# Digital Handcuffs or Electronic Nannies: Children, Privacy and Emerging Surveillance Technologies

**plenary session paper at**
***Watch This Space* children & privacy conference**
**—Melbourne, May 2010 —**

**Bruce Arnold**
**Faculty of Law**
**University of Canberra**

# Digital Handcuffs or Electronic Nannies: Children, Privacy and Emerging Surveillance Technologies

## — Abstract —

Convergence of parental anxieties, commercial opportunism and advances in network technologies is providing the basis for unprecedented surveillance of children and young people. Those technologies extend from automated monitoring of SMS/MMS on mobiles used by minors and mobile-based geolocation tools that allow parental monitoring of the movement of young people to proposals for 'tagging' children (or those experiencing a second childhood) with subdermal identity/tracking chips. The technologies have been promoted as an electronic nanny or as appropriate responses to predation and risk along the digital frontier. They have been damned as digital handcuffs that erode the autonomy of young people, are readily subverted and, more seriously, are open to abuse by people outside the family.

The paper offers an introduction to current and foreshadowed technologies, looking beyond a debate that has centred on surveillance of desktop-based web-browsing and mandatory filtering of internet content. It explores the interaction of regulation, economics and demand, given that technologies are not situated within a legal or commercial vacuum. It assesses the status of those technologies under existing Australian law. In highlighting particular concerns the paper draws on research from Australia and overseas regarding risk, use/misuse of surveillance tools and legal responses to privacy challenges at the level of principle and practice.

It asks whether children are the next generation of 'canaries in the digital coalmine', subject to surveillance perceived as legitimate because of their age and can hence be adapted for management of other groups – such as the elderly or criminal – that are denied full personhood.

The paper also concludes that in a digital environment respect for the privacy of young people is both a legal and practical conundrum. Conflicting advocacy statements by vendors, parents, civil liberties groups, police, social service personnel and other interests will not be reconciled unless we recognise privacy as a human right that should be enjoyed by those under 18.



an earlier version of this paper is available on the Victorian Privacy Commissioner's site

# Digital Handcuffs or Electronic Nannies: Children, Privacy and Emerging Surveillance Technologies

## — Contents —





The author has no commercial interests (eg consulting contracts or equity in privacy solution vendors) that represent a conflict of interest in delivery of this paper. Comments in this document are not necessarily representative of the University of Canberra.

The author gratefully acknowledges advice and encouragement from Geoff Stewart and William Orr. They are not responsible for errors of fact or interpretation in the following pages.

# Digital Handcuffs or Electronic Nannies: Children, Privacy and Emerging Surveillance Technologies

## INTRODUCTION

This paper is concerned with children, privacy and digital surveillance technologies.[1]

Some of those technologies, such as social network services (notably MySpace and Facebook) or aids to parental monitoring of web browsing, are familiar, are available 'off the shelf' and have been the focus of community education campaigns by bodies such the Office of the Victorian Privacy Commissioner (OPC) or the Australian Communication & Media Authority (ACMA). They exist alongside surveillance infrastructure, such as city-wide and site-specific closed circuit television (CCTV) networks, that may be the subject of special regulation and that generate conflicting anxieties about the surveillance of children.[2]

Other technologies, such as automated surveillance of SMS, are being spruiked by vendors and are likely to be available in Australia within a few years, although there are question marks about their commercial viability. Others still, such as geolocation bracelets and subdermal RFID tags, are unlikely to gain traction among the community at large.[3]

All should provoke thought about law, about education, about relationships between minors and parents/guardians, about the commercialisation of surveillance, and about respect for children as individuals in environments where there are inescapable tensions between autonomy and care.

### Basis

The paper is predicated on five notions.

The first is that technology is neutral but its application is not.

A device may be a shield or a sword, an instrument of imprisonment or a protection against danger, depending how it is being used, when it is being used and who is using it. Use of technology always has costs, although we may decide that costs are far outweighed by benefits or privilege a financial calculus over concerns for individual and collective autonomy.[4]

---

[1] Many of the paper's conclusions are applicable to teenagers but the following pages are concerned with children, ie people who are less than 13 years old. The paper concentrates on Commonwealth and Victorian law.

[2] For example, that CCTV will deter child abduction, prevent molestation or instead be used by paedophiles … the latter being one fear voiced by participants in the 'Marginalized Youth, Surveillance and Public Space' study by Dean Wilson, Jen Rose & Emma Colvin reported at the *Watch This Space* conference. As points of entry to the literature on CCTV and youth see Clive Norris, *The Maximum Surveillance Society* (Oxford: Berg 1999); Adam Sutton & Dean Wilson, 'Open-street CCTV in Australia: The Politics of Resistance and Expansion', 2(3) *Surveillance and Society* (2004) 310; and Clive Norris, Jade Moran & Gary Armstrong [ed], *Surveillance, Closed Circuit Television and Social Control* (Aldershot: Ashgate 1998).

[3] There is no authoritative map of the surveillance technologies available in Australia to individuals, families and small businesses or independent institutions. The overseas popular literature, predominantly from the United States and often founded on unacknowledged assumptions regarding US constitutional law, is marked by discrete 'gee whiz' or conspiricist ('Secret State' and 'Spies in the Sky') genres. Little of the academic literature provides an informed and comprehensive view of what is available, what is in use and what is likely to be widely available in the near future.

[4] James Carey, *Communication as Culture: Essays on Media & Society* (London: Routledge 1992) and Langdon Winner, *Autonomous Technology: Technics-out-of-control as a Theme in Political Thought*

The second notion is that surveillance of minors by parents/guardians and third parties, whether out of concern for the minors as small human beings or in an effort to minimise corporate/personal liability, is not new. In a range of circumstances it is appropriate.

Surveillance *per se* is not antithetical to a Rawlsian or Gewirthian 'flourishing'.[5] Our concerns instead should focus on monitoring that stifles the achievement of selfhood (the happy, independent, resilient and responsible child) and on regulatory regimes that either commodify childhood or that expose minors to risks that those children are unequipped to address.

The third notion is that characterisations such as 'digital natives', 'internet generation' and 'e-generation' are unhelpful.[6]

Those characterisations grab attention for marketers and serve to legitimate hyperbolic statements by dot com gurus but are problematical for two reasons. The first is that not all minors are 'wired' … and wired in the same way, at the same time and all the time. We should be wary of a reductionism that elides cultural and economic differences and that treats a five year old, an 11 year old and a 16 year old as having the same motivations, skills, self-discipline and experience. Exposure to digits does not bleach away difference. A second reason for concern is that exposure to new technologies and new media does not necessarily confer wisdom and does not necessarily enhance agency.[7] Familiarity may reduce a child's wariness and inhibit action that would minimise harms involving peers (eg cyberbullying and sexting), marketers or adults engaged in offences such as 'grooming'. It may instead assist a child to differentiate between phantom and substantive dangers, discover that some experiences are unpleasant but not crippling, and conclude that parents will reward rather than abuse expressions of trust (eg will not withdraw all mobile/internet access if the child confesses that there has been a minor transgression of rules or has encountered something unpleasant online).

The fourth notion is that it is useful to move beyond oppositional constructions in which privacy of minors is construed primarily in terms of disagreements between parents or guardians and the children for which those authority figures are (or should be) responsible.

It is tempting to think of child privacy as a vertical relationship: the child as the 'subject of the parental gaze': watched, disciplined by and reacting to parents or parental surrogates. Recognition of children as people rather than subjects, in particular as rather passive subjects that lack agency (and are thus unable to make choices and to subvert surveillance

---

(Cambridge: MIT Press 1977). For fashionable disquiet about notions of neutrality see Neil Postman, *Technopoly: The Surrender of Culture to Technology* (New York: Vintage 1993).

[5] Alan Gewirth, *Self-Fulfillment* (Princeton: Princeton University Press 1998). From an Australian perspective that flourishing – consistent with national and global rights charters – encompasses a happy and fulfilling childhood (eg one in which the child explores, learns self-regulation, socialises with familiar/unfamiliar adults and peers, surmounts difficulties in developing personal resilience, and expresses a deserved trust in parents/guardians. An overemphasis on surveillance tools and practices is antithetical to that flourishing and potentially results in harms that outweigh the dangers from which the child was to be protected.

[6] See for example Don Tapscott, *Growing Up Digital: The Rise of the Net Generation* (New York: McGraw-Hill 1998), John Palfrey & Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books 2008), Wim Veen & Ben Vrakking, *Homo Zappiens: Growing Up In a Digital Age* (London: Continuum 2006). There is a more robust view in Sue Bennett, Karl Maton & Lisa Kervin, 'The Digital Natives Debate: A Critical Review of the Evidence', 39(5) *British Journal of Educational Technology* (2008) 775 and the empirical research reported in Keri Facer, John Furlong, Ruth Furlong & Rosamund Sutherland, *Screen Play: Children & Computing in the Home* (London: Routledge Falmer 2003).

[7] The popular and academic literature about the '419 Scam' (the daily email generously offering you a chance to share in billions misplaced by UK bankers and solicitors or held by the heirs of Idi Amin, Saddam Hussein, Ferdinand Marcos etc) is thus replete with tales of barristers, judges, professors, police officers, psychologists and others swallowing hook, line and stinker. Being able to type (or have a credit card) does not mean that you are smart or able to act on your realisation that something is awry. The notion that absence of bifocals and wrinkles confers digital wisdom would appeal to William Blake and contemporary romantics such as Clay Shirky but is inconsistent with reality.

mechanisms by for example borrowing a mate's mobile phone or personal computer), offers a more realistic model of privacy.

In particular that model recognises horizontal relationships, in which questions about privacy and about potential harms involve the child's peers, for example protection from cyberbullying rather than from the stereotypical overbearing parent of the 'cottonwool kid' or 'bubblewrap child' who smothers little Johnny with digital handcuffs that monitor every mouse-click, keystroke or bus ride.[8]

The final notion is that much of the appeal of child surveillance technologies has a distinctly magical character, with tools offering comfort to anxious parents (or cautious guardians) through solutions that are portrayed as responsible, comprehensive and reductive of dilemmas.

Silver bullets are attractive because they are easy to apply, affirm the user's authority, relieve the user of moral burdens and eliminate challenges. One Australian study, commenting on household use of the internet and other new media, thus reported that –

> The parents in our study wished that family politics in respect of ICT were simpler. If only they could cut through the exhausting rounds of critique, negotiation, argument, and decree that accompany each variation in domestic media presence and with each new stage in their children's independence; if only there was an alternative to wave after wave of admonishment, reasoning, cajoling, raised voices, bargaining, and dire warnings.[9]

## Orientation

The paper is aimed at a general audience, rather than legal or information technology specialists, in an effort to bridge some of the digital divides.

Claims of a 'digital divide' have been a feature of public policy debate over the past two decades and have, for example, driven initiatives such as the One Laptop Per Child (OLPC) project[10] and Australia's National Broadband Network (NBN),[11] both promoted as providing an economic and cultural cornucopia that will enrich the lives of today's children and tomorrow's.[12] Preoccupation with infrastructure – boxes, switches, cables – and with intractable questions such as taming Telstra (the $80 billion gorilla in the cabinet room) has obscured more fundamental divides between lawyers, economists, engineers, educators and other specialists who often seem to be talking to themselves rather than to each other.

The *Watch This Space* conference is thus significant because it brings together participants whose concerns are not unique but who often seem to be using incomprehensible dialects and reaching divergent conclusions about what can or should be done. Much of that discourse is

---

[8] See for example Leanne Franklin & John Cromby, 'Everyday Fear: Parenting and Childhood in a Culture of Fear', 161 in Leanne Franklin & Ravenel Richardson [ed] *The Many Forms of Fear, Horror & Terror* (Oxford: InterDisciplinary Press 2009); Digby Jones, *Cotton Wool Kids* (HTI Issues Paper 7) (Coventry: HTI 2007) and Karen Malone, 'The bubble-wrap generation: children growing up in walled gardens', 13(4) *Environmental Education Research* (2007) 513.

[9] Chris Shepherd, Michael Arnold & Martin Gibbs, 'Parenting in the Connected Home', 12(2) *Journal of Family Studies* (2006) 218.

[10] Marcus Leaning, 'The One Laptop per Child Project and the Problems of Technology-led Educational Development', in Ilene Berson & Michael Berson [ed] *High-Tech Tots: Childhood in a Digital World* (Charlotte: IAP 2010) 231.

[11] See for example the Prime Minister, Treasurer, Minister for Finance and Minister for Broadband joint media release 'New National Broadband Network' (7 April 2009) and Minister for Finance & Deregulation and Minister for Broadband, Communications & the Digital Economy joint media release 'Landmark Study confirms NBN vision is achievable and affordable (6 May 2010) – "the National Broadband Network is achievable, financially viable and will transform life and business in Australia".

[12] Suzanne Willis & Bruce Tranter, 'Beyond the 'Digital Divide': Internet Diffusion and Inequality in Australia', 42(1) *Journal of Sociology* (2006) 43 and Julian Thomas, Scott Ewing & Julianne Schiessl, *The Internet in Australia: CCI Digital Futures Report (*CCI, Swinburne University of Technology 2008).

foreign to the children who are the subject of the conference,[13] despite a generation of worthy (and arguably ignored) education initiatives from government agencies and from enterprises that are seeking to buff their corporate persona. In Australia we have had little success in bridging the divide between minors and the rest of the community, a failure partly due to non-recognition of privacy as a human right that extends beyond a cat's-cradle of statutes, a right that should be enshrined in the national constitution and in institutional practice.[14]

## Coverage

As the final item on the *Watch This Space* conference program this paper does not aim to recapitulate the earlier coverage of Australian privacy statutes,[15] to critique recent recommendations by the Australian Law Reform Commission,[16] or to offer new insights about how minors perceive privacy rights, responsibilities and opportunities.

Instead, the following paragraphs explore the interaction of surveillance technologies, regulation, economics and demand, given that technologies are not situated within a legal or commercial vacuum. They highlight some implications for law and practice regarding new technologies that affect Australian children and potentially affect other people who are seen as having lesser rights – what one colleague refers to as 'privacy lite' – on the basis that those people are stigmatised, disabled or otherwise disadvantaged.[17]

The paper has two parts.

The first part asks questions about how we construe privacy, regulatory and economic frameworks, and agency. Why have we embraced some surveillance mechanisms and will reject others, or valorise tools for parental comfort – substantiated or otherwise – over personal relationships that occur offline?

The second part highlights some technologies that are currently in use, will be commercially available in the near future, or have been mooted as solutions for a range of problems.

Some of those technologies impinge on the privacy of minors and are seen as unexceptional, either construed as involving an appropriate balance between individual autonomy and supervision or not recognised as recognised as posing privacy questions. That non-recognition is inherent in the comment by one ANU law student earlier this year that "animals and children have no privacy rights, because animals are wild and children are not people" … a stance that may resonate with some conference participants.[18]

Some of the technologies, either because of novelty or because of their character, will be seen as egregious infringements of the rights of both minors and parents/guardians.

## OBSERVATION AND ITS DISCONTENTS

A preceding paragraph of this paper asserted that there are always costs in the use of technologies, although those costs may be unrecognised or simply considered as

---

[13] Irrespective of the reality that few minors or their parents are familiar with legal jargon such as tort or academic buzzwords such as governmentality and biopolitics, numerous studies indicate that minors may view law and risk differently to their guardians and accordingly use different language. See for example Australian Law Reform Commission, *Review of Australian Privacy Law: Discussion Paper Vol 3* (ALRC Discussion Paper 72) (Sydney: Australian Law Reform Commission 2007) 1719-1720.

[14] Bede Harris, *A New Constitution for Australia* (London: Cavendish 2002) 31.

[15] Among introductions to the Australian regime see Moira Paterson, *Freedom of Information & Privacy in Australia* (Chatswood: LexisNexis Butterworths 2005) and the ALRC report at 16 below.

[16] Australian Law Reform Commission, *For Your Information: Australian Privacy Law & Practice* (ALRC Report 108) (Sydney: Australian Law Reform Commission 2008).

[17] I am grateful for comments by Paulette Neilsen and Susan Priest regarding the realities of privacy experienced by people undergoing a 'second childhood', inside and outside of institutional care.

[18] For a contrary view, which the author of this paper finds unpersuasive, see Brett Mills, 'Television Wildlife Documentaries and Animals' Right To Privacy', 24(2) *Continuum: Journal of Media and Cultural Studies* (2010) 193. See also Desmond O'Neill, 'Tagging should be reserved for babies, convicted criminals and animals', 326 *British Medical Journal* (2002) 281.

incommensurate with the benefits from using a specific tool or dealing with a particular risk.[19]

How can we make sense of technologies, privacy and children? How do we frame and identify the choices, manage tensions?

## Regulatory Frameworks

Legal historian F W Maitland is recalled, albeit inaccurately,[20] for the characterisation that law is a seamless web, a fabric that to the distress of undergraduate law students and politicians is not readily divisible into discrete patches that can be excised, inserted or manipulated without thought for where they fit in. In thinking about children, privacy and emerging technologies we should recognise interrelationships and questions about practice, rather than assuming problems will disappear if we can darn the privacy patch with some digital thread or add a childrens' protocol to one of the privacy statutes.

Current and emerging technologies impinging on the autonomy of young people involve four interrelated regulatory frameworks: privacy, telecommunications, content management and health. They are also affected by contract law, the elephant whose presence in the lounge room or schoolyard we typically do not refer to or simply do not recognise until it steps on someone's foot.

### Privacy

Participants at the *Watch This Space!* conference will have come to the event with some sense of privacy law at the level of principle and practice, and during the sessions will have encountered discussions about what privacy means in relation to minors, particularly people under the age of 16, 15 or 12.

The fuzziness of those age markers reflects the variation evident in law across Australia about what is a 'child' for purposes of criminal responsibility, concessional fares on public transport and other legal categorisations. In most law, as in life, there is no identikit picture of childhood, a one size fits all definition that covers kids from Carnarvon to Carlton, the stereotypical introverted 'mummy's girl' and the 'feral street kid' 'wise beyond his years'. National privacy law, looking to principles rather than specifics, essentially does not treat the privacy of children as a special category.

Children are instead people, albeit people who are recognised through broad notions of 'reasonable' practice as requiring special treatment because of an assumed lower capacity to understand their status as data subjects and to enter into informed relationships.

Adults, for example, are tacitly assumed to have a sense of themselves as data subjects, an ability to commodify their identity (for example to gift a marketer with personal information in exchange for an opportunity, however remote, to win a prize) and scope for taking action where rights are perceived to be infringed.[21] Adults also have more power than children, a power that is associated with the ability to set and enforce boundaries, hard or permeable, systematic or *ad hoc*. Reasonableness, embodied in industry protocols and in some state/territory statute law, provides a broad protection for children, with the expectation that children's rights – if recognised – will be exercised through an adult.

International agreements such as the Convention on the Rights of the Child (CROC) are broad and as assimilated by Australian law embody a common sense approach to the autonomy of the child, for example as members of a class of people who may be particularly vulnerable,

---

[19] Andrew Stewart, 'On Risk: Perception and Direction', 23 *Computers & Security* (2004) 362 and Barry Glassner, *The Culture of Fear: Why Americans are Afraid of the Wrong Things* (New York: Basic Books 1999).

[20] Frederick Maitland, 'A Prologue to a History of English Law', 14 *Law Quarterly Review* (1898) 13.

[21] Daniel Solove, *The Digital Person: Technology & Privacy in the Information Age* (New York: New York University Press 2004).

who may particularly benefit from parental guidance, who lack substantial physical and financial resources, and who may appropriately be subject to reasonable parental discipline.[22]

Law thus privileges family relationships (or guardianship relationships modelled on that of the family) while in practice providing substantial leeway for marketers. We have not seen the development of child-specific privacy protection statutes, such as those in the United States.[23] Australian law arguably reflects and reinforces the realities of Australian society, with children in practice – as opposed to postgraduate philosophy seminars and the occasional *outré* 'playpower' anarchist such as Richard Neville – having no privacy *vis a vis* their parents.

Put crudely, mum and dad *can* legally search little Johnny's bedroom and track where he has been wandering on the web, irrespective of whether he has a key and of mum's ability to physically pull him away from the keyboard when it is bath-time.[24] If children are people, in terms of privacy law they are people-lite rather than adults.

## Telecommunications

The functionality of much digital technology – and its significance for privacy – is dependent on networking. An isolated device is typically dumb. That device starts to impinge on privacy once it communicates with other devices over public/private networks and for example allows covert/overt tracking of an individual, automated creation and analysis of profiles (such as consumption patterns) of each member of a class, or merely an exchange of messages between human operators (a parent and a child, the online school bully and a target of victimisation, a minor – or a law enforcement officer posing as a child – and an individual engaged in 'grooming').

Australian law regulates the establishment, maintenance and use of those networks primarily through national telecommunications[25] and crimes[26] statutes. Those Acts broadly give substantial immunity to connectivity providers (telecommunication groups such as Optus and Telstra, specialist internet service providers such as iiNet that utilise infrastructure owned by telecommunication companies). They derive from *fin de siecle* legislation concerned with the regulation of telegraphic and postal services, with the service provider being freed of the responsibility to closely monitor every message transmitted via their network.[27]

Telecommunication law is famously 'content neutral', concerned with the 'pipes' rather than the data that flows through them. It does not provide special treatment for or recognition of children. Their status is instead a matter of content regulation law (for example restrictions on the provision to minors of adult content, including responsibilities for online publishers and intermediaries such as internet service providers) and of contract law.

## Conduct and Content Regulation

Why are we concerned about content regulation? The answer to that question is that much of the anxiety about the privacy of children is founded on perceptions that children are

---

[22] For CROC see Philip Veerman, *The Rights of the Child and the Changing Image of Childhood* (Dordrecht: Martinus Nijhoff 1992), Alastair Nicholson, 'The United Nations Convention on the Rights of the Child and the Need for its incorporation in a Bill of Rights', 44(1) *Family Court Review* (2006) 5, essays in Michael Freeman & Philip Veerman, *The Ideologies of Children's Rights* (Dordrecht: Martinus Nijhoff 1992) and Geraldine Van Bueren, *The International Law on the Rights of the Child* (The Hague: Nijhoff 1998).

[23] Notably the *Child Online Privacy Protection Act of 1998* (15 USC 6501-6506) (aka COPPA), a focus of current proposals to strengthen protection of children and teens using online social network services.

[24] The catchphrase 'a man's home is his castle' falls short: children are merely tenants in the castle, subject to direction by the feudal lord and unlikely to gain meaningful protection from those outside the ramparts unless there is egregious abuse such as imprisonment in a cupboard or ongoing deprivation of food.

[25] See in particular the *Telecommunications Act 1997* (Cth).

[26] For example the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2004* (Cth) and *Criminal Code Act 1995* (Cth).

[27] One introduction is provided by Alasdair Grant [ed], *Australian Telecommunications Regulation* (Sydney: UNSW Press 2004).

vulnerable, notably through inexperience, and may encounter harmful content when they are 'online' (for example when browsing the web, receiving email or engaging in short message service and multimedia message service [aka SMS, IM and MMS] interactions). That content may be way is viewed or what is done, including what is done by minors.

Management of content is framed through law that restricts particular activities such as misuse of a carriage service (for example using a mobile phone to abort an exam using a bomb threat) or the creation, provision and consumption of particular words and images.

That framework is a complex mixture of Commonwealth[28] and state/territory statute law, common law and industry protocols. It impacts on the privacy of children as authors and audiences, people who might be the victims or perpetrators of bullying, sexting,[29] stalking,[30] one-off substantive/hoax threats and grooming[31] or who might encounter inappropriate content (pornography, bomb-making guides, DIY suicide instructions).[32]

The presumption in law is that parents, and those acting in their stead, have the ability to disregard a child's expectations of privacy and observe what children are doing online – what they are viewing, what they are communicating. There is some expectation that parents will intervene where the child's use of 'new media' is inappropriate, for example to restrict access to pornography or to stop a minor sending threatening communications.[33]

We can expect to see calls, modelled on litigation in the United States, for parents to be held responsible where they were indifferent to activity such as cyber-bullying (eg resulting in the death of a child's peer), hacking or large-scale copyright infringement. Such calls place the onus on parents and guardians to deny the child's autonomy and override youthful expectations of privacy.[34]

## Health

Finally, what about health? Are questions of health and privacy restricted to disagreement about the autonomy of minors in seeking and receiving medical services, addressable for example using protocols regarding disclosure to parents/guardians of information provided by children to general practitioners or therapists on the basis that 'you can't tell mum'?

Health regulation may become significant as we explore suggestions for subdermal chips or other identification (and hence tracking) biotechnologies. Economics and consumer repugnance aside, the major impediment to implantation of surveillance devices in children – and in people experiencing a second childhood – is a lack of enthusiasm on the part of health

---

[28] Notably the *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) and *Communications Legislation Amendment (Content Services) Act 2007* (Cth).

[29] Among divergent views see Sharon Shafron-Perez, 'Average Teenager or Sex Offender: Solutions to the Legal Dilemma Caused by Sexting', 26(3) *John Marshall Journal of Computer & Information Law* (2009) 431; Amparo Lasén & Edgar Gómez-Cruz, 'Digital Photography and Picture Sharing: Redefining the Public/Private Divide', 22(3) *Knowledge, Technology & Policy* (2009) 205; and Peter Cumming, 'Children's Rights, Children's Voices, Children's Technology, Children's Sexuality' (Roundtable on Youth, Sexuality, Technology, Congress of the Humanities and Social Sciences 2009) (Ottawa: Carleton University 2009).

[30] For example the *Crimes (Stalking) Act 2003* (Vic) and *Crimes Act 1900* (ACT).

[31] For example the *Crimes Amendment (Sexual Procurement or Grooming of Children) Act 2007* (NSW). Cautions are provided in Suzanne Ost, *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press 2009).

[32] *Criminal Code Amendment (Suicide Related Material Offences) Act 2005* (Cth).

[33] Egregious failure to prevent harm associated with sustained exposure to adult content, in particular illegal content, has for example been cited as a justification for intervention by welfare agencies under child protection statutes.

[34] For a discussion of self-management and autonomy in relation to media content see Tanya Byron, *Safer Children in a Digital World: The Report of the Byron Review* (London: Department for Children, Schools & Families 2008) 3. For guardianship roles and risks see Neil Ballantyne, Zachari Duncalf & Ellen Daly, 'Corporate Parenting in the Network Society', 28(1/2) *Journal of Technology in Human Services* (2010) 95.

regulators such as Australia's Therapeutic Goods Authority (TGA) and the US Food & Drug Administration (FDA), rather than Australian privacy statutes.[35]

## Contract

A preceding paragraph referred to contract law[36] as the 'elephant in the room', the unacknowledged legal mechanism that has fundamental implications for the privacy of adults and minors and that reflects Australian law's weighting of commercial values over notions of human rights.

Contract is important for three reasons. The first is that most networked activity involves contract law. Information, to use the tagline used by some cyber-libertarians, might want to be free but service providers rarely want to operate in a legal vacuum and will therefore use contract law to reduce uncertainty and bound liability.

Given that minors broadly lack legal capacity and financial capability (notably credit cards) most 'new media' contracts are between corporations and adults, even though the mobile phone or the internet connection might be exclusively used by the minor … and by that child's friends.[37] Privacy resides with the parties to the contract; children, for example, use the mobile at the parent's pleasure. In contract law the child does not have a right to prevent the parent who has paid for the connectivity from monitoring what use is being made of the mobile phone, landline, mobile phone or other device/service.[38]

The second reason is that Australian privacy law at the state/territory and national levels typically allows individuals to waive some or all statutory protection. Terms & Conditions (T&C) matter!

Use of particular services typically requires consumers to relinquish what they might regard as rights, rights that as the Australian Law Reform Commission and other entities have recurrently noted do not have a constitutional basis.[39] (Neither children nor adults have a comprehensive right of privacy under the Australian Constitution, a right that might have been enshrined if the Rudd Government had embraced recommendations as part of the National Human Rights Consultation exercise).[40]

The final reason is that contract law, underpinned by telecommunication law, allows telecommunication service providers to restrict what some intermediaries do with the service provider's networks. The more ambitious surveillance proposals will fail *before* they reach privacy hurdles because they have not gained the support of the service providers, whether because of squeamishness about bad public relations (and critics have unkindly noted on occasion that major providers such as Telstra seem to be indifferent to community perceptions) or more substantively because the economics are unpersuasive.

---

[35] *Therapeutic Goods Act 1989* (Cth).

[36] Contract is a creature of common law (ie courts rely on precedents established by historic judicial decisions rather than on statutes, the Acts made by parliaments). Although it is not codified, for example you cannot determine your rights and responsibilities by consulting a 'Contract Act', its operation is somewhat circumscribed by consumer protection, trade practices and other statutes. Enhanced protection of privacy, through for example strengthened privacy statutes or a constitutional amendment enshrining privacy as a fundamental human right, could be expected to limit abuse of privacy attributable to contract law.

[37] That lack of capacity is reinforced through the 100 Points regime for identity verification that further restrict minors from acquiring, although not of course from using, mobile phones.

[38] That deficiency is analogous to the circumscribed rights of employees who use corporate networks or operate corporate vehicles monitored using GPS tracking tools.

[39] That relinquishment is not restricted to 'online' or children. The author of this paper was for example interested, when registering at one of Melbourne's more upmarket hotels on the eve of the conference, to see that the registration form claimed that guests authorised the hotelier to provide their address and other details to undisclosed "third parties". That claim was a statement, rather than an option (ie there was no tick box). Given that adults have agency the statement could however be deleted with a pen.

[40] The national *Human Rights Framework* announced by Commonwealth Attorney-General McLelland in April 2010 does not expressly refer to privacy, with economic managerialism arguably taking priority over a formal recognition of the human rights evident in all comparable jurisdictions.

## Technology

This paper has referred generically to 'technologies', rather than specific services such as the internet or devices such as mobile phones. That reference is deliberate, given that privacy concerns in relation to children are best understood as questions of principle rather than in terms of particular boxes, business models or communication protocols.

It is clear that people – including the mythical digital natives – use digital technologies differently. Not everyone has access to the same infrastructure (eg iPods, iPhones, Wii, iPads, Gameboys, wireless laptops, broadband or even a reliable low-cost mobile connection). Not everyone values the same features. Privacy concerns thus vary.

That variation reflects the different affordances of technologies, essentially the functionalities or attributes valued by the consumer and by other parties.[41]

That comment may sound fatuous but consider how children use mobile phones. For some the chief value of the mobile is an indicator of status, quite independent of connectivity. Possession of the mobile signals that the bearer is trusted by the person whose name appears on the contract or is sufficiently senior to have undergone a rite of passage (with receipt of a phone marking the point at which the bearer moves from being a 'littlie' to someone who is responsible … the 2010 equivalent of the transition from trainer wheels or to long pants).[42] Possession may instead simply signal that mum has more money than the parents of the other kids in the schoolyard or is more concerned about maintaining a mobile umbilical cord.[43]

Some children rely on electronic communication for contact with a physically (rather than emotionally) distant parent.[44] Some children eschew voice calls in favour of SMS;[45] an affordance with consequences for monitoring by parents after lights out[46] and for creation of a

---

[41] Donald Norman, *The Invisible Computer* (Cambridge: MIT Press 1998); Michael Hammond, 'What is an affordance and can it help us understand the use of ICT in education?', *Education & Information Technologies* (2009) and Jennie Carroll, Steve Howard, Frank Vetere, Jane Peck & John Murphy, 'Just What To the Youth of Today Want? Technology Appropriation by Young People', 5 *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (2002) 131. For a caution on methodologies see Sampsa Hyysalo, 'Some Problems in the Traditional Approaches to Predicting the Use of a Technology-Driven Invention', 16(2) *Innovation: The European Journal of Social Science Research* (2003) 117.

[42] The transition from trainer wheels is occurring at an earlier age. Normalisation of phone possession among minors, parental acceptance of vendor claims that mobiles will keep kids safe and special connectivity deals in the mobile phone market mean that it is increasingly common for young children (eg in the 4 to 6 year cohort) to receive a mobile. That has been reflected in the development of phones with limited functionality, for example the Firefly or Kyocera Mamorino noted later in this paper. In practice such 'dumbed down' devices do not seem to be selling well in Australia, whether because vendors are charging a premium or because the distribution network is inadequate (the latter being reflected in the incomprehension among retail staff when the author visited shopfronts in Canberra and Sydney seeking a 'kid safe' phone). Network operators have to *want* to push devices in creating or responding to a parental need.

[43] The April 2009 Australian Bureau of Statistics report on 'Children's Participation in Cultural & Leisure Activities' indicates that 60% of five to eight year olds accessed the internet, compared with 96% of 12 to 14 year olds. 31% of children had a mobile phone, although was significant variation by region (highest ownership in Tasmania) and by family type. Less authoritative private surveys claim that 25% of Australian children age seven to ten has a personal (as distinct from shared) mobile. As a point of entry to debate about use of mobiles see Niranjala Weerakkody, 'Mobile Phones and Children: An Australian Perspective', 5 *Issues in Informing Science and Information Technology* (2008) 459.

[44] See for example Bruce Smyth, 'Parent-Child Contact in Australia: Exploring Five Different Post-Separation Patterns of Parenting, 19(1) *International Journal of Law, Policy & the Family* (2005) 1.

[45] Detailed figures on the use by Australian children of SMS are unavailable. As a point of reference the latest report from the Pew Internet & American Life project (February 2010) suggests that 54% of US teens text daily, more than half send over 50 SMS per day and one in three send more than 100 SMS per day. Per capita use of SMS in Australia continues to be higher than that in the US.

[46] Rachel Campbell, 'Teenage Girls and Cellular Phones: Discourses of Independence, Safety and Rebellion', 9(2) *Journal of Youth Studies* (2006) 195. See also Peter Glotz, Stefan Bertschi & Chris

virtual private space when in the company of adults or peers.[47] Some children rely on chat rather than email, with use of the web being centred on Facebook and MySpace or a handful of chat-rooms rather than Wikipedia, the delights of Club Penguin or googling for snaps of Britney Spears' endowments.

Those affordances have privacy consequences if the parental surveillance regime is founded on looking at web browser histories or rummaging through the trash folder for deleted email on a child's personal computer.

Differing affordances affect the nature of privacy concerns – for example is my child being groomed by an interstate stranger (or by his cousin six blocks or six metres away) – and the scope for using technology to address those concerns in ways that may or may not pose privacy conundrums. The same technology, for example, that allows children to text the night away without a parent hearing the 'F word' also potentially allows that parent to receive a copy of the communications … a copy that does not conflict with the contract and does not appear to substantively breach privacy law.[48]

Where is the technology heading? Are we about to see a new generation of digital handcuffs and online nannies? The second part of this paper highlights possible directions. In considering privacy however it is useful to preface that discussion with some cautions.

What is striking about the literature on digital technologies is how often:

- the experts (including the very best MBAs that investment banks, e-government agencies and telecommunication giants could buy) have got it wrong,
- breathless IT journalism has missed the mark (an increasing problem as the mass media groups cut costs by recycling media releases and heading downmarket to compete with Wikipedia), and
- the uptake – or non-uptake – of new technologies or services has surprised technology, regulatory and marketing pundits.

The commercial and regulatory landscape is littered with predictions that in retrospect are laughable.

William Gates, founder of one of the conference's corporate sponsors, thus assured us that the spam problem would be solved by 2006. Other experts have variously announced that no print newspaper would be in existence by 2008, only a few thousand enthusiasts would ever buy a personal computer (and they'd only be using those devices for managing their recipe books or cheque books), the iPod and iPhone would be resounding failures, the Segway would replace the bicycle, bricks & mortar supermarkets would be replaced with etailers by 2005, barcodes would only be used by defence contractors and the auto industry, fewer than 15% of adults would ever use SMS, schoolbooks would be replaced with e-books by 2003 at the latest, email would only every be used by academics, everyone would have and diligently maintain a blog (despite the reality that most blogs have the lifespan of a fruit fly) and social network services such as Facebook would never take off.[49] The list of IT clangers goes on and on … and will do so in future.[50]

---

Locke [ed], *Thumb Culture: The Meaning of Mobile Phones for Society* (New Brunswick: Transaction 2005).

[47] The affordance reflects cost, user perceptions of privacy and perceptions of appropriateness. For example texting OMG, LOL, WTF, ROFL, ROFLMFAO and other acronyms validates parties to an exchange as being smart, subversive and in possession of codes that have somehow escaped both their grandparents and an occasional law professor. For a more detailed analysis see Naomi Baron, *Always On: Language in an Online and Mobile World* (Oxford: Oxford University Press 2008) and Richard Ling & Paul Pedersen [ed], *Mobile Communications: Re-Negotiation of the Social Sphere* (London: Springer 2003) or James Katz, *Magic in the Air: Mobile Communication and the Transformation of Social Life* (New Brunswick: Transaction 2006).

[48] Consistent with earlier comments, there has not been successful litigation by a person under 12 regarding perceived privacy breaches by a parent, not least because Australian law does not yet enshrine a broad right of privacy.

[49] For other examples see 'Forecasting' (2009) at www.caslon.com.au/digitalguide23.htm#clangers.

[50] For cautions regarding technological determinism see Steven Schnaars, *MegaMistakes: Forecasting and the Myth of Rapid Technological Change* (New York: Free Press 1988); Nik Brown & Mike

In thinking about technology's erosion/enhancement of privacy we should accordingly be agnostic.

That agnosticism involves questioning the authority of experts, or people who confuse self-esteem and a loud voice for expertise. It also involves recognition that journalists (like officials) on occasion are uninformed, are unequipped to question promotional literature from vendors and advocacy groups, or are simply quite happy to drink the digital koolade if that results in a tasty headline or a media release that demonstrates your government is responsive and digitally savvy.[51]

One basis for evaluating forecasts is economics.[52] Overall, new technologies – just like traditional mechanisms – offer substantial scope for eroding or enhancing the privacy and protection of minors. The promise of many of those technologies will remain unfulfilled because the dollars and cents do not stack up.

## Privacy Economics?

In the absence of regulatory constraints (ie restrictions under privacy, contract or other law on what you can/cannot do) institutional and consumer uptake of surveillance technology is a function of the balance between demand and cost.

In principle a range of surveillance technologies are, or shortly will be, available. They encompass 'solutions' such as automated monitoring of SMS; alerts that a prohibited site has been browsed; in-home (or in-creche) video surveillance than can be viewed via the web from the comfort of mum's office desk twenty kilometres away;[53] networked fingerprint readers in school libraries or tuckshops;[54] and geospatial tracking mechanisms based on mobile phones, bracelets or even implanted RFID tags (upmarket versions of the microchips used to uniquely identify cats, dogs and livestock and inevitably characterised by some chiliasts as 'the mark of the Beast').[55]

---

Michael, 'A sociology of expectations: Retrospecting prospects and prospecting retrospects', 15(1) *Technology Analysis and Strategic Management* (2003) 3-18; Edward Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences* (New York: Knopf 1996) and Alan Cooper, *The Inmates Are Running The Asylum* (Indianapolis: SAMS 1999).

[51] In opening the conference Noni Hazlehurst noted the media aphorism that 'if it bleeds, it leads'. In technology journalism in the mass media a corresponding aphorism is that if glitters – or has cute features such as talking paperclips and publication on Facebook of results from direct to consumer genetic testing – it leads.

[52] There is a striking paucity of scholarly writing about the economics of children and privacy, in contrast to the substantial literature on the economics of e-commerce and public security, typically reflecting a valorisation of commercial interests and public sector investment over concerns regarding human rights. Among introductions to privacy economics – traditionally characterised as information security economics – see L Jean Camp & Stephen Lewis [ed], *Economics of Information Security* (New York: Kluwer 2004); Andrew Odlyzko, 'Economics, Psychology and Sociology of Security', 2742 *Lecture Notes in Computer Science* (2003) 182; Richard Posner, 'The Economics of Privacy', 71(2) *American Economic Review* (1981) 405; Robert Hahn & Anne Layne-Farrar, 'The Law & Economics of Software Security', 30(1) *Harvard Journal of Law & Public Policy* (2006) 284; Alessandro Acquisti, 'From the Economics to the Behavioural Economics of Privacy', in Ajay Kumar & David Zhang [ed], *Ethics & Politics of Biometrics* (Berlin: Springer 2010) 23; George Stigler, 'An introduction to privacy in economics and politics', 9 *Journal of Legal Studies* (1980) 623; and Robert Anderson, 'Why Information Security is Hard: An Economic Perspective', *Proceedings of the 17th Annual Computer Security Applications Conference* (2001) 358.

[53] Vibeke Jørgensen, 'The apple of the eye: parents' use of webcams in a Danish Day Nursery', 2(2) *Surveillance & Society* (2004) 446.

[54] [UK] Information Commissioner's Office, 'The Use of Biometrics in Schools' (August 2008) at www.ico.gov.uk; and Terri Dowty, 'Overlooking Children: An Experiment With Consequences', 1(1) *Identity in the Information Society* (2008) 109.

[55] For an expression of anxieties about surveillance technologies as actual tools of Satan – a sceptic might argue that the Prince of Darkness does not need the gadgets – see Katherine Albrecht & Liz McIntyre, *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance* (New York: Nelson 2006). A corrective to visions of RFIDs as a harbinger of the 'End Times' see 'RFIDs'

As Robert Mayer comments, for example, global positioning systems –

> are perfect for tracking teenagers who spend lots of time talking on the phone, enjoy wearing jewellery and have few compunctions about sticking things through and into body parts.[56]

Investor uncertainty means that many of those technologies will not be deployed in Australia and overseas. The particular technology does work in the laboratory and might work in a real-world environment across a major city or the nation but potential backers are unpersuaded that there will be a significant return within the required timeframe (for example within the two to five year period used by most venture capital managers). Lessening of dot com euphoria over the past decade and the recent Global Financial Crisis mean that opportunities for small innovators are fewer. Large corporations such as Telstra have capital for infrastructure development, marketing and regulatory approval processes but are typically preoccupied with other concerns and likely to be risk averse.

Many technologies will instead not be sustained (will not go beyond small-scale pilots) because the 'nice idea' does not get sufficient traction in the market and does not attract support from a major telecommunications corporation, education department or other partner.

That is disconcerting for solution developers, enthusiasts, vendors and some regulators who are surprised by the divide between what people say they want in terms of privacy and what they are prepared to pay for. Perceptions of need change when dollars are required up front and where consumers are not locked in to a service through a long-term subscription, a lock-in that has the effect of building a reference population that encourages emulation by mid- to late-adopters as distinct from creatures of fashion who will try almost anything in 'beta' but move on as the current fad loses its newness.

## Desire, Curiosity, Need

Although there have not been comprehensive authoritative studies it appears that the market for child surveillance technologies is vendor driven, rather than responding to a profound need on the part of parents, guardians or third parties.

Put simply, consumers often say that they are greatly concerned about dangers and are committed to being 'conscientious' parents but in practice are not buying the products and are not using the products effectively if there is a purchase.[57]

That observation is counter-intuitive. It is however consistent with privacy practice in general.

Australian, UK and US adults for example typically say that they 'value' or 'greatly value' their privacy.[58] The same individuals, however, self-report that they have gifted information

---

(2009) at www.caslon.com.au/rfidprofile.htm; Kenneth Foster & Jan Jaeger, 'Ethical Implications of Implantable Radiofrequency Identification (RFID) Tags in Humans', 8(8) *American Journal of Bioethics* (2008) 44; and Rodney Ip, Katina Michael & M Michael, 'The Social Implications of Humancentric Chip Implants: A Scenario – Thy Chipdom Come, Thy Will Be Done' (Faculty of Informatics Paper 2008) (University of Wollongong).

[56] Robert Mayer, 'Technology, Families and Privacy: Can We Know Too Much About Our Loved Ones', 26(4) *Journal of Consumer Policy* (2003) 425.

[57] See for example the inconsistencies apparent in responses to the Microsoft 'For Safety's Sake' survey in Australia during 2010.

[58] See for example the studies at http://www.privacy.gov.au/aboutprivacy/attitudes and *Privacy in Diverse Victoria: Attitudes towards information privacy among selected non-English speaking background and Indigenous groups in Victoria* (Melbourne: Privacy Victoria 2002). For overseas points of reference see the discussion in David Lyon, Stephen Marmura, Pasha Peroff, *Location Technologies: Mobility, Surveillance and Privacy: A Report to the Office of the Privacy Commissioner of Canada* (The Surveillance Project, Department of Sociology, Queen's University 2005) and Chris Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies* (2010).

to marketers in return for a mere opportunity to win a prize. (Note that is the opportunity to *enter* a competition rather than to definitely receive a reward, a competition in which the chance of winning is slight and where restrictions on the marketer's use of that information are even slighter). They also endorse the disregard for privacy that is apparent in tabloid print/electronic journalism, with celebrities – or folk devils such as 'dole bludgers' – apparently being construed as having surrendered their privacy as the price for being in/famous.[59]

Overseas studies of parental monitoring of in-home internet use by their children (for example through scrutiny of browser histories or sporadic observation of what is 'on screen') tend to indicate that parents significantly over-report the frequency and effectiveness of that monitoring. Although parents express that they are 'concerned' or 'greatly concerned', they overstate the number of times that they have looked at what is going on.[60]

Similarly, advocacy groups and the mass media have claimed over the past decade that there was substantial parental demand for web content filtering solutions, characterised as protecting children from obscene or other web sites. The reality seems somewhat different, with industry sources reporting that few parents purchased the filtering software that was a mandatory offering by internet service providers under federal law.[61]

Consumers did not flock to providers that marketed their services as being 'safe', ie the ISP would relieve the parent of responsibility for filtering by excluding offensive content before it reached the home, in a local version of the national filtering regime that has been promoted by the Rudd and Howard Governments.[62]

Perceptions of need for child surveillance technologies reflect a push/pull cycle, with solution vendors claiming to consumers and third parties that there is a need, the mass media and regulators or other third parties such as education departments and child advocacy groups endorsing claims of threats properly addressed through surveillance solutions, and consumers responding to that construction of a need by purchasing the product/service.

One of the more disappointing aspects of Australian journalism is thus the willingness of journalists in the mass media (as distinct from some technical journals) to act as cheer squads in an echo chamber, uncritically embracing problematical claims by vendors or advocates and thereby encouraging both poor public policy making and consumption that addresses fictive problems.

Opportunism on the part of politicians, senior public servants and advocacy group representatives is equally disturbing and arguably more egregious, given that those figures typically speak with more authority and thus have a higher responsibility.

---

[59] We might usefully adopt the European model provided by judicial decisions in the *von Hannover* and *Mosley* cases ('F1 Boss Has Sick Nazi Orgy With 5 Hookers'), with law reform shaping community perceptions of rights and responsibilities. Do we *really* need to watch Caroline of Monaco collecting a carton of milk, the Formula 1 czar getting spanked by dominatrix Helga or NSW politician David Campbell leaving a gay sauna frequented by consenting adults? Cf *von Hannover v Germany* (2004) 40 EHRR 1; *Mosley v News Group Newspapers* [2008] EWHC 1777 and discussion in Andrew Kenyon & Megan Richardson [ed], *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge: Cambridge University Press 2006) or Barbara McDonald, 'Privacy, Paparazzi and Princesses', 50 *New York Law School Law Review* (2005) 205.

[60] See for example Larry Rosen, Nancy Cheever & Mark Carrier, 'The association of parenting style and child age with parental limit setting and adolescent MySpace Behavior', 29 *Journal of Applied Developmental Psychology* (2008), 459.

[61] Microsoft Australia's March 2010 'For Safety's Sake' report on a small scale survey in February 2010 for example reports that 49.45% are "completely confident" that "you know what your children are doing when they are on the internet", 62.44% do not "take precautions by running any parental control software", 64.84% have no "software on your computer that can monitor where your children go online and with whom they interact" (25.07% do not have any parental control software; 12.49% don't know), 61.64% allow children to "use the computer unsupervised at home" (albeit there's apparently no question differentiating between online and offline use).

[62] The failure of that software and services does *not* appear to be directly attributable to their problematical effectiveness, ie the tendency to exclude legitimate content but not exclude grossly offensive content.

## Subversion

One reason for caution in uncritical acceptance of claims by solution vendors and their collaborators is that technologies can often be readily subverted. Some technologies work nicely in the laboratory but – like Melbourne's controversial Myki ticketing system, the Victorian smart metering initiative and a succession of other bits of hi-tech bling such as the F-111 – do not quite seem to perform as promised in real world environments.

Subversion typically occurs because designers ignore the human aspect. Humans discover new ways to use technologies. Humans 'break the rules' or simply disregard designer and marketer expectations. Children experiment to discover the rules (and consequences for infringement), assert their independence, validate themselves in interactions with their peers or simply have fun.[63] They take risks because that provides an "emotional rush" that offsets the tedium of confinement.[64] They discover blind-spots, backdoors and patterns of inattention.[65]

It is not difficult to imagine, for example, minors subverting SMS-monitoring systems by texting from a friend or sibling's mobile. Similarly, if a parent/guardian tracks web browsing, that surveillance can be subverted by children escaping the parental gaze via use of a friend's personal computer or a browser-equipped mobile phone, or simply by tweaking a filter.[66] Some children will simply go offline, given that it is possible to have an emotionally satisfying life that doesn't involve electronic interaction.

Subversion also occurs because subversion is implicitly one of the values we encourage in children, although it is more conventionally characterised as exploration, initiative, being independent. Children assert their selfhood, their being as creatures related to but independent of their parents, by testing the rules – something that can be playful rather than disrespectful, might be uninformed in terms of risk assessment but is a key aspect of growing up to be a happy, well-adjusted adult.

A fundamental concern about mooted surveillance technologies is that they embody a mistrust that corrodes personhood and that they are an electronic substitute for the trust (and risk sharing) that we might see as fundamental to family life in 2010.[67]

---

[63] Shepherd et al (2006), op cit, 215 comments that –

> Negotiations around rules associated with ICT – particularly chat, email, and television – become anchor points for our participating parents to declare and fix their stand on important principles and issues, such as the work ethic, good health, violence and exploitation, bullying, feminism, and their own authority as parents; and this stand was reasserted day-by-day with each new television show, computer game, or web site. Similarly, ICT anchored our participating children's expressed position and principles in regard to their own sense of maturity and independence, and to their work ethic, health and safety, and values and morals. ICT thus provide a focus for what a parent is and does and should be, and what a child is and does and should be, and this focus runs thematically through the negotiations, in a transient and particularised way. The point is that rules and negotiations do not just circulate around the unchanging desirable and undesirable qualities of ICT, they circulate around the changing and particular qualities of particular ICT, and the desirable and undesirable qualities of parents and children.

[64] Stephen Lying, 'Edgework: A Social Psychological Analysis of Voluntary Risk Taking', 95(4) *American Journal of Sociology* (1990) 851.

[65] Jen Weiss, 'Scan This: Examining Student Resistance To School Surveillance', in Torin Monahan & Rodolfo Torres [ed], *Schools under Surveillance: Cultures of Control in Public Education* (New Brunswick: Rutgers University Press 2010) 213 and Andrew Hope, 'Seductions of Risk, Social Control and Resistance to School Surveillance', ibid 230.

[66] Andrew Hope, 'Risk Taking, Boundary Performance and Intentional School Internet 'Misuse'', 28(1) *Discourse: Studies in the Cultural Politics of Education* (2007) 87 and 'Panopticism, Play and the Resistance of Surveillance', 26(3) *British Journal of Sociology of Education* (2005) 359.

[67] Sonia Livingstone, 'Children's privacy online: experimenting with boundaries within and beyond the family', in Robert Kraut, Malcolm Brynin & Sara Kiesler [ed] *Computers, phones, and the internet: domesticating information technologies* (Oxford: Oxford University Press 2006) 145. See also Robert

We do not know how much subversion is taking place, for example the extent to which minors borrow phones as a matter of course on a casual basis – sharing is caring, even though today's 'bestest bestest friend' in the playground may be tomorrow's sworn enemy and today's relationship sours after sexting goes wrong – or with a considered intention to evade monitoring.[68]

The nature of childhood sociality means that any figures on the incidence of such subversion are speculative. Claims by some surveillance product vendors or child safety advocates should thus be treated with caution.

## Displacement

One reason for a realistic rather than vendor-driven or media-driven approach in assessing such claims is that many anxieties about risks faced by children (and more broadly about new media)[69] represent a displacement of substantive threats and appropriate responses.[70]

It is clear, as showcased by the noisier child protection advocates and politicians with an eye on the polls, that predators such as Dennis Ferguson do exist.[71] However, several generations of research and a grim parade of judgments in Australian courts demonstrates that most sexual offences against children involve people within a circle of trusted intimates – siblings, parents, uncles, cousins, members of blended families, the much-admired family clergyman – rather than the unshaven anonymous monster lurking in the darker regions of cyberspace.[72] We have moved on from stereotypes of white slavers or grubby men in macs loitering near schoolyards (and addressable through extraordinary legislation, offender registration and a cardboard coffin or two) but have replaced that image with one of the predator parked behind a modem and a Mac.[73] Parental child protection measures based on the image of 'the

---

Mayer, 'Technology, Families and Privacy: Can We Know Too Much About Our Loved Ones', 26(4) *Journal of Consumer Policy* (2003) 419.

[68] There are indications, albeit not confirmed with strong empirical research, that children and teens selectively share passwords rather than merely mobiles.

[69] Shepherd et al (2006), op cit, 220 thus reports that –

> Notwithstanding a number of positive perceptions of ICT as a domestic resource, our parents' attitudes to the relationship their children formed with ICTs is one characterized by nuance, ambiguity, and a distrustful anxiety. All of our participating parents expressed some concerns about free-to-air TV. Almost all Australian parents (92%) express some issue of concern in relation to the Internet, while at the same time almost all (99%) regard it as being of some value ... It may appear something of a paradox that while the dominant parental attitude is one of uneasiness and suspicion, their homes abound in these technologies. Yet parents are concerned about many things in relation to their children. In a sense, everything is of concern to parents, and one concern is not neatly distinguished from another. Rather, our conversations with parents suggest that a good deal of parenting is a process rather like dealing with a huge string ball of tangled concerns, each thread of which is knotted up with a whole number of others.

[70] Anthony Giddens, 'Risk and Responsibility', 62(1) *Modern Law Review* (1999) 1.

[71] Marianne James [ed], *Paedophilia, Policy & Prevention (AIC Research & Public Policy Series, 12)* (Canberra: Australian Institute of Criminology 1997). For a perspective on poll-driven responses see Georgina Wright, 'Paedophiles and Civil Liberties', 19(19) *Eureka Street* (September 2009).

[72] Edward Ingebretsen, *At Stake: Monsters and the Rhetoric of Fear in Public Culture* (Chicago: University of Chicago Press 2001); Anneke Meyer, *The Child at Risk: Paedophiles, Media Representations and Public Opinion* (Manchester: Manchester University Press 2007); and Malcolm Hill & Kay Tisdall, *Children and Society* (London: Longman 1997). For scepticism that challenges lazy assumptions regarding predation see Janis Wolak, David Finkelhor, Kimberley Mitchell & Michele Ybarra, 'Online 'Predators' and Their Victims', 63(1) *American Psychologist* (2008) 111.

[73] Philip Jenkins, *Moral Panic: Changing Concepts of the Child Molester in Modern America* (New Haven: Yale University Press 1998); Hugh Potter & Lyndy Potter, 'The Internet, Cyberporn and Sexual Exploitation of Children: Media Moral Panics and Urban Myths for Middle-class Parents?', 5(3) *Sexuality & Culture: An Interdisciplinary Quarterly* (2001) 31; Kristen Zogba, 'Spin Doctors and Moral Crusaders: The Moral Panic Behind Child Safety Legislation', 17(4) *Criminal Justice Studies* (2004) 385; and Leanne Franklin & John Cromby, 'There might be 10 paedophiles sitting in their front

other' may be simply ineffective. There is little point building a firewall around the five year old or 15 year old if the predator is sitting in the next room.

The flipside of displacement is an over-confidence in technologies, the belief (perhaps inevitable in a culture that valorises science without much sense of scientific principles and construes public good through a lens of economic growth based on relentless innovation) that silver bullet solutions are available off the shelf or about to emerge from the product development pipeline.[74]

If we are concerned about the well-being of our children we might most effectively rely on building relationships of trust, rather than building 'smart' networks or relying on legislation to deter monsters and provide remedies where harms have occurred. Law is a blunt instrument. It is an instrument with commercial values. Concern means seeing minors face to face rather than relying on an automated system for detection of dangerous SMS traffic or online grooming via MySpace; or simply delegating the responsibilities of parenting to K12 teachers (few of whom are paid anywhere near their worth, contrary to rhetoric such as 'children are our greatest asset') and the harried bureaucrats of the child welfare services.

Irrespective of potential challenges to the statement by one vendor that its product is "the only solution today", do you really want to "share in your son or daughter's daily life" through a "parenting tool" service that exhorts you to "schedule appointment reminders, create task lists and communicate about important issues, all from your personal … website"?[75] Is the quality of "sharing" an issue, even if its legality isn't contentious?

We might also acknowledge that a focus on particular harms and technological silver bullets may militate against action regarding other pervasive abuses, such as physical and emotional neglect.[76]

## Tensions

Respect for children as people – and care for them, as both vulnerable individuals and members of a vulnerable class – means that privacy involves tensions.

Those tensions are inescapable. They are inherent in our use of technologies to protect, or merely to manage, the children for whom we as parents, guardians or a society are responsible.[77] They necessitate choices when considering new surveillance technologies that can serve as mummy's digital helper, as electronic handcuffs or as both (depending on circumstances and where you are positioned in the privacy relationship).[78]

We might recognise those tensions in assessing comments such as the statement[79] by Deakin University law academic Mirko Bagaric that –

---

rooms: The 21st Century Monster', at www.inter-disciplinary.net/wp-content/uploads/2009/08/21st-century-monster-leanne-franklin.pdf.

[74] Gary Marx, 'The Engineering of Social Control: The Search for the Silver Bullet', in John Hagan & Ruth Peterson [ed], *Crime & Inequality* (Stanford: Stanford University Press 1991) 225 and Lucia Zedner, 'The Inescapable Insecurity of Security Technologies?', in Katja Aas, Helene Gundhus & Heidi Lomell [ed], *Technologies of InSecurity: The Surveillance of Everyday Life* (New York: Routledge-Cavendish 2009) 257.

[75] Those phrases are used by My Mobile Watchdog; similar statements are found on the site of analogous services.

[76] Adam Foster, 'Reframing Public Discourse on Child Abuse in Australia: Should child sexual abuse and child pornography in particular really be the number one priority in child abuse prevention?', 13(1) *NCPC Newsletter* (2005) 14. Foster was Executive Officer of the National Association for the Prevention of Child Abuse & Neglect (NAPCAN).

[77] The reference to 'society' is deliberate, given that some parents appear to construe children in terms of property rights ('she's my daughter and I can do with her what I want').

[78] For an international perspective see Jack Linchuan Qiu, 'The Wireless Leash: Mobile Messaging Service as a Means of Control', 1 *International Journal of Communication* (2007) 74.

[79] Mirko Bagaric, 'Privacy Is The Last Thing We Need', *The Age* 22 April 2007. Dr Bagaric is co-author of *Privacy Law in Australia* (Leichhardt: Federation Press 2005) and other works, including *Torture: When The Unthinkable Is Morally Permissible* (Albany: State University of New York Press

> privacy is a middle-class invention by people with nothing else to worry about. Normally they would have every right to live in their moral fog, but not when their confusion permeates the feeble minds of law-makers and puts the innocent at risk.
>
> The right to privacy is the adult equivalent of Santa Claus and unicorns. No one has yet been able to identify where the right to privacy comes from and why we need it. In fact, the right to privacy is destructive of our wellbeing. It prevents us attaining things that really matter, such as safety and security and makes us fear one another.
>
> A strong right to privacy is no more than a request for secrecy - refuge of the guilty, paranoid and misguided, none of whom should be heeded in sorting through the moral priorities of the community.[80]

We might also recognise those tensions in acknowledging that 'child' encompasses a range of capabilities and needs, not all of which are appropriately addressed by conceptualising minors as 'small, hairy adults', as devoid of rights or as always so vulnerable that notional rights can be overridden without hesitation in using electronic monitoring tools that parse the child's communication, social interaction or location.

Research suggests that although children (like many parents and policymakers) sometimes fail to correctly identify and act on risks, real or imagined, they *do* conceptualise themselves as having some autonomy and valuing their privacy.[81]

That valuation concerns –

- physical integrity (eg freedom from observation by siblings, parents or peers; disquiet about medical examination and reluctance on occasion to be hugged or kissed),
- spatial privacy (being given a personal physical space, even if that space is restricted to a box or drawer rather than a room, especially a room with a lock) and
- communicative privacy (being able to keep a diary, speak or write messages without close supervision by an authority figure and without unwanted observation by peers).[82]

It is reflected in the empirical research by Piaget, Winnicott and others over the past century which identifies the importance of autonomy for psychological well-being and capability among young and older children. It is also reflected in observations by Goffman about the

---

2007), the latter at odds with the argument in Elaine Scarry, *Rule of Law: Misrule of Men* (Cambridge: MIT Press 2010). Another expression of Bagaric's disquiet regarding privacy (and, apparently, with much Australian law) is evident in ABC Radio National, 'The Law Report: Criminals and Privacy' (28 March 2006) at www.abc.net.au/rn/lawreport/stories/2006/1601294.htm.

[80] For scepticism about the media claims of an overarching 'right to know', using words similar to Dr Bagaric, see David Salter, *The Media We Deserve* (Carlton: Melbourne University Press 2007) 40-41.

[81] See for example Ross Parke & Douglas Sawin, 'Children's Privacy in the Home: Developmental, Ecological and Child-Rearing Determinants', 11(1) *Environment and Behavior* (1979) 87; Maxine Wolfe & Robert Laufer, 'The Concept of Privacy in Childhood and Adolescence', in Stephen Margules [ed] *Privacy* (Stroudsburg: Dowden, Hutchinson & Ross 1974); James Youniss & Jacqueline Smollar, *Adolescent Relations with Mothers, Fathers & Friends* (Chicago: University of Chicago Press 1985); Sandra Petronio, 'Privacy Binds in Family Interactions: The Case of Parental Privacy Invasion', in William Cupach & Brian Spitzberg [ed] *The Dark Side of Interpersonal Communication* (Hillsdale: Lawrence Erlbaum 1994) 241-258; Gary Melton, 'Minors and Privacy: Are Legal and Psychological Concepts Compatible?', 62 *Nebraska Law Review* (1983) 455; Anna Fry & Frank Willis, 'Invasion of Personal Space as a function of the age of the invader', 21 *Psychological Record* (1971) 385; and Larry Nucci, Melanie Kilen & Judith Smetana, 'Autonomy and the personal: Negotiation and social reciprocity in adult-child social exchanges', 73 *New Directions for Child and Adolescent Development* (1996) 7. For a valuable conspectus of the literature see Alice Marwick, Diego Diaz & John Palfrey, *Youth, Privacy & Reputation* (Berkman Center Research Publication 2010-5) (2010).

[82] Those values embody the tensions inherent in privacy: while respecting a child's right not to be wantonly stripped, probed and displayed like a circus animal there would be times when we recognise autonomy rather than full independence and legitimately override a child's modesty or fears in order to provide invasive medical treatment.

importance of spaces where people can relax, take off the masks required by particular relationships and cease to 'perform'.[83] Childhood, for many Australians, is a state in which they are always on stage, always with an audience. There are times when we need to bring down the theatre curtain and not take the cameras backstage.

In dealing with children we should respect rather than dismiss those values, because children are people – in the same way that Australian law and institutions have come to recognise women, NESB migrants, Indigenous Australians and members of the LGBTIQ communities as people.

Respect is also important because effective protection of children from dangers is founded on both an ability to communicate with parents/guardians (ie trust) and the resilience associated with some degree of self-help. Imprisoning children behind a digital shield, denying autonomy or relying on surveillance technologies to "share in your son or daughter's daily life" may be as damaging as exposure to substantive dangers.[84]

## GOING DIGITAL?

The past twenty years have seen celebrations of 'going digital', with nations ranking themselves using measures such as broadband penetration and pundits (echoed by the mass media) expressing concern that families would miss out on the digital cornucopia because parents lacked technology literacy or were unable to provide their children with the requisite connectivity. Schools (and conferences) were assessed on the incidence of digital bling, with easy counts of the number of computers per capita or the availability of data projector for the standard 'death by powerpoint' supplanting more challenging assessments of quality – challenging because subjective, difficult to measure and even threatening if the auditor questions a focus on beefing up the broadband rather than building the library.

It is therefore unsurprising that parents, businesses, educational institutions and governments are turning towards digital technologies that address substantive or imagined threats facing children in Australia and overseas, including grooming by adults (or by teens), cyberbullying, exposure to adult content, naïve provision of personal data on social network services such as Facebook,[85] or simply getting lost in a major shopping centre.

Claims made by some vendors are problematical and, as noted above, reception by the mass media is often uncritical. That is important because, faced by perceived dangers, parents (and politicians facing an election) often appear to err on the side of caution or simply suspend disbelief. What you read about some products/services thus will not necessarily be much help. Parts of the promotional literature will strike some readers as too *Brave New World*, visions that – like the flying car, robot butler, personal jet-pack, atomic-powered lawnmower or internet fridge – will never come to pass. We should, however, look beyond the hyperbole, given that the uptake of technologies such as mobile phones, email and social network services demonstrates that some innovations can quickly become a ubiquitous and unexceptional part of daily life for most Australians despite the 'it will never take off' dismissals voiced by technology analysts and social commentators.

The following paragraphs accordingly highlight some child surveillance technologies that are currently available in Australia, that might become available in the near future if they are perceived to be commercially viable, or that are destined to remain glints in the eyes of enthusiasts.

They are located within the same environment of parental anxiety and commercial opportunism that has seen development in Australia and overseas of services that encourage

---

[83] Erving Goffman, *The Presentation of Self In Everyday Life* (London: Allen Lane 1969) 97. Childhood as a domain of pervasive observation, and thus denial of full personhood, resembles the experience of inmates of the 'total institutions' discussed by Goffman and by Jeffrey Reiman, 'Privacy, Intimacy and Personhood', 6(1) *Philosophy and Public Affairs* (1976) 26.

[84] Valerie Steeves & Cheryl Webster, 'Closing the Barn Door: The Effect of Parental Supervision on Canadian Children's Online Privacy', 28(1) *Bulletin of Science, Technology & Society* (2008) 4.

[85] Zaineb De Souza & Geoffrey Dick, 'Disclosure of information by children in social networking – Not just a case of "you show me yours and I'll show you mine', 29 *International Journal of Information Management* (2009) 255.

parents/guardians to test children or their belongings and surroundings for illicit drug use, exemplified by one service provider's incitement to start a "family drug policy" –

> Start when they are 11 or 12. Say that part of the family drug policy is that there is going to be random drug testing. That doesn't mean I don't love you and I don't trust you. It means that the thing is too serious to take a chance.[86]

Sending little Johnny's urine or little Joanna's hair off for testing may, on occasion, be appropriate but – as with digital technologies that allow parents, schools and others to track what the children are doing, where they have been and with whom they associate – we might be cautious about extreme remedies, irrespective of whether those tools are legal.

## Mummy's Little Helper

The premise of most surveillance technologies marketed to parents and guardians is the extension of the parental gaze, ie watching children when the adult is not present or is otherwise occupied.

That extension relates to content, activity and location.

It may be involve restriction of some communication or activity, for example –

- blocking the child from viewing particular digital content via a mobile phone, personal computer or other device
- stopping the child from using particular communication tools (eg entering an online chat room)
- stopping the child from sending messages to 'blacklisted' recipients or using a mobile phone to communicate with anyone except

The expectation is that restriction will be outright or instead involve alerting the parent/guardian, who can then modify the child's behaviour, ideally through face to face guidance rather than discipline via SMS, IM or email. That alerting might be on a real-time or retrospective basis.

The extension may instead be concerned with where the child *is* (or has been) rather than the specifics of what the child is doing.

The following pages concentrate on digital surveillance of children. However, given preceding comments about technological neutrality and management, it is important to note that the same modes of surveillance are applicable to teenagers, seniors, partners, employees and alleged terrorists or paedophiles. Our acceptance of or revulsion from surveillance tools such as the 'nannycam' (currently being used to monitor small children, amorous teenagers, babysitters, domestic cleaners and stay-at-home seniors) reflects personal or broader cultural values.[87] The tools are indifferent to what is being surveilled and cannot be left to manage themselves.[88]

---

[86] David Newman & Elizabeth Grauerholz, *Sociology of Families* 2 ed (Thousand Oaks: Sage/Pine Forge 2002), 49 notes delights such as the "Parents Alert Home Drug Test Service" which provide testing of a minor's urine, hair or belongings for "up to thirty illicit drugs". In the US the same enterprises are often marketing paternity testing, leveraging uncritical media reporting of claims that around 30% of offspring are not the biological children of their putative father [for which see Michael Gilding, 'Rampant Misattributed Paternity: The Creation of an Urban Myth', 13(2) *People & Place* (2005) 1]. Technology may be neutral but the anxieties around it are not.

[87] Gary Gumpert & Susan Drucker, 'Public Boundaries: Privacy and Surveillance in a technological world', 49(2) *Communication Quarterly* (2001) 115; Renee Smith, 'Can the use of 'Nanny Cams' be morally justified?', 9(24) *Think* (2010) 91; Margaret Nelson, 'I Saw Your Nanny: Gossip and Shame in the Surveillance of Child Care', in Margaret Nelson & Anita Garey [ed], *Who's Watching: Daily Practices of Surveillance Among Contemporary Families* (Nashville: Vanderbilt University Press 2009) 109; and Cindi Katz, 'Me and My Monkey: What's Hiding in the Security State', in Rachel Pain & Susan Smith [ed], *Fear: Critical Geopolitics & Everyday Life* (Aldershot: Ashgate 2008) 59.

[88] That phrasing is of course a misnomer, as tools lack personality and agency. Although we tend to personalise phones, guns, cars, personal computers and other tools (or creatures such as the family pet

## Geoslavery or liberation?

How do we construe the world, in particular dangers and opportunities faced by minors? Giddens argues that contemporary communities read their existence in terms of risk.[89] An uncertain grasp of statistics and poor research/analysis skills (unsurprising in an era where Wikipedia has replaced the *Sun-Herald* or *Daily Telegraph* as the repository of wisdom), exacerbated by opportunistic scaremongering on the part of politicians[90] and uncritical reporting in the mass media, means that many people appear to construe public space as necessarily dangerous. A man's home is his family's castle and the monsters howl at the gate.[91]

An implication is that children can, indeed must, be protected from those monsters by being tracked through public space until they return to the safety of the domestic residence, a residence in which, according to popular myth, dangers always come from outside (in the form for example of kidnappers, home invaders or groomers prowling the *Mad Max* territory known as cyberspace). Tracking both offers a functional tool and a magic talisman, with some parents/guardians presumably assuming that the mere possession of a GPS device – often embodied in a restricted-function child-friendly (or child-safe) phone such as the Firefly or Mamarino – will keep the monsters away. Buy the product and your child will be safe.

Critics, on the other hand, have denounced tracking of minors as an expression of 'geoslavery',[92] in which individuals are denied personhood by being reduced to digits traversing the virtual spaces found in Google Maps and similar geospatial services[93] or are denied autonomy through potential supervision whenever those people are mobile.[94]

How are minors being tracked?

Australia is currently experiencing a normalisation of spatial surveillance via 3G mobile phones, with consumer adoption of services such as Google Latitude[95] and the development of geosocial network services[96] that alert participants to the proximity of a current/potential contact (for example that a potential date is in the same neighbourhood or that a friend is at a nearby café).[97] Those services are predicated on location identification within a network (eg proximity to a particular mobile phone tower) and/or GPS capability (ie determination of position through reference to signals from global positioning system satellites.

Child surveillance service providers are accordingly marketing comfort in the form of phones that report, via the service provider, on the child's location. Give your child the phone, pay the subscription fee and you can then go online to observe the phone's movement across the landscape in real-time or on a retrospective basis.

---

and commercial livestock) we cannot rely on 'them' to manage 'themselves' and thereby relieve the user of responsibility.

[89] Giddens (1999), op cit, 1.

[90] Zogba (2004), op cit and Wright (2009), op cit.

[91] Ingebretsen (2001), op cit, and Wolak et al (2008), op cit.

[92] William Herbert, 'No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery', 22 *I/S: A Journal of Law & Policy* (2006) 409.

[93] Mark Monmonier, 'Geolocation and Locational Privacy: The 'Inside' Story on Geospatial Tracking', in Katherine Strandburg & Daniela Raicu [ed] *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Berlin: Springer 2006) 75; and Lyon et al (2005) op cit.

[94] Trine Fotel & Thyra Thomsen, 'The Surveillance of Children's Mobility', 1(4) *Surveillance & Society* (2004) 535.

[95] www.google.com/latitude

[96] Patrick Heneise, *I – The Digital Me: Digital Communication and Identity Development in Mobile Geosocial Networks* (Hochschule Furtwangen University dissertation, 1 March 2009); and Steven Strachan & Roderick Murray-Smith, 'Nonvisual Distal Tracking of Mobile Remote Agents in Geosocial Interaction' in Tanzeem Choudhury, Aaron Quigley, Thomas Strang & Koji Suginuma [ed], *Location and Context Awareness, 4th International Symposium* (Berlin: Springer 2009) 88.

[97] US geospatial 'friending' services include grindr.com, foursquare.com and loopt.com.

Overseas some providers are offering geospatial quarantining facilities that extend the service's functionality. The adult paying for the service can thus arrange to receive an SMS alert if the bearer of the phone moves outside a particular area or enters what the parent (or helpful service provider) has determined as a prohibited zone. That virtual 'no go' space might be a precinct such as the central business district (haunted by molesters and other monsters of the urban imagination) or merely the vicinity of a prohibited schoolmate, boyfriend or non-custodial parent.

Tracking across urban spaces or within a more confined domain such as a school campus, a major shopping centre or the family quarter acre block does not require a mobile phone. We are thus seeing exploration in Australia of overseas developments that involve digital bracelets, watches and even 'tattletale' stuffed animals or schoolbags that use the same positioning technology to identify a bearer's location and convey that information to another party.

Westfield, Australia's dominant shopping centre operator, has trialled removable Kidspotter bracelets to allay parental concerns that minors will get misplaced among the acres of bling and other consumer goodies.[98] The same tool is in use in UK and Danish theme-parks.[99]

In the US and Japan there has been marketing of watches and bracelets that serve as positioning devices and that are promoted as anti-abduction tools, with a remote alarm going off if there is an attempt to remove the device or if the wearer moves outside a specified zone.[100]

Lok8u ('locate you') thus claims that –

> Unlike other locator products, nu·m8 is a child's digital watch that cannot be removed or deactivated without your knowledge. If this should happen an instant alert is sent straight to your phone and/or email with your child's location. No other child locator in the world can match this. Another great feature of nu·m8 is the ability to set up a virtual fence as a 'safe zone'. If your child steps outside this zone you'll be notified.[101]

---

[98] A cynic might speculate that the operator presumably has some potential to mine the electronic breadcrumbs dropped by the future consumers as they wander through the malls and thereby enhance commercial layouts. As noted above, technologies can serve as both swords and shields. Charles Miranda, 'No more shopping terror of lost kids at Westfield shopping centres', *Courier Mail* (5 January 2009) quotes Kidspotter's co-founder as explaining that "Kidspotter reduces the anxiety for parents and children by significantly reducing the time elapsed between the child going missing and being re-united." Miranda indicates that –

> Parents can rent a tag about the size of a thick credit card when they enter the shopping centre and attach it to their child's wrist. They type a security number on their mobile phone which is entered on to the shopping centre's database. If they become separated from their child, the parents can call the security desk which can instantly tell them the location of the tag and the missing child. The device was developed in Legoland in Denmark in 2004 and is used by theme parks across Europe. Only now has it been picked up by Westfield. There have already been alerts and in all cases, the children have been found within 15 seconds to three minutes.

[99] Roisin Burke, 'Hi-tech visionaries are inventing the coolest stuff in a lab near you', *Irish Independent* (8 February 2009) in gee whiz mode those explains "Kidspotter is a device that aims to actually enhance children's freedom to roam rather than restrict it … there is also a help button that the child can press in an emergency and an alarm that will signal if a child wanders beyond a certain area". For use at Legoland in Denmark see James Roh, Anand Kunnathur & Monideepa Tarafdar, 'Classification of RFID Adoption: An expected benefits approach', 46(6) *Information & Management* (2009) 360 and Henrik Moen, *A Study of Wi-Fi RFID Tags in Citywide Wireless Networks* (MSc dissertation, Norwegian University of Science & Technology 2007).

[100] For the Japanese i-safety system (a wearable tag for children) see Claire Swedberg, 'RFID Watches Over School Kids in Japan', *RFID Journal* January 2005, 1.

[101] The Australian distributor of the 'new mate' was quoted in Leesha McKenny, 'Watch out children: Big Mother is watching', *Sydney Morning Herald* 11 January 2009 as commenting that "It helps with working parents … They could just jump on the computer at a quarter past three just to see that the kids got home, or are they on the bus when they said they'll be, because the device updates every minute or two minutes."

Children, like adults, are known to lend, lose, damage or destroy mobile phones. It is not hard to envisage children illicitly removing surveillance bracelets and watches or simply forgetting to retain a tattletale rucksack or teddy-bear, particularly if that device is associated with criticism or punishment. Some enthusiasts have accordingly promoted the idea of putting the tracking device within the child rather than in the child's pocket. [102]

Subdermal implants – essentially placing a very small tag under the skin of a person, in much the same way that many family pets are now uniquely identified – have attracted more media coverage than commercial success. Arguably they represent an answer in search of a question, despite proposals for identification and/or tracking of officials (eg adoption by some Mexican narco police), military personnel, ambulatory seniors (with alarms for example set to ring when a dementia patent wanders away from an aged care facility), sex offenders, juvenile offenders sentenced to home detention and of course children.[103]

Scott McNealy, otherwise famous for advice[104] that "your privacy is gone … so get over it" (no unicorns there, despite his corporation's express commitment to respecting customer privacy) is reported as commenting in 2000 that –

> If I could embed a locator chip in my child right now, I know that I would do that. Some people call that Big Brother; I call it being a father.[105]

Is that geoslavery? Liberation of the child (or merely the parent) from fear and risk? People construe parenthood and the rights or capacities of minors in different ways, influenced by circumstances and by philosophical or legal positions. Would you tag a minor, a loved one whose second childhood involves a regrettable tendency to wander,[106] or even yourself (no need, for example, to remember the PIN if the perimeter control sensor or billing system 'reads' a chip that has been injected into your arm)?[107] You just need to trust that the information will not be misused.

---

[102] Herbert (2006), op cit, 438; Kevin Warwick, 'Cyborg Identity' in David Birch [ed] *Digital Identity Management: Perspectives on the Technological, Business and Social Implications* (Aldershot: Gower 2007) 227; and Katina Michael, M Michael & Rodney Ip, 'Microchip Implants for Humans as Unique Identifiers: a Case Study on VeriChip' (Faculty of Informatics Paper, 2008) (University of Wollongong).

[103] For an example of promotion of the VeriKid tool see 'Solusat, Exclusive Distributor of VeriChip for Mexico, Signs Cooperation Agreement with Mexico's National Foundation for the Investigation of Lost and Kidnapped Children' (Business Wire, 1 October 2003). "It is expected that the VeriKid application will soon become available in other countries, including the United States, after its introduction in Mexico … Solusat will work with the National Foundation to develop a program for the distribution of VeriChip scanners to police stations, hospitals and other strategic locations to help with the emergency child identification program". Despite excitement about rolling out VeriKid to "supermarkets, airports, bus stations and other entities", tagging minors with RFID implants has not taken the world by storm. See however Maya Gadzheva, 'Getting Chipped: To Ban or Not to Ban', 16(3) *Information & Communications Technology Law* (2007) 217.

[104] Polly Sprenger, 'Sun on Privacy: 'Get Over It'', 7(1) *Wired* (January 2009).

[105] Robert Mayer, 'Technology, Families and Privacy: Can We Know Too Much About Our Loved Ones', 26(4) *Journal of Consumer Policy* (2003) 427. Mayer at 428 notes the disadvantages of implants, quoting a commentator's query –

> Will there be a 'taking out' party when the child reaches 18? What happens if the child leaves home or the parents die before then? How many parents will say "Now, dear, as long as I'm paying the bills you're going to keep that chip in your arm"?

[106] As an illustration of differing values see Ruth Landau, Shirli Werner, Gail Auslander, Noam Shoval & Jeremia Heinik, 'Attitudes of Family and Professional Care-Givers towards the use of GPS for Tracking Patients with Dementia: An Exploratory Study', 39(4) *British Journal of Social Work* (2009) 670.

[107] Antony Young, *Accountants' Acceptance of a Cashless Monetary System Using an Implantable Chip* (PhD dissertation, RMIT 2007) and Katina Michael & M Michael, 'The Diffusion of RFID Implants for Access Control and ePayments: A Case Study of Baja Beach Club in Barcelona' (2010) go a stage further, exploring use of subdermal RFID tags as verification mechanisms for electronic payment systems in financial institutions and resorts.

## Surf's Up

Debate in Australia about online content regulation over the past decade has been bedevilled by disagreement about the efficacy and appropriateness of content filtering, ie use of black-lists, white-lists or 'on the fly' content evaluation to block access by minors or others (eg employees or customers) to websites, images and services that are deemed to be offensive or merely high-risk.

That disagreement has been characterised with a shrill polemic that reinforces coalitions of the uncritical and provides soundbites for hungry journalists but inhibits understanding of principles and practices. It has also been characterised by uninformed, opportunistic or disingenuous statements from politicians and regulators.

The shouting inhibits a nuanced understanding of online dangers, responsibilities and remedies. Such an understanding is important in assessing claims by some solution vendors regarding surveillance and hence supervision of what minors see, say and do online – including via personal computers and mobile phones – and who those children encounter while visiting cyberspace. In essence those vendors market themselves as agents for parents/guardians, providing both comfort and tools that allow adults to watch what the kids are up to rather than tracking their mobility.

SoftEyes for example promotes its product as a tool to –

> see everything your kids see … you too will share in the peace of mind of seeing everything your kids see.

CyberSieve similarly –

> gives you the ability to control and monitor your child's use of the Internet, irrespective of where you are: in the neighbouring room, at work, even on vacation, thus enabling you to protect your child from the dangers of the Internet.

Competitor PC Tattletale urges you to "Take control of your child's online experiences and keep them safe", promising to –

> give you valuable insight into your child's behavior online, and the peace of mind to know exactly where they are surfing online & what kind of content they are trying to access. If not, return it for a full refund.

Are those services legal? The child's consent is not required, given that legally the consent is regarded as meaningless. The parent/guardian can subscribe to the service in the child's stead, with a contract between the service provider and the adult. Five and ten year olds do not get to cut their own deals; contract trumps privacy law … and parents presumably hope that the provider is not mining the data and is meeting its obligations under its terms & conditions. That hope might be misplaced, given the opacity of some T&C and acknowledgement by some major corporations that in the past they have breached both ethical and legal obligations.

Other vendors offer a record of SMS, ie surveillance of messages from mobile phones rather than just what appears on the desktop. Those digital helpers can be set to alert a parent/guardian when a particular phrase appears, a facility that might of course be subverted by parties to an exchange of messages using a code.[108]

Again, the contract is between mum or dad and the service provider: minors haven't successfully litigated against parents listening to their phone calls and there is little reason to believe that they would enjoy greater success in launching action over surveillance of what was texted on a mobile. Subscription does not breach covert surveillance law because the surveillance is not covert, ie monitoring has been solicited by the parent.

---

[108] One acquaintance was bemused to discover that his teenage daughter's enthusiasm for "doing the Discovery Channel" involved a particular form of gymnastics with her boyfriend in front of the latter's camera rather than contemplation of cute meerkats, pandas and gazelles.)

US service Net Nanny Mobile, which offers filtering of content on mobile phones, access to SMS and other content, and 'alert' features, accordingly asks "Is Net Nanny Spyware" and answers that –

> Emphatically NO. Net Nanny is for parents who want to keep their kids safe. Net Nanny is Mobile is not stealthy, and is not hidden on the phone.

Preceding pages of this paper argued that the privacy of children embodies an inescapable tension. Reading over the child's shoulder, with or without their knowledge (and with or without their consent) is arguably appropriate in situations of high risk. We might want however to be wary of eroding trust, of overestimating dangers and of imprisoning children with electronic handcuffs.

A better response to many threats might be to encourage the child to seek guidance where that minor is uncertain or perceives danger.

A corollary is to enhance the digital literacy of both parents and children, given that as noted above not all are 'digital natives', some degree of risk-taking is inevitable and no software solution or network management law will make all the dangers go away. If you want total freedom from online danger the only way to ensure that safety is to go offline, a drastic remedy that will be subverted by many children (who will for example covertly go online at the homes of their peers) and that imprisons the minor in an offline ghetto that shapes the child's character and opportunities by characterising 'online' as the domain of terror.

Overall it might be better to build relationships and resilience rather than build firewalls and the bankrolls of surveillance service providers.

## Who watches the watchers?

We have become accustomed, even inured, to incidents of privacy bad practice – a major data leak here,[109] gawking at airport bodyscan displays there, spyware arriving with hot snaps of Lady Gaga or purported video of the adorable Mr Shuffles at Taronga Zoo or merely what claims to be yet another update for yet another bug in software from Redmond. Among educators this year is likely to be recalled for a US school district's ineptness in protecting laptops issued to K12 students.

The road to privacy hell is paved with good intentions or no imagination, so it is unsurprising that the Lower Merion School District in the US sought to protect its precious laptops – community assets, after all – with what one colleague characterises as 'ET phone home!' software, designed to allow the school network administrator to identify the device if it strayed and was then used by the thief or finder to go online.[110]

The devices were equipped with an onboard camera, handy for the telepresence touted as the next big thing in e-learning. Unfortunately, the cameras could be activated remotely … and indeed were, by the network administrators, capturing a mere 56,000 images (allegedly including those of nude teens and of a parent or two) in what the District administrators later

---

[109] For indications of the scale and severity see the discussion in 'Consumer Data Losses' at www.caslon.com.au/datalossnote.htm.

[110] The NSW Education Department, in promoting its distribution of 130,000 laptops by mid-2010 (NSW Government Media Release, '2010 Student Laptop Rollout' 16 March 2010), notes that –

> The laptops will be remotely monitored and managed wherever they are. What's more, a stolen laptop can be disabled and the thieves tracked and prosecuted. These safety measures protect your child by removing any incentive for theft.

See the description of 'The Digital Education Revolution in NSW' [2009] at www.schools.nsw.edu.au/gotoschool/highschool/dernsw/thelaptop.php. The Department takes its role as a minder of children and parents seriously, going on to indicate under 'Signing the charter' that –

> Before students take their new laptops home, they'll be asked to sign the *Laptop User Charter*. This is an agreement that they have read and understood their responsibilities. The charter must also be signed by parents or carers. The charter includes a commitment to take the laptop home each day and bring it back to school the next day fully charged.

acknowledged as "overzealous and questionable use of technology … without any apparent regard for privacy considerations".[111]

The US incident is outrageous and, as far as we know, exceptional.[112] It has attracted more attention than a succession of 'nanny-cam' incidents, in which anxious parents or grandparents have covertly used webcams to detect misbehaviour by childminders, along with the occasional impropriety by a cheating spouse or disobedient elder child.

That lack of outrage is arguably because of dichotomies in the way that we conceptualise privacy and conceptualise risk.

A school (or its hired-gun IT operative, who may or may not have satisfied 'working with minors' vetting) surreptitiously watching parents is appalling, given that *we* are innocent. It is unacceptable that we should be surveilled, or that our virtue should be in question.

Covert surveillance of nannies, babysitters and relatives, on the other hand, seems to be accepted by many people as somewhat regrettable but ultimately justified because childminders – unlike mum and dad – are dangerous. In a culture of fear childminders are dangerous, monsters who may emerge from under the bed and may get into the bed. They are the 'other' from which we need to be protected, even if the grim statistics suggest that most assaults on small children involve intimates rather than itinerant hired help.

Rightly or wrongly, children like social network services such as MySpace and Facebook or online venues such as Club Penguin. [113] Arguably most children face less danger from online grooming or exposure to offensive content[114] and more danger from 'Big Sister', the corporations that operate the online social spaces and that mine data so obligingly provided by participants in those fora.

That mining is undertaken by and on behalf of government and commercial interests; we cannot rely on Mr Zuckerberg and his peers to patrol their venues on behalf of parents and – arguably – on behalf of children.

Questions of trust and surveillance are relevant in considering Facebook's ongoing notoriety regarding what might generously be characterised as a fluid privacy policy.[115] Privacy International cogently questioned Facebook's stance, commenting that –

> Facebook operates on a business model that requires it to monetise the data harvested from customers. That means ensuring that the maximum flow of

[111] Associated Press, 'Report: No Spying in Pa. School Laptops Case', *New York Times* 3 May 2010); *Blake J Robbins v. Lower Merion School District*, US District Court for the Eastern District of Pennsylvania (2010) and documents at www.lmsd.org/sections/laptops/, notably the 72 page 'Report of Independent Investigation' by Ballard Spahr.

[112] Reference to 'as far as we know' is deliberate. It is quite conceivable that some corporate (and institutional) laptops are being remotely activated by bored or malicious network administrators or third parties; we will not know until such misbehaviour is detected and publicised, in contrast to incidents where detection does not occur or where the matter is hushed up behind closed doors. The author has sighted images of a laptop thief made remotely by the laptop's owner when the thief incautiously went online. That skillset is not common but equally is not a fantasy from a Tom Cruise *Mission Impossible* video.

[113] Danah Boyd, 'Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life', in David Buckingham [ed] *Youth*, *Identity, and Digital Media* (Cambridge: MIT Press 2008) 119.

[114] Claims about a profound commitment to sheltering innocent minds from bedroom athletics seem questionable when many parents are complaisant in child access to violence on DVD and broadcast/cable television

[115] Kurt Opsahl, 'Facebook's Eroding Privacy Policy: A Timeline', Electronic Frontier Foundation (2010), at www.eff.org/deeplinks/2010/04/facebook-timeline/ and Danah Boyd, 'Facebook's privacy trainwreck: Exposure, invasion, and social convergence, 14(1) *The International Journal of Research into Media Technologies* (2008) 13.

> information is achieved. Changing the settings will marginally affect that business model, but for the vast majority of Facebook users, nothing has changed.[116]

Some minors subvert expectations about surveillance, in the same way that at least one grizzled male academic deals with data-mining using an online persona of a 99 year old Afro-American millionaire who is resident in Antarctica. Breaking the rules is encouraged when rule-makers are disingenuous. The *New York Times* for example recently noted[117] that US teens are responding to corporate profiling by adopting pseudonyms –

> For high school students concerned with college acceptance, Facebook presents a challenge. It encourages making public every thought and every photo, an opportunity for posturing and bravado nearly irresistible to teenagers. But this impulse for display clashes with the need to appear circumspect and presentable to college admissions agents, who some high school guidance counselors have warned are likely vetting applicants by trolling the Web. …
>
> Charlotte Kaye, who went to the Brearley School in Manhattan, did not take any chances. To avoid detection, Ms. Kaye, now a freshman at Colorado College in Colorado Springs, said she and others began changing their names on Facebook beginning in their junior year of high school. New spellings are standard: Amy is now Aim E, and Ms. Kaye became Charlotte K. A nickname will also do. At the Ramaz School in Manhattan, Amanda Uziel changed her Facebook name to Uzi Shmuzi. Puns and wordplay are held in higher esteem.

In practice, however, use of the social graph – identifying people through reference to their associates – means that such pseudonyms will often be ineffective and service operators or their partners will be able to readily strip away the masks.[118]

In thinking about the protection of children we might move beyond anxieties about individual predators and contemplate whether we need both significantly strengthened privacy legislation at the national and state/territory levels (a coherent and principle-based body of statute law rather than the current ad hoc regulatory bric a brac that discourages both enforcement and establishment of a 'privacy consciousness' among the community at large), in accord with recommendations by the Australian Law Reform Commission and the provincial law reform agencies.

We might further think about encouraging a more activist approach on the part of privacy agencies, on the basis that their traditional 'softly softly' negotiation and co-regulatory approach is ineffective in dealing with abuses by individuals, government agencies and private sector bodies.

Finally we might think about whether we participate in particular online fora and endorse the practices of traditional media organisations.[119]

In teaching Law to journalism students the author of this paper has thus responded to undergraduate laments about privacy abuses on the part of tabloid newspapers and tabloid current affairs television by noting that there is *no* obligation to feed the beast. If you are unhappy with the journalism, deny it your eyeballs.

---

[116] Privacy International, 'Facebook announcement: a promising start but mainly a red herring' (News, 26 May 2010) at www.privacyinternational.org.

[117] Sarah Maslin Nir, 'An Online Alias Keeps Colleges Off Their Trail', *New York Times* 23 April 2010

[118] See for example Joseph Bonneau, Jonathan Anderson, Ross Anderson & Frank Stajano, 'Eight Friends Are Enough: Social Graph Approximation via Public Listings', *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems* (2009) 13; Arvind Narayan & Vitaly Shmatikov, 'De-anonymizing Social Networks', *30th IEEE Symposium on Security and Privacy* (2009) and Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (University of Colorado Law Legal Studies Research Paper 9-12, 2009).

[119] Rachel Finn & Michael McCahill, 'Representing the Surveilled: Media Representation and Political Discourse in Three UK Newspapers', 60th Political Studies Association Annual Conference, Edinburgh, 2010)

## WHERE THE WILD THINGS ARE

### Urban panopticism, children and the synoptic sort

A recent article by this paper's author and Margalit Levin of Melbourne University traversed questions about privacy in urban environments. Those environments are where people navigate through cascades of closed circuit television networks (public and private), city-wide ticketing systems, automated numberplate recognition systems and wireless vehicle tag readers.[120] Some of the people traversing the spaces are children. Much of that urban surveillance is justified on the basis the cameras and other sensors will enable public/private sector entities to find lost children, discourage misbehaviour by children or deter offences against children.

Arguably some parents justify their use of digital surveillance tools on the basis that surveillance is normal. Normal is what the Victoria Police, Myer, Woolworths, Starbucks, the Education Department, NAB and the operators of the metropolitan rail/tram networks do. The people who own those cameras – which may or not be working and may or may not be viewed by a human, given that many CCTV installations are a form of street theatre rather than a functional surveillance tool – embody social values regarding the 'soft cage' of social discipline. They practice what parents may regard as a model – the Big Mother model – for watching their children, in which digital technologies have a magical aspect and the watched are denied full personhood through treatment as data subjects rather than as individuals with personal identity and agency.[121]

It is clear from the presentation by Wilson, Rose & Colvin at *Watch This Space* that some minors are aware of being publicly by Big Mother. As in an any relationship with a parent, the surveilled children express a mix of emotions – resentment, fear, acceptance – that reflect attitudes to authority (independent of action/inaction by the authority figure), perceptions that surveillance is punitive and perceptions that urban panopticism on occasion potentially protects them from street crime or facilitates intervention by ambulance services.

If we are all children of the state – and complicit[122] in a culture of urban synopticism[123] – we should appreciate that urban surveillance, like the surveillance within individual families, can be both beneficial and negative, ignored, subverted, ineffective or punitive.

### Canaries down digital coalmines?

In the Age of Steam, when industrial infanticide was an acceptable cost of production, miners famously went underground in the company of canaries – feathered early-warning devices whose demise would signal that the air quality was insufficient to sustain a human.[124] (Rats, ferrets and fox terriers posed management problems; popular culture to the contrary, there *are* some things that lawyers refuse to do … and acting as a $CO_2$ monitor in a deep dark hole is one of them.)

---

[120] Bruce Arnold & Margaret Levin, 'Ambient Autonomy in the Virtualised Landscape: Autonomy, Surveillance and Flows in the 2020 Streetscape', 13(1) *M/C: A Journal of Media & Communication* (2010).

[121] Torin Monahan & Tyler Wall, 'Somatic Surveillance: Corporeal Control through Information Networks, 4(3) *Surveillance & Society* (2007) 154; Emilio Mordini & Sonia Massari, 'Body, Biometrics and Identity', 22(9) *Bioethics* (2008) 488; and Kirstie Ball, 'Organization, surveillance and the body: towards a politics of resistance', 12(1) *Organization* (2005) 89 on the 'informatised' and abstracted body.

[122] See for example arguments about agency in Wolfgang Sofsky, *Privacy: A Manifesto* (Princeton: Princeton University Press 2009).

[123] Roy Boyne, 'Post-Panopticism', 29(2) *Economy and Society* (2000) 285-307; Thomas Mathiesen, 'The Viewer Society: Michel Foucault's 'Panopticon' Revisited', 1(2) *Theoretical Criminology* (1997) 215-234.

[124] The canary down the mine is, alas, a fiction, an illustration of the way that popular (and academic) culture recreates the past. Prior to development of the Davy safety-lamp – and for several generations afterwards, in locations where life was cheaper than safety devices – the bird was more likely to be a starling, sparrow, thrush or other avian vermin. Canaries were exotic and expensive, premium status signals. If you could afford a canary in 1840 you would be an engineer or mine owner, rather than a 'horny-handed son of toil'.

In the age of digital coalmines, where those who have variously been characterised as the binary proletariat or cyberiat – people like you and I – are increasingly subject to a range of surveillance technologies, from monitoring of web browsing and telephone calls in the workplace (eg acceptance that *all* office communications in some finance sector businesses will be recorded) or tracking of company vehicles using GPS tools through to large-scale data-mining of financial transactions and 'presence' in online fora, who sounds the warnings?

It is tempting to suggest that children are the canaries down the digital coalmine, people who – like seniors, criminals, alleged terrorists and recipients of state welfare – are denied full personhood and deemed to be appropriately managed through current and emerging surveillance systems. The geolocation tools – watches, bracelets, badges, even implants – that are being marketed to anxious parents are also being marketed (arguably more successfully) to those who responsible for people undergoing a second childhood and for alleged/convicted criminals inside and outside physical custody.[125] The flourishing of the marginalised (and thus readily surveilled), along with the recognition or non-recognition of them as people rather than disembodied data subjects, should tell us something about how our society construes privacy and construes law.

This paper has referred to normalisation of surveillance practice. The reality is that children, although treated as less than people, are *not* the canaries down the mine. Instead we have embraced surveillance tools as a society and have yet to engage in an informed and positive debate about privacy values, privacy mechanisms (in particular the role of the state in addressing failures of self-management among Australian and global businesses), media responsibility and individual self-help.

Lack of regard for the recommendations in the Australian Reform Commission's latest privacy report among politicians, senior officials, business figures, leading journalists (and the eyeballs that legitimate tabloid violations of privacy in print and electronic venues) is disappointing and means that much privacy in Australia will continue to be characterised as 'dead duck' rather than 'canary at the coalface'. That is something we should and indeed can change.



[125] For RFID bracelets and implants see Isaac Rosenberg, 'Involuntary Endogenous RFID Compliance Monitoring As A Condition of Federal Supervised Release – Chips Ahoy?', 10 *Yale Journal of Law & Technology* (2008) 331, Kevin Werbach, 'Sensors and Sensibilities', 28(5) *Cardozo Law Review* (2007) 2321, Dick Whitfield, *The magic bracelet: technology and offender supervision* (Winchester: Waterside Press 2001), Erin Murphy, 'Paradigms Of Restraint, *57 Duke Law Journal* (2008) 1321.

## BIBLIOGRAPHY

- Statutes
- Cases and Submissions
- Books and Articles
- Reports, Dissertations and Discussion Papers
- Media Releases
- Other

### Statutes

*Crimes Act 1900* (ACT)

*Therapeutic Goods Act 1989* (Cth)

*Criminal Code Act 1995* (Cth)

*Telecommunications Act 1997* (Cth)

*Broadcasting Services Amendment (Online Services) Act 1999* (Cth)

*Crimes (Stalking) Act 2003* (Vic)

*Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2004* (Cth)

*Criminal Code Amendment (Suicide Related Material Offences) Act 2005* (Cth)

*Communications Legislation Amendment (Content Services) Act 2007* (Cth)

*Crimes Amendment (Sexual Procurement or Grooming of Children) Act 2007* (NSW)

*Child Online Privacy Protection Act of 1998* (15 USC 6501-6506)

### Cases and submissions

*von Hannover v Germany* (2004) 40 EHRR 1

*Mosley v News Group Newspapers* [2008] EWHC 1777

*Blake J Robbins v. Lower Merion School District*, US District Court for the Eastern District of Pennsylvania (2010)

### Books and articles

Katherine Albrecht & Liz McIntyre, *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance* (New York: Nelson 2006)

Robert Anderson, 'Why Information Security is Hard: An Economic Perspective', *Proceedings of the 17th Annual Computer Security Applications Conference* (2001) 358-366

Alessandro Acquisti, 'From the Economics to the Behavioural Economics of Privacy', in Ajay Kumar & David Zhang [ed], *Ethics & Politics of Biometrics* (Berlin: Springer 2010) 23-26

Bruce Arnold & Margaret Levin, 'Ambient Anomie in the Virtualised Landscape? Autonomy, Surveillance and Flows in the 2020 Streetscape', 13(1) *M/C: A Journal of Media & Communication* (2010)

Associated Press, 'Report: No Spying in Pa. School Laptops Case', New York Times 3 May 2010)

Mirko Bagaric, 'Privacy Is The Last Thing We Need', *The Age* 22 April 2007

Kirstie Ball, 'Organization, surveillance and the body: towards a politics of resistance', 12(1) *Organization* (2005) 89-108

Neil Ballantyne, Zachari Duncalf & Ellen Daly, 'Corporate Parenting in the Network Society', 28(1/2) *Journal of Technology in Human Services* (2010) 95-107

Naomi Baron, *Always On: Language in an Online and Mobile World* (Oxford: Oxford University Press 2008)

Sue Bennett, Karl Maton & Lisa Kervin, 'The Digital Natives Debate: A Critical Review of the Evidence', 39(5) *British Journal of Educational Technology* (2008) 775-786

Joseph Bonneau, Jonathan Anderson, Ross Anderson & Frank Stajano, 'Eight Friends Are Enough: Social Graph Approximation via Public Listings', *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems* (2009) 13-18

Danah Boyd, 'Facebook's privacy trainwreck: Exposure, invasion, and social convergence, 14(1) *The International Journal of Research into Media Technologies* (2008) 13-20

Danah Boyd, 'Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life', in David Buckingham [ed] *Youth, Identity, and Digital Media* (Cambridge: MIT Press 2008) 119-142

Roy Boyne, 'Post-Panopticism', 29(2) *Economy and Society* (2000) 285-307

Nik Brown & Mike Michael, 'A sociology of expectations: Retrospecting prospects and prospecting retrospects', 15(1) *Technology Analysis and Strategic Management* (2003) 3-18

L Jean Camp & Stephen Lewis [ed], *Economics of Information Security* (New York: Kluwer 2004)

Rachel Campbell, 'Teenage Girls and Cellular Phones: Discourses of Independence, Safety and Rebellion', 9(2) *Journal of Youth Studies* (2006) 195-212

James Carey, *Communication as Culture: Essays on Media & Society* (London: Routledge 1992)

Jennie Carroll, Steve Howard, Frank Vetere, Jane Peck & John Murphy, 'Just What To the Youth of Today Want? Technology Appropriation by Young People', 5 *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (2002) 131-140

Alan Cooper, *The Inmates Are Running The Asylum* (Indianapolis: SAMS 1999)

Peter Cumming, 'Children's Rights, Children's Voices, Children's Technology, Children's Sexuality' (Roundtable on Youth, Sexuality, Technology, Congress of the Humanities and Social Sciences 2009) (Ottawa: Carleton University 2009)

Zaineb De Souza & Geoffrey Dick, 'Disclosure of information by children in social networking – Not just a case of "you show me yours and I'll show you mine', 29 *International Journal of Information Management* (2009) 255-261

Terri Dowty, 'Overlooking Children: An Experiment With Consequences', 1(1) *Identity in the Information Society* (2008) 109-121

Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia* (Leichhardt: Federation Press 2005)

Neil Ballantyne, Zachari Duncalf & Ellen Daly, 'Corporate Parenting in the Network Society', 28(1/2) *Journal of Technology in Human Services* (2010) 95-107

Keri Facer, John Furlong, Ruth Furlong & Rosamund Sutherland, *Screen Play: Children & Computing in the Home* (London: Routledge Falmer 2003)

Adam Foster, 'Reframing Public Discourse on Child Abuse in Australia: Should child sexual abuse and child pornography in particular really be the number one priority in child abuse prevention?', 13(1) *NCPC Newsletter* (2005) 14-16

Kenneth Foster & Jan Jaeger, 'Ethical Implications of Implantable Radiofrequency Identification (RFID) Tags in Humans ', 8(8) *American Journal of Bioethics* (2008) 44-48

Trine Fotel & Thyra Thomsen, 'The Surveillance of Children's Mobility', 1(4) *Surveillance & Society* (2004) 535-554

Leanne Franklin & John Cromby, 'Everyday Fear: Parenting and Childhood in a Culture of Fear', 161-174 in Leanne Franklin & Ravenel Richardson [ed] *The Many Forms of Fear, Horror & Terror* (Oxford: InterDisciplinary Press 2009)

Leanne Franklin & John Cromby, 'There might be 10 paedophiles sitting in their front rooms: The 21st Century Monster', at http://www.inter-disciplinary.net/wp-content/uploads/2009/08/21st-century-monster-leanne-franklin.pdf

Michael Freeman & Philip Veerman, *The Ideologies of Children's Rights* (Dordrecht: Martinus Nijhoff 1992)

Anna Fry & Frank Willis, 'Invasion of Personal Space as a function of the age of the invader', 21 *Psychological Record* (1971) 385-389

Maya Gadzheva, 'Getting Chipped: To Ban or Not to Ban', 16(3) *Information & Communications Technology Law* (2007) 217-231

Alan Gewirth, *Self-Fulfillment* (Princeton: Princeton University Press 1998)

Anthony Giddens, 'Risk and Responsibility', 62(1) *Modern Law Review* (1999) 1-10

Barry Glassner, *The Culture of Fear: Why Americans are Afraid of the Wrong Things* (New York: Basic Books 1999)

Peter Glotz, Stefan Bertschi & Chris Locke [ed], *Thumb Culture: The Meaning of Mobile Phones for Society* (New Brunswick: Transaction 2005)

Erving Goffman, *The Presentation of Self In Everyday Life* (London: Allen Lane 1969)

Alasdair Grant [ed], *Australian Telecommunications Regulation* (Sydney: UNSW Press 2004)

Gary Gumpert & Susan Drucker, 'Public Boundaries: Privacy and Surveillance in a technological world', 49(2) *Communication Quarterly* (2001) 115-129

Robert Hahn & Anne Layne-Farrar, 'The Law & Economics of Software Security', 30(1) *Harvard Journal of Law & Public Policy* (2006) 284-351

Michael Hammond, 'What is an affordance and can it help us understand the use of ICT in education?', *Education & Information Technologies* (2009)

Bede Harris, *A New Constitution for Australia* (London: Cavendish 2002)

William Herbert, 'No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery', 22 *I/S: A Journal of Law & Policy* (2006) 409-473

Malcolm Hill & Kay Tisdall, *Children and Society* (London: Longman 1997)

Chris Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies* (2010)

Andrew Hope, 'Panopticism, Play and the Resistance of Surveillance', 26(3) *British Journal of Sociology of Education* (2005) 359-373

Andrew Hope, 'Risk Taking, Boundary Performance and Intentional School Internet 'Misuse'', 28(1) *Discourse: Studies in the Cultural Politics of Education* (2007) 87-99

Andrew Hope, 'Seductions of Risk, Social Control and Resistance to School Surveillance', in Torin Monahan & Rodolfo Torres [ed], *Schools under Surveillance: Cultures of Control in Public Education* (New Brunswick: Rutgers University Press 2010) 230-246

Sampsa Hyysalo, 'Some Problems in the Traditional Approaches to Predicting the Use of a Technology-Driven Invention', 16(2) *Innovation: The European Journal of Social Science Research* (2003) 117-137

Edward Ingebretsen, *At Stake: Monsters and the Rhetoric of Fear in Public Culture* (Chicago: University of Chicago Press 2001)

Rodney Ip, Katina Michael & M Michael, 'The Social Implications of Humancentric Chip Implants: A Scenario – 'Thy Chipdom Come, Thy Will Be Done'' (Faculty of Informatics Paper 2008) (University of Wollongong)

Marianne James [ed], *Paedophilia, Policy & Prevention (AIC Research & Public Policy Series, 12)* (Canberra: Australian Institute of Criminology 1997).

Philip Jenkins, *Moral Panic: Changing Concepts of the Child Molester in Modern America* (New Haven: Yale University Press 1998)

Vibeke Jørgensen, 'The apple of the eye: parents' use of webcams in a Danish Day Nursery', 2(2) *Surveillance & Society* (2004) 446-463

Cindi Katz, 'Me and My Monkey: What's Hiding in the Security State', in Rachel Pain & Susan Smith [ed], *Fear: Critical Geopolitics and Everyday Life* (Aldershot: Ashgate 2008) 59-72

James Katz, *Magic in the Air: Mobile Communication and the Transformation of Social Life* (New Brunswick: Transaction 2006)

Andrew Kenyon & Megan Richardson [ed], *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge: Cambridge University Press 2006)

Ruth Landau, Shirli Werner, Gail Auslander, Noam Shoval & Jeremia Heinik, 'Attitudes of Family and Professional Care-Givers towards the use of GPS for Tracking Patients with Dementia: An Exploratory Study', 39(4) *British Journal of Social Work* (2009) 670-692

Amparo Lasén & Edgar Gómez-Cruz, 'Digital Photography and Picture Sharing: Redefining the Public/Private Divide', 22(3) *Knowledge, Technology & Policy* (2009) 205-215

Marcus Leaning, 'The One Laptop per Child Project and the Problems of Technology-led Educational Development', in Ilene Berson & Michael Berson [ed] *High-Tech Tots: Childhood in a Digital World* (Charlotte: IAP 2010) 231-248

Richard Ling & Paul Pedersen [ed], *Mobile Communications: Re-Negotiation of the Social Sphere* (London: Springer 2003)

Sonia Livingstone, 'Children's privacy online: experimenting with boundaries within and beyond the family', in Robert Kraut, Malcolm Brynin & Sara Kiesler [ed] *Computers, phones, and the internet: domesticating information technologies* (Oxford: Oxford University Press 2006) 145-167

Patricia Loughlin, Barbara McDonald & Robert Van Krieken, *Celebrity and the Law* (Leichhardt: Federation Press 2010)

Stephen Lying, 'Edgework: A Social Psychological Analysis of Voluntary Risk Taking', 95(4) *American Journal of Sociology* (1990) 851-886

Frederick Maitland, 'A Prologue to a History of English Law', 14 *Law Quarterly Review* (1898) 13-33

Karen Malone, 'The bubble-wrap generation: children growing up in walled gardens', 13(4) *Environmental Education Research* (2007) 513-527

Alice Marwick, Diego Diaz & John Palfrey, *Youth, Privacy and Reputation* (Berkman Center Research Publication 2010-5) (Cambridge: Berkman Center, Harvard University 2010)

Gary Marx, 'The Engineering of Social Control: The Search for the Silver Bullet', in John Hagan & Ruth Peterson [ed], *Crime & Inequality* (Stanford: Stanford University Press 1991) 225-246

Thomas Mathiesen, 'The Viewer Society: Michel Foucault's 'Panopticon' Revisited', 1(2) *Theoretical Criminology* (1997) 215-234

Robert Mayer, 'Technology, Families and Privacy: Can We Know Too Much About Our Loved Ones', 26(4) *Journal of Consumer Policy* (2003) 419-439

Barbara McDonald, 'Privacy, Paparazzi and Princesses', 50 *New York Law School Law Review* (2005) 205-236

Gary Melton, 'Minors and Privacy: Are Legal and Psychological Concepts Compatible?', 62 *Nebraska Law Review* (1983) 455-493

Anneke Meyer, *The Child at Risk: Paedophiles, Media Representations and Public Opinion* (Manchester: Manchester University Press 2007

Katina Michael, M Michael & Rodney Ip, 'Microchip Implants for Humans as Unique Identifiers: a Case Study on VeriChip' (Faculty of Informatics Paper, 2008) (University of Wollongong)

Katina Michael & M Michael, 'The Diffusion of RFID Implants for Access Control and ePayments: A Case Study of Baja Beach Club in Barcelona' (2010)

Brett Mills, 'Television Wildlife Documentaries and Animals' Right To Privacy', 24(2) *Continuum: Journal of Media and Cultural Studies* (2010) 193-202

Torin Monahan & Tyler Wall, 'Somatic Surveillance: Corporeal Control through Information Networks, 4(3) *Surveillance & Society* (2007) 154-173

Mark Monmonier, 'Geolocation and Locational Privacy: The 'Inside' Story on Geospatial Tracking', in Katherine Strandburg & Daniela Raicu [ed] *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* (Berlin: Springer 2006) 75-92

Emilio Mordini & Sonia Massari, 'Body, Biometrics and Identity', 22(9) *Bioethics* (2008) 488-498

Erin Murphy, 'Paradigms Of Restraint, *57 Duke Law Journal* (2008) 1321-1410

Arvind Narayan & Vitaly Shmatikov, 'De-anonymizing Social Networks', *30th IEEE Symposium on Security and Privacy* (2009)

Margaret Nelson, 'I Saw Your Nanny: Gossip and Shame in the Surveillance of Child Care', in Margaret Nelson & Anita Garey [ed], *Who's Watching: Daily Practices of Surveillance Among Contemporary Families* (Nashville: Vanderbilt University Press 2009) 109-134

Alastair Nicholson, 'The United Nations Convention on the Rights of the Child and the Need for its incorporation in a Bill of Rights', 44(1) *Family Court Review* (2006) 5-30

Sarah Maslin Nir, 'An Online Alias Keeps Colleges Off Their Trail', *New York Times* 23 April 2010

Donald Norman, *The Invisible Computer* (Cambridge: MIT Press 1998)

Clive Norris, Jade Moran & Gary Armstrong [ed], *Surveillance, Closed Circuit Television and Social Control* (Aldershot: Ashgate 1998)

Clive Norris, *The Maximum Surveillance Society* (Oxford: Berg 1999)

Larry Nucci, Melanie Kilen & Judith Smetana, 'Autonomy and the personal: Negotiation and social reciprocity in adult-child social exchanges', 73 *New Directions for Child and Adolescent Development* (1996) 7-24

Andrew Odlyzko, 'Economics, Psychology and Sociology of Security', 2742 *Lecture Notes in Computer Science* (2003) 182-189

Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (University of Colorado Law Legal Studies Research Paper 9-12, 2009)

Kurt Opsahl, 'Facebook's Eroding Privacy Policy: A Timeline', Electronic Frontier Foundation (2010), at www.eff.org/deeplinks/2010/04/facebook-timeline/

Suzanne Ost, *Child Pornography and Sexual Grooming: Legal and Societal Responses* (Cambridge: Cambridge University Press 2009)

John Palfrey & Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books 2008)

Ross Parke & Douglas Sawin, 'Children's Privacy in the Home: Developmental, Ecological and Child-Rearing Determinants', 11(1) *Environment and Behavior* (1979) 87-104

Moira Paterson, *Freedom of Information & Privacy in Australia* (Chatswood: LexisNexis Butterworths 2005)

Sandra Petronio, 'Privacy Binds in Family Interactions: The Case of Parental Privacy Invasion', in William Cupach & Brian Spitzberg [ed] *The Dark Side of Interpersonal Communication* (Hillsdale: Lawrence Erlbaum 1994) 241-258

Richard Posner, 'The Economics of Privacy', 71(2) *American Economic Review* (1981) 405-409

Neil Postman, *Technopoly: The Surrender of Culture to Technology* (New York: Vintage 1993)

Hugh Potter & Lyndy Potter, 'The Internet, Cyberporn and Sexual Exploitation of Children: Media Moral Panics and Urban Myths for Middle-class Parents?', 5(3) *Sexuality & Culture: An Interdisciplinary Quarterly* (2001) 31-48

Jack Linchuan Qiu, 'The Wireless Leash: Mobile Messaging Service as a Means of Control', 1 *International Journal of Communication* (2007) 74-91

Jeffrey Reiman, 'Privacy, Intimacy and Personhood', 6(1) *Philosophy and Public Affairs* (1976) 26-44

James Roh, Anand Kunnathur & Monideepa Tarafdar, 'Classification of RFID Adoption: An expected benefits approach', 46(6) *Information & Management* (2009) 360

Larry Rosen, Nancy Cheever & Mark Carrier, 'The association of parenting style and child age with parental limit setting and adolescent MySpace Behavior', 29 *Journal of Applied Developmental Psychology* (2008), 459-471

Isaac Rosenberg, 'Involuntary Endogenous RFID Compliance Monitoring As A Condition of Federal Supervised Release – Chips Ahoy?', 10 *Yale Journal of Law & Technology* (2008) 331-359

David Salter, *The Media We Deserve* (Carlton: Melbourne University Press 2007)

Steven Schnaars, *MegaMistakes: Forecasting and the Myth of Rapid Technological Change* (New York: Free Press 1988)

Sharon Shafron-Perez, 'Average Teenager or Sex Offender: Solutions to the Legal Dilemma Caused by Sexting', 26(3) *John Marshall Journal of Computer & Information Law* (2009) 431-487

Chris Shepherd, Michael Arnold & Martin Gibbs, 'Parenting in the Connected Home', 12(2) *Journal of Family Studies* (2006) 203-222

Renee Smith, 'Can the use of 'Nanny Cams' be morally justified?', 9(24) *Think* (2010) 91-96

Bruce Smyth, 'Parent-Child Contact in Australia: Exploring Five Different Post-Separation Patterns of Parenting, 19(1) *International Journal of Law, Policy and the Family* (2005) 1-22

Wolfgang Sofsky, *Privacy: A Manifesto* (Princeton: Princeton University Press 2009)

Daniel Solove, *The Digital Person: Technology & Privacy in the Information Age* (New York: New York University Press 2004)

Valerie Steeves & Cheryl Webster, 'Closing the Barn Door: The Effect of Parental Supervision on Canadian Children's Online Privacy', 28(1) *Bulletin of Science, Technology & Society* (2008) 4-19

Andrew Stewart, 'On Risk: Perception and Direction', 23 *Computers & Security* (2004) 362-370

George Stigler, 'An introduction to privacy in economics and politics', 9 *Journal of Legal Studies* (1980) 623-644

Steven Strachan & Roderick Murray-Smith, 'Nonvisual Distal Tracking of Mobile Remote Agents in Geosocial Interaction', in Tanzeem Choudhury, Aaron Quigley, Thomas Strang & Koji Suginuma [ed], *Location and Context Awareness, 4th International Symposium* (Berlin: Springer 2009) 88-102

Adam Sutton & Dean Wilson, 'Open-street CCTV in Australia: The Politics of Resistance and Expansion', 2(3) *Surveillance and Society* (2004) 310-322

Don Tapscott, *Growing Up Digital: The Rise of the Net Generation* (New York: McGraw-Hill 1998)

Edward Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences* (New York: Knopf 1996)

Julian Thomas, Scott Ewing & Julianne Schiessl, *The Internet in Australia: CCI Digital Futures Report (*CCI, Swinburne University of Technology 2008)

Geraldine Van Bueren, *The International Law on the Rights of the Child* (The Hague: Nijhoff 1998)

Wim Veen & Ben Vrakking, *Homo Zappiens: Growing Up In a Digital Age* (London: Continuum 2006)

Philip Veerman, *The Rights of the Child and the Changing Image of Childhood* (Dordrecht: Martinus Nijhoff 1992)

Kevin Warwick, 'Cyborg Identity' in David Birch [ed] *Digital Identity Management: Perspectives on the Technological, Business and Social Implications* (Aldershot: Gower 2007) 227-238

Niranjala Weerakkody, 'Mobile Phones and Children: An Australian Perspective', 5 *Issues in Informing Science and Information Technology* (2008) 459-475

Jen Weiss, 'Scan This: Examining Student Resistance To School Surveillance', in Torin Monahan & Rodolfo Torres [ed], *Schools under Surveillance: Cultures of Control in Public Education* (New Brunswick: Rutgers University Press 2010) 213-229

Kevin Werbach, 'Sensors and Sensibilities, 28(5) *Cardozo Law Review* (2007) 2321-2372

Dick Whitfield, *The magic bracelet: technology and offender supervision* (Winchester: Waterside Press 2001)

Suzanne Willis & Bruce Tranter, 'Beyond the 'Digital Divide': Internet Diffusion and Inequality in Australia', 42(1) *Journal of Sociology* (2006) 43-59

Dean Wilson & Adam Sutton, 'Watched Over or Over-Watched: Open-Street CCTV in Australia', 27(3) *Australian and New Zealand Journal of Criminology* (2004) 211-230

Langdon Winner, *Autonomous Technology: Technics-out-of-control as a Theme in Political Thought* (Cambridge: MIT Press 1977)

Janis Wolak, David Finkelhor, Kimberley Mitchell & Michele Ybarra, 'Online 'Predators' and Their Victims: Myths, realities and implications for prevention and treatment', 63(1) *American Psychologist* (2008) 111-128

Maxine Wolfe & Robert Laufer, 'The Concept of Privacy in Childhood and Adolescence', in Stephen Margules [ed] *Privacy* (Stroudsburg: Dowden, Hutchinson & Ross 1974)

Georgina Wright, 'Paedophiles and Civil Liberties', 19(19) *Eureka Street* (September 2009)

James Youniss & Jacqueline Smollar, *Adolescent Relations with Mothers, Fathers & Friends* (Chicago: University of Chicago Press 1985)

Lucia Zedner, 'The Inescapable Insecurity of Security Technologies?', in Katja Aas, Helene Gundhus & Heidi Lomell [ed], *Technologies of InSecurity: The Surveillance of Everyday Life* (New York: Routledge-Cavendish 2009) 257-270

Kristen Zogba, 'Spin Doctors and Moral Crusaders: The Moral Panic Behind Child Safety Legislation', 17(4) *Criminal Justice Studies* (2004) 385-404

**Reports, dissertations and discussion papers**

Australian Bureau of Statistics, *Children's Participation in Cultural & Leisure Activities,* (Canberra: Australian Bureau of Statistics 2009), at www.abs.gov.au

Australian Law Reform Commission, *Review of Australian Privacy Law: Discussion Paper Vol 3* (ALRC Discussion Paper 72) (Sydney: Australian Law Reform Commission 2007)

Australian Law Reform Commission, *For Your Information: Australian Privacy Law & Practice* (ALRC Report 108) (Sydney: Australian Law Reform Commission 2008)

Tanya Byron, *Safer Children in a Digital World: The Report of the Byron Review* (London: Department for Children, Schools & Families 2008)

Patrick Heneise, *I – The Digital Me: Digital Communication and Identity Development in Mobile Geosocial Networks* (dissertation, Hochschule Furtwangen University 1 March 2009);

Digby Jones, *Cotton Wool Kids* (HTI Issues Paper 7) (Coventry: HTI 2007)

David Lyon, Stephen Marmura, Pasha Peroff, *Location Technologies: Mobility, Surveillance and Privacy: A Report to the Office of the Privacy Commissioner of Canada* (The Surveillance Project, Department of Sociology, Queen's University 2005)

Henrik Moen, *A Study of Wi-Fi RFID Tags in Citywide Wireless Networks* (MSc dissertation, Norwegian University of Science & Technology 2007).

Pew Internet & American Life project (February 2010) www.pewinternet.org

Ballard Spahr, *Report of Independent Investigation* (Lower Merion School District) [2010], at www.lmsd.org/sections/laptops/

Antony Young, *Accountants' Acceptance of a Cashless Monetary System Using an Implantable Chip* (PhD dissertation, RMIT 2007)

**Media releases**

Prime Minister, Treasurer, Minister for Finance and Minister for Broadband joint media release 'New National Broadband Network' (7 April 2009)

NSW Government Media Release, '2010 Student Laptop Rollout' (16 March 2010)

Minister for Finance & Deregulation and Minister for Broadband, Communications & the Digital Economy joint media release 'Landmark Study confirms NBN vision is achievable and affordable' (6 May 2010)

### Other

ABC Radio National, 'The Law Report: Criminals and Privacy' 28 March 2006 at www.abc.net.au/rn/lawreport/stories/2006/1601294.htm

Information Commissioner's Office, 'The Use of Biometrics in Schools' (August 2008) at www.ico.gov.uk

NSW Government, 'The Digital Education Revolution in NSW' (2009) at www.schools.nsw.edu.au/gotoschool/highschool/dernsw/thelaptop.php

Microsoft Australia, 'For Safety's Sake' (March 2010)

Office of the Privacy Commissioner (Australia), 'Attitudes to Privacy' (2008) at www.privacy.gov.au/aboutprivacy/attitudes

Privacy Victoria, *Privacy in Diverse Victoria: Attitudes towards information privacy among selected non-English speaking background and Indigenous groups in Victoria* (2002)

## Author

Bruce Arnold teaches law at the University of Canberra and previously consulted in Australia and overseas on regulatory aspects of digital technologies, along with market analysis for public/private sector clients. He has a *Juris Doctor* degree and is currently undertaking a PhD on Australian law's construction of identity.

Mr Arnold has been widely cited in journals, monographs and reports on privacy, law and new technologies and has written keynote articles on privacy in journals such as *Privacy Law Bulletin* and *Security Systems*. He has also presented papers at government, industry and academic conferences. He has a particular interest in biometrics and geospatial privacy, the latter being reflected in articles with Margalit Levin (Melbourne University) on urban informatics, such as the 2010 article in *M/C Media & Communications Journal* on ambient surveillance and synopticism in 'digital cities'.