whereabouts of their child's phone but not

whether it is still in the child's possession. Any false sense of security may increase the risk that a child who is, in reality, not yet competent to be out alone will meet the more likely danger of a traffic accident.

It is hard to see how a child's independence is fostered by powerful messages that the outside world is a predatory place so full of dangers that they cannot possibly cope alone. Whilst it is understandable that parents would prefer to avoid the inevitable anxiety of their child's first essays in independence, it is that very anxiety that ensures they weigh up the risks and equip their children to handle the unexpected. The ultimate goal of parenthood is, after all, to bring a child to competent, confident maturity.

Biometrics

During the last five years, increasing numbers of schools have installed library, canteen and registration systems that monitor and analyse children's habits, such as their choice of reading matter (including by age, ethnicity and gender) or their individual school meal choices.

Typically these systems scan children's fingerprints in order to increase efficiency and eliminate such problems as lost library cards. They are also promoted as a means of addressing a catalogue of current anxieties: advertising straplines include such assertions as: 'A cashless system is an effective anti-bullying tool'; 'The scheme promotes healthy eating'; 'Pupils are happy to borrow and return books'.

After undertaking a literature review of the use of children's biometrics, Dr Sandra Leaton-Gray of Homerton College, Cambridge contacted the campaign group, 'Leave Them Kids Alone' to inform them that:

> 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. (Leaton-Gray 2007)

There is currently no requirement for schools to seek parental consent before taking a child's fingerprints, and the Information Commissioner has said that the practice does not raise data protection problems. Manufacturers have attempted to calm the mounting anxiety amongst parents by asserting that the data derived from a fingerprint cannot be reverse-engineered, and that the systems are protected by 128-bit encryption.

Even were such statements to be reassuring, they do nothing to counter concerns that children are becoming habituated to giving up their irreplaceable biometrics for low-level purposes; that schools are not secure environments; that data is not fully cleansed from systems when a child leaves the school and that security cannot be guaranteed in the years to come. On the issue of the potential use of biometrics by other agencies or individuals, Microsoft's Chief Identity Architect, Kim Cameron, points out:

> 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. (Cameron 2007)

Perhaps the final comment on this subject should go to the head teacher of a school in York, who justified the invasiveness of taking children's fingerprints as preparation for life:

> All the measures to do with ID cards will possibly invade their privacy even further, but the world has no answer to terrorism without using these things and I would see us as getting them ready for the world in which they will have to live. (York Press 2007)

Databases and assessment systems: The School Census and National Pupil Database (NPD)

The termly School Census provides a classic example of function-creep. While the Education Act 1996 empowered the government to collect information about pupils directly from schools, this specifically could not include the name of any pupil. Since then, a series of amendments and regulations has changed that situation to enable a regular 'pupil level' (individual) census of every pupil in a state-maintained school. The range of information collected has also increased incrementally to more than 40 individual-level data items, including attendance and behaviour data.

Because the legislation requires schools to supply the data, a statutory gateway that provides an exception to certain requirements of the Data Protection Act, parents and children are not asked for consent. Data is taken directly from schools' management systems, and also from pre-school providers, including childminders, via the local authority.

Once collected, the information is held on the National Pupil Database (NPD). Initially the government maintained that:

> The Department has no interest in the identity of individual pupils as such, and will be using the database solely for statistical purposes, with only technical staff directly engaged in the data collation process having access to pupil names. (Timms, January 2002)

In this same written answer the Government also confirmed that data held on the NPD would not be deleted. Since then, the NPD has been used for a variety of purposes (DfES 2005) including the identification of individual 'gifted and talented' pupils. (Dracup 2006) It will also be used to populate the national 'Contactpoint' database, which is described below.

'Connexions'

The Learning and Skills Act 2000 provided for information about all teenagers to be collected and shared without consent across a wide range of health, education, social care and youth justice agencies in order to identify young people in the target age group, and to spot those 'disengaged' from education.

The Act was passed in order to set up the Connexions service, the aim of which was to encourage participation in education, identify personal problems that might create a 'barrier to learning' and offer:

> a much better support service, founded around personal advisers, to guide young people through their teenage years and help them get around the problems that might stop them from making the most of learning. (Social Exclusion Unit 1999:6)

Every young person is allocated a 'personal adviser' who brokers access to services, and is responsible for carrying out an in-depth personal assessment of the young person. This assessment process, known as the APIR (Assessment, Planning, Implementation and Review), considers all areas of a young person's life, including mental health, sexual behaviour and criminal offending, and includes information about his parents, family and friends.

Data is stored on the Connexions Customer Information System (CCIS). Although consent is normally sought before information is shared with other agencies, it is a single act of consent that grants all agencies access to the young person's electronic record until such time as consent is withdrawn. In the Government's words:

> Young people have the right to see all information held about them by Connexions, and are able to request correction of any inaccurate data. They are not able to control access to Connexions partnerships' databases, but partnerships must ensure that all processing of information about young people complies with data protection principles. (Timms, March 2002)

The Connexions service can be seen as a prototype for other childhood risk management systems—those that use assessment tools and information-sharing in an attempt to predict problems and offer early intervention.

'Predicting' children who may commit offences

A similar approach to Connexions has been developed in the youth justice sector where there is an increasing emphasis on monitoring, screening, and identifying children 'at risk' of delinquency. As the emphasis on the risk-management of children has grown, an increasing number of schemes, each with their own acronyms, have sprung up to monitor and divert children thought likely to commit criminal offences.

Children aged 8–13 may be referred to their local Youth Inclusion and Support Panel (YISP) if they are thought to be 'at risk' of offending. Following referral, the local Youth Offending Team (YOT) will assess the child, using a screening tool called 'ONSET', developed by the Youth Justice Board (YJB) and described as follows:

> Onset promotes the YJB's prevention strategy by helping to identify risk factors to be reduced and protective factors to be enhanced. It also provides information which might be helpful in selecting appropriate interventions for those identified as needing early intervention. (YJB 2003)

If the child reaches the threshold for intervention, he will be referred onwards to a local prevention programme.

YOTs in 70 local authority areas also run a preventive scheme called the 'Youth Inclusion Programme' (for 13–16 s) and a 'Junior Youth Inclusion Programme' for 8–12 s (YIP and Junior YIP).

YIPs target the 50 young people in the area who are thought most likely to offend, identified via a process called 'ID50' which involves referrals from local agencies, or uses other information. The YJB ID50 guidance says:

> There are clearly young people that are at risk but are not known by local agencies: the YIP must endeavour to access these young people. We believe that there is a considerable amount of local intelligence with regard to these young people—the YIP should assume the role of an identifying agency by collating information about these young people from local contacts, residents, tenancy associations, community groups, street wardens, etc. (YJB, undated)

In addition to the youth justice schemes, each area also has a 'Crime and Disorder Reduction Partnership' (CDRP), a Home Office initiative that, like the YOT, involves all statutory agencies and also includes voluntary sector and community representatives.

The CDRP is responsible for delivering a Home Office-designed scheme called 'Prolific and Other Priority Offenders' (PPO) which is divided into three tiers. The first tier, called 'Prevent and Deter', focuses on those thought to show signs of being predisposed towards offending. There is no lower age limit for entry to the scheme.

If a child has actually committed an offence, he will be screened with the 'ASSET' tool, (Youth Justice Board 2000) another profiling system that calculates the likelihood of re-offending by allocating a score to various assessment categories. The YJB has recently confirmed that future sentencing recommendations to the courts will be based on a child's ASSET score. (YJB 2008)

Police Databases

Different police forces have a range of systems for sharing information about children who come to their attention. (FIPR, 2006: 72–74) Sometimes these are run in partnership with other agencies: for example, the 'Nipper' database in York is run in conjunction with the 'Safer York Partnership' and records information about children at risk of harm, truants and those whose behaviour is described as 'unacceptable'—which includes playing ball-games in the street.

The Metropolitan Police Service's 'MERLIN' system records details of any child who 'comes to notice' for any reason, ranging from child protection to bullying; being present when premises are searched; where a police officer thinks that a family member has mental health problems or that the family needs social services involvement. The data on MERLIN is available to all Metropolitan Police officers, to civilian staff on completion of training and other local agencies if they have signed an information-sharing agreement with the MPS.

'Every Child Matters'

In November 2003 the Government published a green paper entitled 'Every Child Matters' (ECM) setting out an agenda that would, amongst other things, bring together the approaches developed within the Connexions service and the youth justice sector in order to monitor and intervene early in the lives of all children from birth to 18.

The green paper was ostensibly a response to Lord Laming's report into the abuse and murder of 8-year-old Victoria Climbie by her aunt and her aunt's boyfriend, with whom she was living, and was presented as a child protection agenda. In fact ECM was the continuation of the Government's 'Identification, Referral and Tracking' project that had been announced in August 2002, aimed at identifying children at risk of social exclusion (Cabinet Office 2002).

ECM set out five outcomes for children, and changed the definition of 'at risk'-previously established by the Children Act 1989 as 'at risk of significant harm from neglect or abuse'—to mean at risk of not achieving the five outcomes. These were set out as: being healthy; staying safe; enjoying and achieving; making a positive contribution; achieving economic wellbeing. This subtle shift of definition passed unnoticed by the general public, leading many to support the ECM agenda as a child protection measure.

The subsequent Children Act 2004 reconfigured local authority and health agencies into Children's Trusts, charged with working together and sharing information about children. A set of 26 Public Service Agreement Targets and 13 'Key Indicators' (Department for Education and Skills 2005) was issued to local authorities, designed to measure their progress towards achieving the five outcomes, giving the responsibility for a child's development to the Children's Trust rather than the child's parents.

The Information Sharing Index—now renamed 'ContactPoint'

The Act also provided for the establishment of a national database containing basic information about every child, details of their health and education providers and a contact list for all the services involved with him. When these plans were scrutinised by the Parliamentary Joint Committee on Human Rights, they expressed concern that:

> …if the justification for information-sharing about children is that it is always proportionate where the purpose is to identify children who need welfare services, there is no meaningful content left to a child's Article 8 right to privacy and confidentiality in their personal information. (JCHR 2004)

ContactPoint has been delayed by a series of security alerts—indeed, a government-commissioned report from Deloitte, of which only the executive summary has been published, confirms that it will not be possible to make the system fully secure. (Deloitte 2008) The latest time estimate indicates that the population of Contactpoint will begin in January 2009.

The Common Assessment Framework (CAF)

The Common Assessment Framework is a central feature of the 'Every Child Matters' agenda, and can be seen as occupying the database layer beneath

ContactPoint. Like the Connexions APIR and the Youth Justice Board profiling tools, it is a comprehensive personal assessment system that facilitates information-sharing by introducing a standardised set of criteria for agencies that have, until now, had their own distinct in-house assessment procedures.

Where it appears to any practitioner that a child has needs that are beyond the scope of that particular agency, or that the child is not progressing towards the 'five outcomes', it is expected that a Common Assessment will be carried out in order to assess what services should be provided. The government says that around half of the child population needs such services at some point.

The CAF practitioner's guide (HM Government 2006) gives a six-page list of the assessment criteria, and although practitioners are advised that they should base their assessment on evidence, several of the areas covered require the practitioner to form an opinion on issues such as whether children's relationships or parental behaviour is 'appropriate'.

The CAF has been developed into an electronic format—the eCAF—and In July 2007 the Government announced that it is in the process of creating a single, national database to hold all eCAF assessments.

Consent

A key issue with all of the existing and proposed database systems is that of gaining the consent of those to whom the information refers. It is accepted that information can and should be shared without consent when a child is at risk of significant harm but, particularly in the youth justice sector, the threshold is often far lower than this and any refusal to consent may in any case be overridden by an agency's reliance on a general, discretionary duty to prevent crime. YJB guidance on sharing information about those thought to be potential young offenders advises that: 'obtaining consent remains a matter of good practice, as opposed to a requirement of law' (YJB 2005).

The situation is further complicated by the issue of when an older child can give consent in their own right. Settled law established in Gillick v West Norfolk and Wisbech Area Health Authority (Gillick, All ER 1985) provided an exception to the common law principle that parents are responsible for their under-age children by allowing health professionals to provide contraception to under-age girls who insisted that their parents should not be informed. The rules governing this eventuality were strict.

Subsequent case law has developed the circumstances in which children can consent to include other areas, but these have largely involved medical scenarios or family law proceedings. In its non-statutory information-sharing guidance, the Government asserts that a child from the age of 12 can usually be presumed able to give valid consent to data-sharing without the need for parental involvement; however, a legal study for the Nuffield Foundation which ARCH is currently undertaking indicates that this whole area is highly contentious, and it is a vast over-simplification to make such a bold assertion.

While it is important that a child or young person can seek help and advice in confidence, and may be perfectly capable of consenting to counselling or medical treatment, this is not the same as being competent to understand the full implications of complex and/or ongoing acts of data-sharing. This data may not only be about the

child herself. The practitioner guidance to the CAF (HM Government, 2006:18) advises that:

> Opinions should be recorded and marked accordingly (for example 'Michael said he thinks his dad is an alcoholic').

Unless there are genuine concerns about possible maltreatment, should that information be recorded at all without the consent of Michael's father?

Child protection

It is a dangerous strategy to blur the boundaries between child protection and more general welfare concerns. Few would dispute the necessity of sharing information when a child is at risk of harm from abuse or serious neglect, but extending this practice to children and families seeking services carries a number of risks.

If children or their parents fear that their privacy will be violated, or that they will be disempowered by unwelcome intervention, there is a danger that help will only be accessed when a crisis has been reached. If it deters access to services at an earlier and more tractable stage, the strategy could prove entirely counterproductive. Research with children using ChildLine, a confidential phone service, highlighted the importance of confidentiality:

> The offer of confidentiality is one of the prime reasons children call ChildLine. One of the most common questions they ask of our counsellors is, 'Are you going to tell anyone about this?' (Easton, Carpentieri 2004:26)

Since the advent of 'Every Child Matters', several studies of children's views have been carried out, all of them giving a clear message that children are worried about their privacy:

> A number of the young people indicated that they would be less likely to talk to adults about their problems if they thought there was a risk that they might be communicated to other adults. (Hilton and Mills 2006:28)

> When we asked whether their decision to seek sexual health advice would be affected if they knew health workers could pass details of sexually active under-16 s to social workers [] 74% of under-16 s said they would be less likely to seek advice in these circumstances (Brook 2005)

> There was general agreement that it was essential to try to get permission before sharing information, and only break refusal of permission in the most exceptional circumstances. (Children's Rights Alliance for England 2006:7)

Practitioners may fail to notice the children who are at risk of abuse in the welter of information about low-level problems. Overloading an already under-staffed social care system with low-level concerns would not appear to be a useful child protection strategy. As the Information Commissioner famously remarked to the Education and Skills Select Committee:

> …if you are looking for a needle in a haystack I am not sure it is wise to make the haystack even bigger. (Information Commissioner 2005)

Regarding child protection as merely one possible element in a child's needs confuses two entirely different sets of circumstances. When social workers become involved with a family in need of help, they aim to engage with a family in a supportive and friendly manner. By contrast, when investigating allegations of abuse, they must adopt a far more challenging approach in the awareness that parents are likely to hide their wrongdoing and that the quality of evidence that is gathered will be important in any subsequent court proceedings. It is essential for children's safety to maintain a clear distinction between protection and welfare.

There are risks that children's data will be corruptly or carelessly disclosed, a possibility acknowledged by the Government's intention to shield the records of some children:

> Children who have a reason for not being traced—for example, where there is a threat of domestic violence or where the child has a celebrity status—will be able to have their details concealed. (Adonis 2006)

It is in any case misguided to believe that we can protect children from harm by habitually intruding upon their private space; rather, we risk increasing their potential to be victims. Abuse is about gross invasion of children's personal boundaries, and the best protection that we can offer is to empower them to recognise such incursions for themselves. But if we are to help them to develop the strong sense of self that they need to withstand or recover from abuse, we have to be scrupulous about maintaining unambiguous boundaries ourselves. We cannot in all seriousness say to a child: 'you belong to yourself—but we can watch you, share your secrets and discuss you behind your back.'

The right to privacy

Privacy is not an absolute right. It has to be balanced proportionately against the human rights of other people and, particularly in the case of children, the subject's own vital interests. However, that does not mean that a child's private life is unimportant. Although a helpless baby can have little privacy, that situation gradually changes as a child's independence flowers into the firmly-closed door and the private telephone conversations of adolescence. If children are to mature, those of us responsible for raising them to adulthood can only welcome these signs of a growing sense of competence and individuality.

Alan Westin made clear the significance of privacy for maturity and self-determination when he said:

> Changing personal needs and choices about self-revelation are what make privacy such a complex condition, and a matter of personal choice. The importance of that right to choose, both to the individual's self-development and to the exercise of responsible citizenship, makes the claim to privacy a fundamental part of civil liberty in democratic society. (Westin 2003)

Privacy is the means by which we draw our personal boundaries, categorising others into friend, acquaintance or potential threat and regulating our self-revelation accordingly. It is about how we form relationships and about the way that we define ourselves as distinct human beings. Westin rightly recognised it as a crucial part of

development: without privacy, a child cannot learn to differentiate himself from others. The ethicist, Jeffrey Reiman, makes this explicit when he says:

> Privacy is necessary to the creation of selves out of human beings, since a self is at least in part a human being who regards his existence, his thoughts, his body, his actions as his own (Reiman 1976:39)

Psychoanalytic literature is rich in discussion of the fundamental importance of boundaries to the development of ego-strength, self-awareness and creativity. Donald Winnicott maintained that the gradual evolution of 'the capacity to be alone' was essential to imagination, play and the 'symbol-making' at the heart of the creative process. (Winnicott 1971) More, he believed it essential to the development of an authentic self. (Winnicott 1965)

Anthony Storr similarly recognised the importance of solitude:

> It appears therefore that some development of the capacity to be alone is necessary if the brain is to function at its best, and if the individual is to fulfil his highest potential. Human beings easily become alienated from their own deepest needs and feelings. Learning, thinking, innovation and maintaining contact with one's own inner world are all facilitated by solitude. (Storr 1997: 28)

It is hard to see how the child who is made the object of persistent scrutiny can ever feel truly alone in his internal world—or that the external world is anything other than a dangerous place where he cannot manage unaided. What, then, are the implications of surveillance for his development of integrated, creative selfhood?

We simply do not know the long-term effects of bringing a child up under constant monitoring. In the rush to buy and sell the latest spy-gadgets and information systems, the deepest threats have not even been considered. It is meaningless to tell a child that they have independence of thought and the private space to discover who they are, if we are habitually demonstrating through our actions that this is simply not true.

Accentuating children's passivity by relentless observation is a highly dangerous experiment. In the guise of protection, we are in fact exposing children to risk and habituating them to an unprecedented level of surveillance in adult life. On a deeper level, we are impinging upon their development of personal boundaries. The events that have created the potential for 24-h surveillance of children have occurred in a piecemeal fashion, and it is now time to pull back and consider urgently just what the deeper consequences might be of overriding the child's right to privacy.

References

Adonis LA. Lords Hansard 20 March 2006; column 88

Brook. Wise Up! survey of Brook clients. London: Brook; 2005

Cabinet Office. Children at risk green paper, press release, 30th October 2002. http://www.gnn.gov.uk/Content/Detail.asp?ReleaseID=40870&NewsAreaID=2 (2002).

Cameron K. Kim Cameron's Identity Weblog. http://www.identityblog.com/?p=775 (2007).

Children's Rights Alliance for England. Children and young people talk about information sharing. London: CRAE; 2006

Deloitte. Contactpoint Data Security Review: executive Summary. Deloitte; 2008

Department for Education and Skills. Appendix to the House of Lords Select Committee on Merits of Statutory Instruments, 18th report, December 2005

Department for Education and Skills (DfES). Every Child Matters Outcomes Framework. http://www.everychildmatters.gov.uk/_files/F25F66D29D852A2D443C22771084BDE4.pdf (2005)

Dracup T. Head of the Gifted and Talented Education Unit, DfES, Teachernet webcast, 12 October 2006. http://www.teachernet.gov.uk/community/webcasts/giftedandtalented/transcript/ (2006).

Easton C, Carpentieri J. Can I talk to you again. Restoring the emotional and mental well-being of children and young people. London: ChildLine; 2004.

FIPR, Foundation for Information Policy Research. Children's databases—safety and privacy. a report for the Information Commissioner. FIPR, 2006:72–74.

Gillick v West Norfolk and Wisbech Area Health Authority. 3 All ER 402; 1985.

Hilton, Zoe and Mills, Chris, 'I think it's about trust': the views of young people on information sharing. London: Office of the Children's Commissioner; 2006

HM Government. The Common Assessment Framework for children & young people: Practitioners' guide. http://www.everychildmatters.gov.uk/_files/A19154AA073AF2F7216B25A693916CF6.pdf (2006).

Information Commissioner. Evidence to Select Committee on Education and Skills, Minutes of Evidence Q355, 24 January 2005

Joint Select Committee on Human Rights (JCHR). 19th Report, 8th September 2004

Jørgensen V, The apple of the eye: parents' use of webcams in a Danish Day Nursery. Surveillance & Society, CCTV Special (eds. Norris, McCahill and Wood), 2004; 2(2/3): pp. 446–463

Leaton-Gray S. Quoted on 'Leave Them Kids Alone' website. http://www.leavethemkidsalone.com/expert.htm#fact_00 (2007).

Manchester Evening News. School puts CCTV in toilets to stop bullies, 7th February 2007

Reiman J. Privacy, intimacy, and personhood. Philos Public Aff 1976;6(1):26–44.

Social Exclusion Unit. Bridging the gap. HMSO; 1999

Storr A. Solitude. London: Harper Collins; 1997.

Timms S. HM Government Minister for Schools, Hansard: Written Answer 28th January 2002, Hansard Column 110W

Timms S. HM Government Minister for Schools, Hansard: Written Answer 20th March 2002, Hansard Column 341W

Warner M. Managing monsters—six myths of our time. The Reith Lectures, Vintage, 1994

Westin AF. Social and political dimensions of privacy. J Soc Issues 2003;59(2):431–53.

Winnicott DW. The maturational processes and the facilitating environment: studies in the theory of emotional development. London: Hogarth; 1965.

Winnicott DW. Playing and reality. London: Tavistock; 1971.

York Press. Anger over York schools that fingerprint their five-year-olds, 8th January 2007

Youth Justice Board (YJB). Onset referral and assessment framework. http://www.yjb.gov.uk/en-gb/practitioners/Assessment/Onset.htm (2003)

Youth Justice Board. ID50- guidance document for partners (YJB current). http://www.yjb.gov.uk/NR/rdonlyres/0233E9E7-8E58-45E0-ACF8 E3190B8EAD19/0/ID50guidancedocumentforpartners.doc (undated)

Youth Justice Board (YJB) and Association of Chief Police Officers. Sharing personal and sensitive information on children and young people at risk of offending: a practical guide. YJB; 2005

Youth Justice Board (YJB). Youth justice: the scaled approach (D99). YJB; 2008

Youth Justice Board (YJB). Asset (B108). http://www.yjb.gov.uk/Publications/Scripts/prodView.asp?idproduct=203&eP= (2000)