"An open society depends on individuals rediscovering the social value of privacy..."

UK CONFIDENTIAL

Edited by Charlie Edwards
and Catherine Fieschi

COLLECTION 25

DEMOS

Contributors:

Jonathan Bamford
Peter Bazalgette
Chris Bellamy
Peter Bradwell
Gareth Crossman
Simon Davies
Peter Fleischer
Niamh Gallagher
Tom Ilube
Markus Meissen
Perri 6
Charles Raab
Jeffrey Rosen
Robert Souhami
Zoe Williams
Marlene Winfield

First published in 2008

Magdalen House, 136 Tooley Street,
London, SE1 2TU, UK

ISBN 978-1-84180-192-6
Copy edited by Julie Pickard, London
Series design by modernactivity
Typeset by Chat Noir Design, Charente
Printed by Lecturis, Eindhoven

Set in Gotham Rounded
and Baskerville 10
Cover paper: Flora Gardenia
Text paper: Munken Premium White

UK CONFIDENTIAL

Edited by Charlie Edwards
and Catherine Fieschi

COLLECTION 25

DEMOS

Contents

PRIVACY'S PUBLIC DEATH?

THE PUBLIC'S PRIVATE LIVES

REGULATING OUR PRIVATE LIVES IN AN OPEN SOCIETY

Acknowledgements

We would like to thank BT for their generous support of this collection.

We are enormously grateful to all those whose essays, comments and feedback helped to shape the collection and the introduction: Jonathan Bamford, Peter Bazalgette, Chris Bellamy, Peter Bradwell, Gareth Crossman, Simon Davies, Peter Fleischer, Niamh Gallagher, Tom Ilube, Markus Meissen, Perri 6, Charles Raab, Jeffrey Rosen, Robert Souhami, Zoe Williams and Marlene Winfield.

Demos staff provided invaluable advice and generous support: Alessandra Bounfino, John Craig, Celia Hannon, Duncan O'Leary and Jack Stilgoe. We are particularly grateful for Peter Bradwell's help.

We were ably supported by a regular wave of interns; we are especially keen to thank Mhairi Guild for all her hard work.

Charlie Edwards and Catherine Fieschi
May 2008

Foreword

Patrick O'Connell

The global technology and communication revolution of the last two decades has created an unprecedented quantity and quality of easily accessible information.

The data collected, categorised, analysed and accessed through modern technology has created better, faster and cheaper products and services in every part of the public and private sectors of democratic countries. Every citizen of these countries is both required to share, and able to access, more personal data than ever before. It is unsurprising therefore that the increase in personal data held in this way should be accompanied by an upsurge of interest in issues relating to the security and privacy of this data from individuals, civil society and businesses like BT.

As a global leader in communications services, BT helps a significant number of public and private sector customers to gather and use data in the most efficient, effective and secure way. As a company, we are conscious of the responsibility that we have to ensure both security and privacy are protected. As individuals we are all contributors and consumers of information and so the way in which institutions, businesses and governments use and protect that information matters to each of us.

The Prime Minister, in his April 2007 speech to the University of Westminster, highlighted the importance of these issues. Even before recent events involving security of data, he had called for a wider public debate about how data used in public and private realms could be subjected to oversight and independent scrutiny. He also discussed the opportunity afforded by technology to improve security of information and protect individual liberty.

In the interests of furthering the public debate of these and other related issues, we are pleased to support the work of Demos in collecting a number of engaging, challenging and thought-provoking essays, which together address the theme 'the social value of privacy'.

The views expressed here do not necessarily represent those of BT, but they are all of great interest to us and we welcome this report as a significant and timely contribution to the debate.

Dr Patrick O'Connell is Managing Director, BT Major Programmes.

Introduction

Charlie Edwards and Catherine Fieschi

The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire.[1]

A society that doesn't value and protect the privacy of the individual is one without intimacy, honesty or trust.[2]

Privacy seems to be in the midst of a very public death. Recent work on privacy has tended to focus on its disappearance: with the increase in surveillance and technological innovations, and the transformation of our social lives. But privacy is neither dead nor dying. Instead, as the essays in this collection suggest, it is our perception of what constitutes privacy that is radically changing, and with it our sense of what privacy means in today's open society.

Privacy protects a set of deeply significant values that no society can do without; it is about the lines, boundaries and relationships we draw between and among ourselves, communities and institutions. Rather than an empty ideal or state, attitudes to privacy tell us much about those fundamental relationships; what people think and expect of their neighbours, their fellow citizens and their government.

We all value our private life but as individuals our understanding of what constitutes privacy today is different from past generations. Our definition of what constitutes privacy has become increasingly stretched as we rely on each other more; lives become increasingly connected through everyday activities and virtually through a panoply of social networking sites. Already an unprecedented volume of stimuli and interventions come at us daily – solicited and unsolicited – at speed and with breath-taking ease.

Frequently conversations about privacy fail to consider context and the impact privacy has on our core values such as dignity, trust, honesty, intimacy and anonymity. The absence of this contextual anchor means such debates on privacy float meaninglessly above our everyday lives. It is why we need to consider the *social value* of privacy, which transcends our own individual interpretation of what privacy means, the role it plays in defining our social and political relationships, and the way in which 'if one individual or a group of individuals waives privacy rights, the level of privacy for all individuals decreases because the value of privacy decreases'.[3]

This entails the exploration of a *politics of privacy* in which we continually re-negotiate the relationship between privacy concerns and other values in specific circumstances. We must accept that individual claims to privacy impact on one another and may even be in tension,[4] and that privacy concerns may be of less importance in some situations than in others.

UK Confidential

This collection focuses on the status of privacy in the UK today. The collection deliberately offers a wide arc of opinion, context and commentary as privacy is 'too often debated in terms of laws and rights and technologies, when the interest of the issue is grounded in what people feel about, want for and value in the experience of private life and the personal projects, ties and commitments that it represents'.[5] As Catherine Fieschi points out in the opening essay, privacy and the extent to which it is valued is intimately connected to the extent to which people can influence the society and political landscape around them. In *Letters from America* in 1951 Alastair Cooke remarked on the cultural shocks of summer in New York, where people would be dogged from public place to public place by transistor radios carried by sports fans. The effect, he wrote, should 'produce a shudder in you. If it doesn't, then Britons are not what they used to be, and their passion for privacy… is dead and gone.'[6]

From this traditional sense of privacy as freedom from intervention into one's personal space, we have reached a point where our privacy has become a commodity to be exchanged for goods or services. Personal information has become the currency of the information age, distributed to corporations and governments alike and bartered away by the majority of us with scarcely a second thought as we accrue points on our Tesco club cards, rack up bills on Amazon and run around town using our Oyster cards. With each click and each swipe, we accept this continuous surveillance – tacitly or explicitly – in exchange for the services that are increasingly reliant on it.

The use and manipulation of personal information constitutes a global industry and as this commercial currency flows across public and private spheres with ease, social, economic and political boundaries appear to dissolve: information sourced in commercial transactions or by government departments and agencies; information about where and how we live, work, shop and drive; information about our histories and preferences.

Understanding privacy today

But privacy is more than this; it cannot be about data or information per se, nor even about transient cultural obsessions like reality TV. Privacy can be better understood as an elastic concept that acts as a gateway to a cluster of values such as dignity, trust, honesty, intimacy and anonymity.

And herein lies the problem. We lack the language to discuss privacy holistically. We use outdated frames of reference that are no longer adequate to discuss the contemporary landscape of privacy concerns or re-frame complex issues about data protection and vulnerability in other terms. To reduce cash-point theft, for example, the Home Office announced an initiative to paint out 'privacy spaces' around ATM machines to increase our sense of security: 'Consisting of a marked out box on the pavement around bank machines, the spaces are designed to give people privacy as they use the machines.'[7]

Privacy is an elastic concept. We all share certain understandings of it: a freedom to conduct our own personal lives free from prying eyes; that certain types of information are not to be revealed outside limited circumstances; that the 'Englishman's home is his castle'. Yet there is no monolithic definition of 'privacy' that holds firm across sectors and cultures.

For the most part, definitional wrangling occurs around a few broad nodal points. When we guard our privacy we fear the loss of a personal space in which to reflect and exercise autonomy, free from scrutiny, pressure or risk, whether it is the ability to organise our financial affairs, enjoy intimate relationships or participate in political life. We fear that dignity and power have been wrested from us to the extent that we are no longer in control of the access others have to us.

Many have argued that a general concept or 'right' to privacy is meaningless with 'privacy' often defined in terms of property (as exemplified by the instances in which celebrities go to the High Court over photographic rights) or liberty (when we protest governmental surveillance of our communications). This instrumentalisation of the concept of privacy means that it may better be thought of as the 'gatekeeper' to our core values.

In different cultures, different eras and different spheres of life, expectations of privacy relate closely to relations of power, concepts of dignity and social organisation. This elasticity reinforces the need to consider privacy as a shared concept, not an individual right, and one that evolves alongside the political, social and economic worlds in which we operate.

In defence of public life

For most of us, however, it is the elastic nature of 'privacy' that helps conceal rather than reveal the tensions between our individual rights and our collective responsibilities. As such the current debate on privacy has become polarised. In political, legal and business language alike, complex problems are reduced to recognisable conceptual frameworks that serve both to render the issue 'manageable' and to structure and influence the outcome of debate. This kind of reductionism rarely fits our complex societies without making serious omissions and is of little help in seeking to navigate them. And worst of all, 'privacy' now essentially denotes the data protection policy of a particular company or organisation.

For example, it was argued in a 2005 paper of the UK Presidency of the EU that 'to turn our backs on proven biometric technology, to ignore the use made of fingerprints, iris and digital photos by both government and the private sector would be to reject the twenty-first century'.[8] In such a discursive representation, only the obstructive Luddite, fighting the tides like King Canute, as described by Tom Ilube, could object to these developments. We need to go beyond the limitations of this bleak dichotomy and accept that while biometric technologies at our borders may well be an important part of the future, they come with attendant costs and benefits that we are yet to discover.

Just as importantly, attention is often so focused on the possibilities of government abuse that the status of privacy in other spheres – from the NHS to popular culture – is overshadowed in public discourse. We are regularly reminded that ‘there is no part of people’s lives which is free from snooping. State intervention and control expands every day.’[9]

Yet it is not only the state that is watching; we need a sense of the bigger picture in all its complexity. Recently an online map of central London, which includes aerial photography at four times the resolution of existing online maps, was launched. In the right conditions, images at this resolution are enough to identify individuals. The chief executive of the company was unapologetic. In an interview Alastair Crawford said the company, 192.com, was considering holding a competition. ‘We want to challenge people to find out how much naughty stuff is happening. If you’re having an affair in London, you’d better be careful!’[10]

While we may question whether such an initiative is at all useful we must remember that technology is only a medium through which the ideas and aspirations of individuals are developed. Technology is not the ‘problem’ confronting our civil liberties, nor will it define the future of privacy. However, society’s polarised views on privacy work to foreclose the debate, to establish ideological battlegrounds over civil liberties, security and the route to economic success. We need to open the discussion up, to accept ambiguity and conflicting social and political goals, and start arguing about our values.

At present, privacy issues are considered separately by sector and by sphere, in terms of information, communication, territory or the individual. Yet these divisions are becoming less salient in the twenty-first century. It is no longer possible to separate out these aspects as it once was. The fluidity between spheres of life and the extent to which areas are interlinked should therefore caution us against viewing privacy debates in isolation, where each is legislated for vertically, however limited our ability to regulate comprehensively across such different sectors may be.

Privacy is about the lines we draw between ourselves and others, one world and another. As such we should begin to think about privacy in terms of ‘border crossings’, instances where ‘a border of the person is crossed’, whether this is a physical or socio-cultural barrier.[11] This metaphor is particularly pertinent in the context of globalisation as the world is rapidly being moulded into a shared social space by economic and technological forces which results in diverse impacts between and on regions or sectoral forces which were previously unconnected.[12]

The invisible transaction

The exchange of our privacy is increasingly an active transaction we take part in every day. However, it is not one that we are always cognisant of, let alone in a strong bargaining position for. Personal information is attached to a market decision in most cases and is increasingly hidden from view. In the most obvious scenario, we enter our personal details in-store or online in order to purchase a product we want, thus accepting the probability that our details will be used to target us for similar transactions in future. We pay less attention, however, to the 'cookies' that are placed on our hard drives as we browse online, monitoring our activities.

We rarely make an objective decision about how much of our privacy we are willing to trade for goods or services we receive in return. Privacy is thus often reduced to a mere procedural question in the commercial context – where it is up to us to pursue the details and 'opt out' if such an option is offered. Today activities such as driving, opening a bank account, even shopping, require a lot of information, a lot of subsequent monitoring and, as things stand, a substantial degree of acquiescence to the higher wisdom of the necessary agency or corporation not to misuse it. As information is used to tailor services ever more precisely, we increasingly have only the choices we are offered.

While governments have always needed to tow a line between privacy concerns and the demands of service provision, private companies have traditionally tended to downplay the issue of consumer privacy. They have often argued that the market or new technologies will define the future of privacy. Recently, research from Harvard and Carnegie Mellon has suggested that large companies may not have much of an economic incentive to prevent privacy breaches, while others have pointed out that privacy is 'a latent concern: the more people know about information risks, the more concerned they become'.[13]

Managing a climate of fear

If concern over the status of privacy is becoming more high profile in the private sector, in the political sphere an intensified 'ambition to control and managerialise the future'[14] has sought increasing stores of personal information about its citizens. This occurs simultaneously as a function of emotionalism and of rationalism in public life, each working towards the 'elimination' of risk, whether from terrorism and crime or from inefficiency and human error in service delivery.

Perri 6 suggests that privacy can be understood as a claim for protection against a series of risks: to property, to liberty, to reputation, to physical security.[15] In the age of information, which otherwise benefits us in so many ways, privacy can be seen not only as our protection against risks, but as itself increasingly *at risk* as a result of our attempts to control against other hazards; for example, the focus of many counterterrorism measures has been physical territorial borders through the innovative use of biometric technologies and registration schemes. It has been pointed out, however, that the border-control mode of response to current security threats does not really answer the problem posed by terrorism.[16] In the matter of security, therefore, we would do well to remember the warnings of Dietrich Dorner that 'failure does not strike like a bolt from the blue; it develops gradually according to its own logic'[17] as understandings of both problems and solutions acquire their own momentum.

At both the domestic and the international level there are strong justifications for a degree of surveillance; even those in favour of stronger safeguards for privacy expect to negotiate their level of privacy against other needs in practice.[18] But as Jeffrey Rosen points out, many of the security measures we accept, or even demand, in the name of security play primarily to emotional responses and not to empirical analyses of the problem.

Some commentators go one step further suggesting that security has too long been taken as its own vindication, a pursuit that legitimises all measures. In fact, 'absolute security is a chimera, perpetually beyond reach' and one can indeed have 'too much security'.[19] That said, this rarely stops us pursuing technological answers, whether it is the 'naked machine' at the airport as described by Rosen or compulsory ID cards. If this is the case it becomes important that the values attached to privacy are articulated. More importantly, the burden of proof must remain on those who would erode it. As Liberty warns: 'We are moving away from a position where information is not shared unless necessary, towards one where it will be shared unless there is a reason not to.'[20]

What have you got to hide?

Unsurprisingly, given the loss of data by government departments, agencies and some companies, there is a presumption of distrust in the practice of information gathering by government, and growing consternation that a reluctance to hand over personal data implies that one has 'something to hide'. Such a disposition is not only unpleasant for the texture of society but corrodes the social contract. As Richard Thomas, the Information Commissioner, has warned of ID cards, such systems of surveillance effect a very significant sea change in the relationship between the state and every individual in this country.[21]

We are reminded by Jonathan Bamford, for example, that Britons are the most watched people in the world, with one closed circuit television (CCTV) camera for every 14 people. Our collective anger at such information often hides our individual support for such measures. As David Lyon argues, surveillance has 'two faces – one that intrudes and impacts on privacy, and one that watches and, potentially protects – but both may [be] visible simultaneously'.[22] And despite the lack of conclusive evidence that CCTV prevents crime, for example, it *has* been shown to have success at minimising road accidents.[23]

As Joan Smith argued in the *The Moral Universe*, reticence about disclosures relating to one's private life 'becomes synonymous, to many journalists, with having something to hide',[24] an observation that has tended to be reflected in the political sphere in recent years. Significantly, it is in the context of our right to scrutinise public figures that privacy laws have often been most tested. As Western culture has become increasingly fascinated with celebrity, aided by the speed and technological sophistication of the media and communications industries, the level of intrusion has intensified far beyond unseemly gossip.[25] High-profile court cases such as those brought by Catherine Zeta Jones and Michael Douglas or Naomi Campbell in recent years, as well as paparazzi harassment such as that preceding the death of Princess Diana, have ironically served as significant nodes of public debate for how we think of privacy, consent and intrusion.

As Zoe Williams argues one is more likely to discuss privacy in terms of the right of celebrities to be free of excessive paparazzi intrusion or harassment by the tabloids, than in terms of the data-sharing practices that so regularly affect our *own* lives. In the media industry, we also see the harsh tension between the market and broader social values. Sometimes players self-regulate, as they have at times with the younger royals. This was seen in the case of Kate Middleton, girlfriend to Prince William but otherwise a fairly normal young woman, who was subjected to continuous press surveillance. The tabloids finally stepped back in response to threats of legal action.

A final development relates to the private figure in the public sphere, as the last decade has witnessed the phenomenal rise of reality TV, particularly *Big Brother*. Unique among reality formats, the programme strips away all privacy: contestants are filmed 24 hours a day – eating, sleeping, brushing their teeth, losing psychological control and screaming and rowing with one another. In this instance meaningful privacy relates less to information or bodily access per se than to the more pervasive erosion of intimacy in our 'access all areas' culture.

As Peter Bazalgette argues, the generation growing up as we write has developed entirely different parameters for privacy from those preceding it.[26] Do we need to know if David Cameron, or anyone else for that matter, took drugs at school? Bazalgette's answer is no: politicians are entitled to a past that is private and remains private. Do we need to know if a prominent politician has cheated on his wife or had an affair with a married woman? Only if we suspect further corruption or abuse of his position is involved. As scandals of recent years have shown, the lines are blurred between the 'conflict of interest' story we may be entitled to, and the personal, salacious minutiae that are often dug up. The tendency towards function-creep is again in evidence as 'necessity, proportionality and consent' pale in the face of the de facto technological capability to circulate such stories. We have the conversation after – and *because* – the private information is made public, not in advance of the fact.

Conclusion

When asked, we tend not to want our personal information to be used and manipulated without our consent, the chance to correct it or to limit its accessibility; yet every day we make decisions and choices that suggest we ultimately don't care or know enough.

As this collection demonstrates, our collective ignorance means we get the privacy culture we deserve. What seems clear is that any settlement between the individual and society, the public and the state, the consumer and business must be accommodating enough to develop alongside new technologies, varied cultural needs and emergent patterns of governance. What matters is our active participation in negotiating the terms and conditions of privacy.

Notes

[1] A Westin, *Privacy and Freedom* (New York: Athenaeum, 1967).

[2] S Chakrabarti, 'Yet another step along a dangerous road', speech, published in the *Independent*, 15 Jan 2007.

[3] P Regan, *Legislating Privacy: Technology, social values, and public policy* (Chapel Hill, NC: University of North Carolina Press, 1995).

[4] C Bennett and C Raab, *The Governance of Privacy: Policy instruments in global perspective* (Cambridge, MA: MIT Press, 2006).

[5] Perri 6, *The Future of Privacy*, vol 1 (London: Demos, 1998).

[6] A Cooke, 'It's a democracy, isn't it?', 15 June 1951, *Letters From America* (London: Penguin, 2004).

[7] Home Office, 'Privacy spaces will tackle robbery', press release, 8 Feb 2007, see http://press.homeoffice.gov.uk/press-releases/privacy-spaces?version=1 (accessed 25 Feb 2008).

[8] UK Presidency of the European Union, 'Liberty and security: striking the right balance', 7 Sep 2005, see www.eu2005.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1107293561746&a=KArticle&aid=1125560449884&date=2005-09-07 (accessed 25 Feb 2008).

[9] 'Tories attack data-sharing plans', *BBC News*, 14 Jan 2007, see http://news.bbc.co.uk/1/hi/uk_politics/6260767.stm (accessed 25 Feb 2008).

[10] See www.guardian.co.uk/technology/2008/jan/24/privacy.internet (accessed 8 Mar 2008).

[11] GT Marx, 'Seeing hazily (but not darkly) through the lens: some recent empirical studies of surveillance technologies', *Law and Social Enquiry* 30, no 2 (Apr 2005).

[12] D Held et al, *Global Transformations: Politics, economics and culture* (Stanford: Stanford University Press, 1999).

[13] Perri 6, *The Future of Privacy*, vol 2 (London: Demos, 1998).

[14] Ibid.

[15] Perri 6, *The Future of Privacy*, vol 1 (London: Demos, 1998).

[16] E Guild, 'International terrorism and EU immigration, asylum and borders policy: the unexpected victims of 11 September 2001', *European Foreign Affairs Review* 8 (2003).

[17] D Dorner, *The Logic of Failure* (New York: Perseus Books Group, Sep 1997).

[18] Perri 6, 'Introduction', *Future of Privacy*, vol 2.

[19] L Zedner, 'Too much security?', *International Journal of the Sociology of Law* 31 (2003).

[20] Liberty, 'Position paper on ID cards', 2006.

[21] Ibid.

[22] D Lyon, *The Electronic Eye: The rise of surveillance society* (Minneapolis: University of Minnesota Press, 1994).

[23] Surveillance Studies Network, *A Report on the Surveillance Society*, for the Information Commissioner (Sep 2006), see www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed 8 Mar 2008).

[24] J Smith, 'Private lives, public property?' in T Bentley and D Stedman Jones, *The Moral Universe* (London: Demos, 1998).

[25] SD Warren and LD Brandeis, 'The right to privacy', *Harvard Law Review* IV, no 5 (15 Dec 1890), available at www-swiss.ai.mit.edu/6805/articles/privacy/Privacy_brand_ warr2.html (accessed 2 Mar 2008).

[26] P Bazalgette, 'House proud', *Prospect*, Mar 2007.

Essay summaries

Privacy's public death?

The social value of privacy

Catherine Fieschi

The received conception of privacy under which we operate is rooted in the language of rights, and perhaps more specifically in the Universal Declaration of Human Rights. The European Convention on Human Rights and the UK's corresponding 1998 Human Rights Act and other constitutional guarantees make it a ubiquitous right in most advanced industrial democracies. While we know that the concept of privacy varies from one culture to another, this variance raises some profound questions as to our understanding of privacy, its elasticity and the way in which it might evolve in the future.

Whose privacy is it anyway?

Zoe Williams

Individuals have never had so much privacy. Daunted by the surveillance possibilities of modern technology, we forget how many surveillance possibilities our nearest and dearest used to have just by opening their curtains. So we funnel essentially irrational anxieties into a wider fear for our privacy from the prying eyes of the world, and by a happy dovetailing, our celebrity ego ideals reflect those anxieties right back at us, at greater volume. Our irrational anxieties have no basis in reality at all.

Where everybody knows your name

Tom Ilube

A world rich in personal information brings with it risks. And this world of information is a reality, a necessary part of globalised business, international communication and interaction. The amount of personal information about us increases exponentially every year. Instead of being fearful, we need to understand how to prosper in this world. Appreciating promotion, through the technologies that spawn such a wealth of data, is as important as privacy protection.

Drunken students, beauty queens and pole dancing

Peter Bazalgette

The bulk of users employ their MySpace and Facebook entries for self-advertisement, social networking and the generally raw process of growing up. They are the first generation that can tell you precisely how many 'friends' they have. They are also the first generation whose sexual adventures, drug taking, immature opinions and personal photographs are shared electronically.

The public's private lives

Being watched

Peter Bradwell and Niamh Gallagher

Shutting the door, drawing the curtains, disconnecting the phone, deleting the files and stashing the diaries; the realm of the private is at once comforting and essential. But the scent of the illicit or illegal is never too far away. In the connections between 'closeness' and affiliation there sit expectations about what we want, or are entitled, to know of others, and vice versa. The way we talk about privacy can tell us a lot about our social fabric, yet it is often seen as 'merely' a civil liberties problem, a predictable whine of the chattering classes or paranoid libertarians. We should understand privacy as being about control, context and choice. Across all three dimensions the privacy challenge is changing.

A place of greater safety? Information sharing and confidentiality

Perri 6, Chris Bellamy and Charles Raab

Information sharing across public services is seen as key to coordinating the efforts and support of government departments. But this poses particular problems for privacy, often phrased in the language of balance – between confidentiality and collaborative working. But these decisions over risk are not about balance or general rules; they involve *judgement* and *choices* about individual cases and the risks attached to each. Guidance at the moment concentrates on the risks of not sharing. But future government intervention needs to be based around training to develop the skills and capacities for these judgements to be made, rather than more guidance or legislation.

The case of electronic patient records: is the privacy debate a smokescreen?

Marlene Winfield

If the majority of us are 'privacy pragmatists', then we need to understand why the current phase of NHS reform, based around electronic medical information and better sharing of it, is happening, and what the benefits are. The NHS IT programme is centred on changing the relationship between health service and patient by putting the emphasis on patients' informed choices, and allowing them to have a greater voice in the health system. There are compelling and necessary benefits to connected health records, from better-informed patients and staff, to better research into medical and health trends. The opposition, in particular from doctors, can be seen as a reaction against the empowering of patients in this system with a greater voice, and better health information.

How personal medical data can improve the public's health

Robert Souhami

The opportunities for UK research to improve the health and lives of the population are now exceptional. But just at this moment of opportunity, changes in the laws concerning privacy, combined with confused interpretation and regulation of these laws and a conflicting and multilayered bureaucracy, have put such research at risk. As citizens we know we have responsibilities as well as rights.

Regulating our private lives in an open society

Sleepwalking into a surveillance society

Jonathan Bamford

The thirst for more information about individuals seems unquenchable but it would be unduly pessimistic to believe that data protection and privacy laws are at best anachronistic, and at worst completely useless. It is fair to say that data protection and privacy regulation has struggled to keep pace with the technological, economic and political changes that have driven the expansion in the breadth and depth of personal details held about individuals.

Towards global privacy standards

Peter Fleischer

Information and data now flows easily and instantly around the globe. But our data protection legislation does not match this reality. Instead, there is either no protection, or, where it exists, it is not compatible enough with information protection regimes in other countries or regions. Because of the complex and interconnected nature of the global information economy, we need to develop the patchwork of alternative approaches into a coordinated drive to develop global privacy standards, consistent with commercial realities, political needs and technological realities.

The naked machine: privacy and security in an age of terror

Jeffrey Rosen

When it comes to the protection of privacy, legal values tend to reflect and follow social norms, rather than the other way around. Perhaps those who hope to import a European understanding of privacy into the US, and vice versa, should focus on changing social understandings of privacy rather than on passing new laws. But can social understandings of privacy easily be changed to accommodate both honour and liberty? A society where citizens refuse to respect their own privacy is not one where privacy will be long respected; and the US experience suggests that citizens in an individualistic market democracy may perceive too many market rewards for exposure to respect their own privacy for long.

The culture of control

Simon Davies

The current interest in privacy stems from the broader concern over loss of human autonomy. The number of people who are restrained or disciplined by legal, administrative and judicial mechanisms each year is a thousand per cent greater than 20 years ago. Legislation regulating conduct in public has increased 15-fold in the same period. The requirement for ‘permission’ to initiate group activities has soared. It can now be argued successfully that individual freedom is no longer conditioned by what is expressly prohibited in law, but instead is circumscribed by what the law expressly permits. In this context privacy takes on a libertarian aspect and thus becomes the standard bearer for the general issue of freedoms.

The architecture of privacy: space, power and human rights

Markus Miessen and International Festival

This chapter looks at privacy as a socio-spatial concept. Like the boundaries between our home and the street, the space around us comes to reflect the priorities of privacy: whom we choose to let in to spaces and whom we choose to keep out. Through stipulations about minimum overlooking distance and the often mandatory half metre between pavement and front door, such considerations are in fact at the heart of the UK planning system. The way spaces are organised is not only a result of, but helps to shape, relationships between people and groups, and influences how people understand their identity, position vis-à-vis others, and culture of everyday life.

Regulating privacy

Gareth Crossman

In 2008 we are subject to levels of state and private sector intrusion and surveillance unimaginable ten years ago. This is not necessarily a bad thing. Surveillance techniques need to adapt to deal with modern criminality while data sharing can make life more convenient and improve access to public services. What has been missing in government policy in recent years is a sense of proportionality limiting privacy intrusion so that it is targeted and appropriate. This overarching principle can be applied across the range of privacy-relevant subjects. Citizens are dubious about the extent to which their personal details and images will be accessible through tools such as the National Identity Register, National DNA Database and CCTV cameras. A government that is willing to listen to the growing expressions of public concern about privacy intrusion will provide a crucial opportunity for progressive change and will help make privacy a meaningful concept once again.

PRIVACY’S PUBLIC DEATH?

1 The social value of privacy

Catherine Fieschi

The idea of human beings as social animals has deep philosophical and emotional appeal, and following in Aristotle's footsteps we easily acquiesce to our unfailingly social nature. The Roussseaus and Hobbes of this world may have periodically introduced a note of scepticism as to the inherently positive nature of social relationships; recent research has tended to bear out the sociability thesis for better or for worse. Whether this sociability gives rise to tribalism and sectarian instincts, or whether it is perceived as enabling 'the better angels of our nature', it is understood as pivotal to our understanding of human motivation.[1]

Examining the concept of privacy is an additional lens through which we can usefully examine the nature and ways of sociability because it allows us to examine human beings as they really are – neither entirely social, nor primarily individualistic, neither needy busybodies nor not-so-noble savages, but rather as beings who thrive and survive through exchange and whose needs can be fulfilled only through a form of interdependence that entails knowledge of each other and various forms of trust. Privacy allows us to posit human beings as relational. The aim of this chapter is to move beyond individualistic and spatial understandings of privacy towards a more relational one – an understanding that moves beyond the paradoxes of modern and postmodern life and hopefully nuances a received wisdom deeply rooted in an eighteenth-century view of human beings as having no choice but to be either estranged from society or riveted to one another. We have already begun to use, if not properly to think about, privacy as a commodity, but we have not yet begun to contemplate the needs of the relationships that we trigger through this new conception of privacy, nor about the parameters of these relationships and the choices to which they give rise and the adjustments that they require us to make in our very understanding of the concept of privacy. If we can start to think of privacy as the regulatory mechanism through which we can construct our relationships to each other and to the state, then we can leave behind a very clunky public/private division, just as we can move beyond banal and misleading statements about global villages.

To do this I'll outline a couple of paradoxes, examine one or two clichés, and delineate what we might call a 'relational' understanding of privacy as it relates to a world where community and collective action – and therefore how we relate to one another – hold the key to our wellbeing and survival. We know that relationships are at the heart of politics. How can thinking about privacy in new ways help us to structure these relationships in the twenty-first century?

The private realm

Much of liberal political thought is structured around the dichotomy between the public and the private – in fact, it is an almost inescapable axiom of the liberal mindset and one which many have rightly striven to define, protect and defend. But I would suggest that we need to re-think and re-phrase this axiom slightly. In a world of dissolving spaces and boundaries and increased information, the shape of each of these spheres is changing irreversibly. What may matter more and more are the tools with which we negotiate these increasingly fluid barriers and our evolving needs and aspirations rather than camping stubbornly on a territory that is shifting beneath our feet.

What we have until now referred to as 'the private realm' may well become more nebulous (parenting is coming under increasing public scrutiny for educational and other purposes; family life is regularly examined for its impact on lifestyle and behaviour; private beliefs and convictions are 'outed' both in the name of recognition as well as for the purposes of cohesion and security). In such a climate, the 'personal' and the 'intimate' may well take on ever more importance and we need new perspectives and instruments to defend and understand their relevance.

As for the 'public realm', it is continuously reshaped by more ephemeral but also unforeseen and powerful forces (linked to obvious changes in IT, the Web 2.0 revolution and its consequences, but also linked to population pressures, migration and capital flows). In this situation, where the intimate and the anonymous, the personal and the disembodied collide, the concept of privacy as a regulatory mechanism between new versions of the personal (and not only the private) and the public may well be one of the many tools we need to negotiate those new boundaries that emerge as older ones dissolve.

Privacy and paradox

It has become commonplace to argue that one of the hallmarks of late- or postmodernity is both the speed at which information travels and the amount of information that is both held about us and that we hold about others – all this against a background of ever-increasing levels of alienation, isolation and depression. In other words there are two paradoxes. The first is that information and the flows of information which we once held to be the secret to connecting to each other and to securing shared goals, values and objectives, as well as an increased capacity to realise them (a conception of progress linked to our capacity to know more about each other and thereby work together better), seem to come at the cost of deep disconnection and alienation in part undermining their very aim.

The second paradox – not unrelated to the first – is that we use and trade information every day (including personal information, which can be slowly and increasingly collated and interpreted across public and private boundaries) much as we would any other currency or commodity in exchange for better and more tailored services. Personalisation in public services, ease of movement and increased convenience have in part come at the expense of received notions of privacy. And as pointed out by analysts, many of these transactions have become invisible, such is their degree of embeddedness in technologies, practices and our daily lives. Yet, while information is collected, processed, stored and distributed on an unprecedented scale by both private and public organisations (and by our own selves), the conditions under which most of us live out our respective existences suggest that we share less and less with those who are spatially closest to us. And, further, while we may know our neighbours less, the information universe we inhabit allows us to develop relationships across the ether with perfect (or imperfect) strangers with whom we share concerns, lifestyles and secrets. For example, Aron Ben Ze'ev makes a compelling argument in his book *Love Online*[2] about the extraordinary degree of intimacy achieved thanks to hitherto unknown levels of anonymity through online relationships.

Why do these paradoxes matter? First, because they partly explain our scrambling for the communal, the neighbourly: the turn to a 'politics of proximity' in an attempt to return to a spatial scale that might seem more in tune with both traditional interaction as well as governmental capacity to govern and deliver goods at a time of increasing differentiation of needs. This can, of course, yield both the worst of tribal results (an increase in gang culture, rampant nimbyism, and the aggressive hopelessness of communities ridden with anti-social behaviour orders and the rampant paranoia of those who live next door) or create a much-needed palpable sense of place and belonging. But, no matter which, it highlights our deep unease in the face of a dissolving sense of boundaries between the personal and the public, the visible and the invisible, the familiar and the new.

For the purposes at hand, two further reasons make these paradoxes relevant to a discussion on privacy.

The first is that the reading of our human condition through the lens of this paradox relegates us to the status of near-passive victims – a situation in which we are no more than flotsam in a churning sea of global forces. This scenario depicts us as utterly unable to negotiate the complexity and sheer force of international pressures – in the form of population diversity, capital flows, information exchanges and all that is generally associated with globalisation. I balk both at the characterisation of our condition and at the overwhelmingly negative rendition of globalisation that it implies. We can do better than that on both counts – make more of these deep transformations, seize the opportunities for development, wellbeing, wealth creation and redistribution and mobilise creatively enough to mitigate the negative effects of these transformations and make the most of what they offer. But in order to do this we must find new tools to negotiate new boundaries, permeate new fields and understand evolving human reactions and needs in the face of these.

The paradox matters in a second sense as well because it tempts us into thinking of privacy as a possible escape from modern life to a primeval human state of self-sufficiency and self-containment. Privacy here is a retreat into a pristine, individualised space, but more importantly even, it is almost a fantasy of a 1950s, or even prewar, space, emblematic of a more traditional lifestyle and depicted as if it were in direct opposition to the world we live in – a time during which families sat down for dinner together, neighbours knew and helped each other.

In this communal fantasy (modern, but not too modern) 'bob-a-job' communities had clear boundaries and obvious gatekeepers. Never mind the fact that – where it existed – this fantasy lasted no more than a handful of decades, politicians hark back to a time when communities had contours and when, once behind the closed door of the family home, people did as they saw fit, and thankfully everyone (or so the fantasy goes, dismissing any notion of power or lost voices) 'saw fit' in the same manner.

Behind the 1950s fantasy lurks the ghost of a made-up figure of the individual – self-contained, emotionally restrained but also more authentic, but above all decisive in embracing a certain place in a world full of certainties.

These visions of privacy are less than helpful. This is privacy 'on the back-foot' – all about retreat and threat rather than a key tool to help us navigate the new shape of the relationships in which we find ourselves. How do we move on from this nostalgic concept of privacy, to one that is fit for the twenty-first century? Traditional interpretations don't help.

Negotiating the received wisdom

Most of us operate with a conception of privacy rooted in the language of rights, and perhaps more specifically in the Universal Declaration of Human Rights, whose Article 12 specifically enshrines the right to privacy as protection from arbitrary interference. The European Convention on Human Rights as well as the UK's corresponding 1998 Human Rights Act and other constitutional guarantees make it a ubiquitous right in most advanced industrial democracies.

We also know that the concept of privacy varies from one culture to another, but this variance raises some profound questions.

The Universal Declaration of Human Rights refers to 'privacy'; the French, Italian, Spanish and German translations, to name a few, refer to 'private life'. Scandinavian translations on the other hand use their word for 'privacy' (in Finnish for instance 'yksityisyys'). But beyond the much-noted absence of a word for 'privacy' in some languages (and anyone with, say, Italian relatives will know that such an absence has very tangible repercussions in day-to-day life), it is worth asking ourselves what this absence means.

Enshrining the concept of 'privacy' in the highest law means enshrining a fundamental human need or human value – much as one would refer to dignity or compassion for example. What we value here is precisely that, a value. And in a sense what we recognise and are committed to – beyond the value itself – is our capacity to be emotionally attached to it collectively (in that we undertake to defend it should it come under attack). Such enshrining gives this value a social meaning and a political status. What we value – and celebrate – is both our capacity to hold the personal dear and publicly make that dearness a social good. The concept of privacy is therefore in part defined by its capacity to link the personal to the social and public. For example we recognise the fact that we all value the affection and commitments that hold a family together as a unit, and we publicly declare this unit's functioning to be a social good. By enshrining privacy in the law we give the personal a very public status.

When we use the language of 'private life' (rather than 'privacy') on the other hand, what we value is a space rather than a value. It is a particular kind of space and the law recognises its importance to all human beings, but it is outside us, no matter how much value we want to ascribe to it. So what? I would argue that the vying between these two understandings of privacy prevents us from ascribing to it the value and role it deserves.

First, taking privacy as a space leads to some positive and some negative results. On the up side, a space can be tended: such an understanding places emphasis on the communal; it highlights the value of the commons and a rich civic society structured around notions of public space. On the down side, it can create strong, near-impermeable boundaries between the public and the private that often prove difficult to negotiate in political terms. More to the point, with its emphasis on space rather than people it creates a version of itself in which is difficult to maintain what Baumann calls our 'liquid' state of modernity.[3]

On the other hand, taking privacy as an inherent human need has equally contrasting results. On the negative side it creates the kind of individualism (some have even referred to a culture of narcissism) that is the hallmark of Anglo-Saxon democracies, but more particularly of the US, and can lead to the kind of commodification of privacy of the sort we delineated earlier: something to be traded and exchanged at will. This means that it can be both eaten away at through a process of constant re-calibrating of the ladder of values, dangers and needs, or held up as non-negotiable trump-cards, a situation that leads us down the blind alleys of non-negotiability: security vs freedom, privacy vs security, etc.

More positively, however, privacy in this model can more easily be adapted to the needs of societies whose borders have become more fluid.

So both of these conceptions yield negative and positive results, but I would argue that privacy, rather than being about how we protect our own turf or maintain our own backyard free of strangers, could just as easily be seen as an instrument through which we regulate relationships, in other words, how we relate to others, to organisations and to institutions.

Towards a relational concept of privacy

Conceiving of privacy as 'border crossings' – that is instances where 'a border of the person is crossed', whether this is a physical or socio-cultural barrier – is a step in the right direction. In this regard, as Gary Marx has suggested,[4] the empirical status of what was known is altered, going from 'private' to 'public' to some degree. I would argue, building on that, that a better way of understanding what this relational approach might mean is to think of privacy in this instance as a tool for transformation. In other words something that allows us to move from one perception of someone to another one. For example, from foreigner to neighbour, from stranger to friend. Negotiating the different levels of privacy, pacing the relationship and using the notion of privacy as regulator and, more to the point, gauge of intimacy is one way of thinking about it.

The case for a relational approach is particularly appropriate to an understanding of information sharing with the state. In this case privacy needs to be a lens through which we systematically assess and construct our relationship to the state and becomes the cornerstone of a dynamic and progressive citizenship project. Because in order to be good citizens we need privacy as a space (to develop relationships, to forge our identities in the midst of different communities), but upstream from that we need privacy as a way of constructing the primary public relationship we are in, namely to other citizens and through that to the state.

Within the realm of this particular relationship with the state, it is clear that the terms of the relationship are in perpetual flux. How do we balance out the need for heightened security against the equally important need for anonymity? The need for cohesion and shared (basic) values against the right to express dearly held beliefs? The traditional, liberal response is one that throws us right back into the paradox outlined earlier. It isn't that the distinction between the public and the private isn't of paramount importance, but rather that our understanding of what makes up the private realm is undergoing enormous change. By arguing that there is a clear line between the public and the private, the rigorous toeing of which can allow us to uphold the principle of least harm, thereby ensuring allegiance to a minimal set of shared values and plenty of space for the private expression of beliefs. The fact is that that stark distinction between the two spheres is becoming inoperable – and while it remains valuable, it needs to be updated and re-examined in light of people's evolving allegiances, patterns of belonging and demands on the state (and vice versa). Privacy therefore is what will allow us to build the kind of relationship we want with the state in order to arrive at that balance. So privacy is not the result, but is the instrument with which to achieve and negotiate a better citizenship settlement.

What about the role of privacy with respect to the relationship between citizens? In many ways this relationship, with citizens whom we don't know, is mediated by the institutions of the state. As Claus Offe and colleagues suggest, shared institutions allow us to make assumptions about others and to pretend that we know others a little better than we actually do.[5] It is in the relationship that we each have with institutions that we can make a certain set of assumptions about each other and maintain that necessary illusion – that we share something with other citizens.

But, on another level, that relationship (between citizens) is also mediated by what else we know about each other, by the ways in which polls and statistics construct images of groups and of 'the other'. Our perceptions of others are fashioned by such information and its presentation: the number of immigrants who came to the UK and are planning to stay; the number of people entitled to UK citizenship who didn't take it; the number of recent arrivals being granted housing.

One of the key things that we may need to focus on in terms of our future uses of privacy is that we need privacy in order to build relationships. To create the kind of solidarity we need – the kind of civil society we need – it is paramount that we both construct institutions that foster cooperation as well as protect our capacity to relate to one another on the terms we choose. In this respect it means that cherishing the social means granting space for the personal, both in terms of what we expect of the people we know, as well as what we expect of more public figures.

This goes right to the heart of our notions of citizenship – it means that we need to embed a notion of privacy in the way in we choose to relate to others. Rather than use the concept of privacy as a way of marking out borders, I suggest that we use it as a way of asking questions about the kinds of relationships we want to build with different institutions and organisations. Rather than talk only in terms of our right to information and our right to privacy, and then to retrench behind the walls that spatial conceptions of privacy have allowed us to build (some of which for the better), let's use the opportunity to examine the terms on which we want to build some of the key relationships in our lives – be it to institutions or to other people. This is a subtle rather than a radical shift – it still leaves in place a combination of the two conceptions of privacy and private life that I outlined earlier, but it forces us to examine not the borders we want to cross but the sunny uplands we want to reach and on what terms.

Catherine Fieschi is the Director of Demos.

Notes

[1] M Hewstone, W Stroebe, GM Stephenson, *Introduction to Social Psychology: A European perspective*, 2nd edn (Oxford: Blackwell Publishers, 1996).

[2] A Ben Ze'ev, *Love Online: Emotions on the internet* (Cambridge: Cambridge University Press, 2004).

[3] Z Baumann, *Liquid Modernity* (Cambridge: Polity Press, 2000).

[4] GT Marx, ‘Seeing hazily, but not darkly, through the lens: some recent empirical studies of surveillance technologies’, *Law and Social Inquiry* 30, no 2 (Spring 2005).

[5] C Offe, J Elster and UK Preuss, *Modernity and the State: East and West* (Cambridge, MA: MIT Press, 1996).

2 Whose privacy is it anyway?

Zoe Williams

When we discuss privacy, we mean one of three things: privacy vis-à-vis the government; privacy within our families and social networks, between us and the people we know; and finally, privacy in relation to 'the public' – people who are distinct from us and our friends and not known to us personally.

This latter group falls under the category of 'cultural privacy', in the sense that it covers age-old tools of sub-legislative censure – shame, vilification and exclusion. It is private in the sense that, being sub-legislative, its catalysing event is almost always sex. You don't hear people talking about a breach of privacy when they're accused of fraud or corruption or indeed any misdeed that is fiscal or political. They talk about clearing their name.

In terms of the government, in this non-totalitarian state, talk of privacy invariably comes down to principles. 'I don't want to be monitored.' 'Why not, if you're not doing anything illegal?' 'Because it's the principle of the thing; I don't want the structures in place, should this *become* a totalitarian state; if I do nothing to defend these freedoms, I don't *deserve* these freedoms.' I over-use italics advisedly, here – most of this stuff is rhetorical.

This area really lends itself to great, persuasive theatrical sweeps; it reminds us of the oratorical bells and whistles of the last century, and we all feel a certain tingling in our toes listening to it, but it's not a going concern. A government that wants to invade its citizens' privacy can do so, no problem.

With or without ID cards, CCTV, the DNA database, a pliable civil service or a somnambulant populace, if there's one thing the last century taught us, where there's a will, there's a way. The surveillance impulse, like that of warfare, drives technology; it is not driven by it. So all the facilitating apparatus that is supposedly unique to our times will never pose as great a threat to our private lives as a government that's interested in the first place. And we know it.

We enjoy unprecedented privacy, and the way we fixate over small incursions is indicative of the freedom of retreat we have come to expect. For example, there was a brief scandal concerning Google and the search strings, in which it was discovered that you could, as a regular punter (albeit quite a computer-literate one) trace a person's Google searches, and in that way work out who they were, and what they were up to.

The example given was a man who had looked up 'vacancies plumbing San Diego', 'wife cheating private detective', 'divorce lawyer', 'revenge wife cheating', 'cheating bitch revenge', 'dating San Diego', 'care home Florida', 'sell rotivator'; from this, an acutely attentive neighbour or friend could pretty accurately identify this cuckolded fellow and plot the trajectory of his betrayal and recovery.

In case that didn't sound serious enough – a hypothetical example was then given: 'Baptist church Rochester New York', 'recipe cherry chocolate brownie', 'menopause symptoms', 'hot flush herbal remedy', 'sex toys female'; here, it becomes rather more problematic, since of course there'd be no forgetting who'd made the cherry chocolate brownies in a relatively small church, and the personal shame endured by the imaginary menopausal lady would be enormous.

But set these possible breaches against the vast potential for privacy that we now enjoy – the fact that you need never again be spotted buying a vibrator because you can buy one on the internet; the fact that you can seek advice on personal matters from internet strangers, where once you'd have had to rely on people known to you; the fact that you will never again be caught red-handed in a phone box; the rolling out of credit availability so that you can spend, undetected, as much as you want, and needn't be rumbled until and unless you bankrupt yourself.

Personal liberty, to pursue one's ends in total privacy, can only be absolute for those who have no meaningful social bonds. And yet, all day-to-day technological advances, alongside making life more convenient, also make it harder for us to monitor one another.

This is a natural enough progression, since the harder things are, on a practical level, the more we need to cooperate, and the more we will, by necessity, know about one another's business. The general trend, with consumer transactions getting easier and easier, and neighbourly cooperation getting less and less necessary, is towards anonymity. As is often the paradoxical way with our perception of risk, the harder it is to monitor one another, the more anxious we get about the possibility that someone might want to.

So, for instance, last year there was a minor, Radio 4-scale controversy about mobile-phone-tracking companies like Verilocation, whose number had really exploded since the software to track individual phones became available roughly five years ago. It was an open invitation to stalkers, claimed the consumer programme *You and Yours*, and it's true that if you did want to stalk someone this might be your first investment.

But never mind that these software programs only work with *consenting* phones, and never mind that most of us, however much we kid ourselves, have sufficiently predictable routines that the last thing a stalker would need is satellite capability; the obvious point is that, ten years ago, we could all locate one another geographically without even thinking about it, by the simple precaution of using a landline.

In every instance where we perceive our personal privacy to be under threat, all we need to do is ask ourselves what it would have been like a decade or two ago: almost invariably, the potential for secrecy has increased and not diminished.

Cultural privacy should be even less of a concern, and yet in the same way, occupies us irrationally. None of us holds any particular interest for those who don't know us. The sliding scale is as follows: for the extremely famous, every aspect of their lives is interesting to every possible observer; for the quite famous, it is interesting to a lesser degree, until you get to the bottom half of the alphabet, the M-list down, if you like, whereon personal details are interesting only if they relate in some way to the thing this person is famous for.

This being the case, our fear about our privacy in relation to this amorphous mass of 'public' is totally unfounded, since it isn't in jeopardy. Nobody, for example, wants to know about what I drink in a pub. There probably isn't an activity I could do that would interest the public that wasn't illegal, in which case considerations of privacy would have been trounced by those of the law. So, we claim to put a high value on cultural privacy, because to do so is to identify oneself with society's most successful strata, and yet, the only conceivable route any of us could take to ascend to that strata is by abnegating privacy altogether – deliberately seeking fame, which entails at least the promise of total self-exposure.

The showbiz metaphor for this is the starlet who gets on to the fame carousel by stripping, and then spends the rest of her career tracking down and exterminating images of herself naked. This tension, between pretending to value privacy much more highly than in fact it warrants, and in reality being prepared to jettison it in a heartbeat, for the higher purposes of fame, is most keenly felt and obviously manifested in the so-called Big Brother generation, the 16–24-year-olds whose attention is the holy grail for all media.

In a YouGov poll early last year,[1] a sample of 777 *Big Brother* watchers (these were actually younger than the standard age bracket, all under 20) were asked why they wanted to be famous, and which particular famous people they emulated. The answers were instructive: the vast majority were in it for the money and, while there was very little consensus on celebrity role models, nobody at all wanted to be Jade Goody and the largest single share (11 per cent) said Richard Branson. Nobody wanted to be Callum Best, or Abi Titmuss, or Tara Palmer Tomkinson.

Attention-seekers are universally derided, and yet we have totally dropped the notion that money is a dirty word, totally dropped the idea that pursuit of fame for the sake of cash is a cynical business. Wealth was once considered an undignified end, but it's a lot more dignified than its alternative, the youth of today point out, which is the indiscriminate pursuit of attention. And yet, fame, certainly in its reality-TV form, carries no guarantees other than attention, least of all wealth (some of them get rich, but they are very much the minority).

Handbag economics

It is interesting, given that so many other social taboos have been swept away – it is no longer *de trop* to be grasping, or selfish or money-grabbing, or even gold-digging; it is acceptable to be girlish or boyish, to refuse to grow up, to maintain the sartorial and behavioural conventions of a person 20 years younger than you, to idealise youth at the cost of rationality, to be vain, to reject maturation. And yet attention-seeking – which has traditionally been frowned on simply as a component of immaturity – is still disparaged, while the immaturity itself is embraced. Why would that be the case? Why should attention-seeking be singled out to retain its taboo? Precisely because its opposite, privacy, is prized, even while so few of us are in a position where our privacy is genuinely under threat, and of those whose is, most sought out that threat in the first place.

Partly, this is just an extension of handbag economics, wherein a ten-grand bag can look like a rat on a string, and will still be an object of lust purely because it costs £10,000 – this idea occupied ad executives in the 1970s, but has passed out of notice simply because it's such a no-brainer that to remark on it is unnecessary: a thing's desirability is in inverse proportion to how affordable it is, and furthermore, as an ironic gesture (I like to think), this thing is often made *less visibly desirable* to ram home the message that it's so expensive, you're going to want it anyway.

Celebrities are integral to this process of cranking up our handbag urges, since aspiration is a pretty coarse impulse, and doesn't appeal in the abstract: we need to see someone embody a lifestyle before we will aspire to it. Naturally, the one thing more valuable than the thing that is incomprehensibly expensive is the thing that is priceless. What do all celebrities always want? Privacy. It is the only thing whose lack unites them and yet excludes us. Everything else they can either easily afford or none of us can buy and there's already a Beatles song about how it can't be bought.

Sex

All of which takes us back to sex. If we are not privileging cultural privacy, and are simply aping celebrities, what are *they* doing? On certain, rather rare, occasions, it'll be about money, such as Catherine Zeta Jones and Michael Douglas's privacy, in their case against *Hello! Magazine*. Their aim was to set themselves up as a legal precedent in the protection of other celebrities' photo licensing agreements (in doing so the *Hello!* photographs disturbed the existence, and very lucrative, deal with *OK!* magazine).

A more obvious and representative case would be, say, David Beckham calling for privacy in the text-tapping with Rebecca Loos, when he actually meant 'stop telling my wife these things'. This was effectively a call for old-fashioned personal privacy within a family. But there's no honour in appealing to the public to keep your secrets from your actual wife. You appeal instead to an impulse, which (a) sounds as if it has a higher moral purpose and (b) seems to you to be universal.

During the thirteenth century, when the concept of defamation first featured in English law, privacy did have a moral dimension. The entire concept that one's reputation could be diminished in the eyes of right-thinking persons, and that anyone would consider this a bad thing, relies on the concept of reputation, and the existence of right-thinking persons. It relies on this Utopian notion (Moore's Utopia) that public shame is a useful and meaningful tool of control, and therefore, that privacy ought not to be invaded flippantly since, whether or not the misdemeanour was real, the forces of public censure were powerful, and not to be taken lightly, nor brandished disproportionately.

Nowadays, of course, such thinking is ludicrous – public censure is no longer a powerful tool. There is no such thing as a 'right-thinking majority'; there is pluralism; there is contrariness; there is no such thing as absolute right; there is scant notion of respectability. All this has been jettisoned by forces good and bad – most of them, it has to be said, good; a lot of civil control, of women, of the economically excluded, relied on disapproval to keep people quiet. On balance, I'd say we're better off without it. But the language of it remains attractive, since it lends dignity to privacy appeals which would otherwise be a whiny, self-justifying, 'don't tell my wife! It weren't me!'

The appeal for empathy, the notion that there's a universal urge for privacy which we all share, is another aspect of this bid for dignity, and is even more false – celebrities and their defenders always end with this: 'Everyone needs some privacy.' And we all nod along, because in colluding with it we become a little bit more like these golden gods, even while we are nothing like them, our needs are totally different, and if we were offered greater privacy, we would have no use for it, it would be like feeding grass to a mouse.

But just because it is ridden with sleight of hand and disingenuousness doesn't mean that debate around privacy has no meaning or value – indeed, it's probably the last arena in which we discuss our views on sexual morality in a meaningful and honest way. As such, it's the last bastion of morality, really, since everything else we have either abandoned or delegated to the legal system.

In conclusion, we've never had so much privacy in all the most meaningful ways. Daunted by the surveillance possibilities of modern technology, we forget how many surveillance possibilities our nearest and dearest used to have just by opening their curtains.

So we funnel essentially irrational anxieties into a wider fear for our privacy from the prying eyes of the world, and by a happy dovetailing, our celebrity ego ideals reflect those anxieties right back at us, at greater volume. It has no basis in reality at all. But I ought to add the rider, here, that I never had any sense of privacy in the first place, and will tell anybody anything.

Zoe Williams is a Guardian *columnist.*

Notes

[1] See www.yougov.com/archives/pdf/BRO050101012_1.pdf (accessed 18 Mar 2008).

3 Where everybody knows your name

Tom Ilube

The internet is great. It used to take me two to three weeks to gather everything I needed to steal an identity. Now I can get it done in two to three hours online.

This quote is from a fraudster, in a report commissioned by Garlik and produced by the research criminologists 1871 Limited. We hear a lot about the dangers of personal information being made available online, and we commissioned this report to try to gain some insight into what is really going on.

Two important messages emerged from the research, which illustrates the challenges that individual consumers face. With the proliferation of data, fraudsters have become all too aware of how easy it is to collate personal data online as it has become much easier than intercepting mail or rooting around in bins for old documents. This is great news for fraudsters as it is not even clear whether doing this 'personal information harvesting' is actually an offence in the UK.

The second message is that the 'identify theft industry' is becoming more organised. A federated, loosely coupled organisational structure is emerging, with two 'tiers'. There are people who specialise in personal information harvesting, searching online looking for likely targets, amassing their details and passing them on to the second group. This second group are the identity fraudsters, who use these packaged identities to fraudulently acquire credit cards, loans, fake passports, driving licences, benefit claims – and even to arrange sham marriages.

But while this all sounds very scary in theory, does it really happen in practice? How easy is it to acquire enough information about you to start to steal your identity?

The answers are yes, and 'very easy' – if you know where to look. In contrast to the average consumer who will be fairly ignorant of where their personal information is online, the average identity fraudster knows exactly where to find you.

Recently Garlik was asked to conduct a short exercise. A TV researcher selected a social networking user at random and pointed me in her direction. The lady in question had a pretty typical webpage – first name only, age, star sign, some general gossip and a few photos. Nothing, in short, that was particularly revealing. Within about an hour I had managed to collate enough about her that, had I been a fraudster, I could have sold her details on as a nice neat package ready for identity theft.

So, what had I done and what had I found? It is important to stress that explaining what I did will not reveal anything that either identity fraudsters or the authorities do not know already. The only people without this understanding is the target – you. It can be difficult to work out what warnings of 'identity theft' really mean, and how it happens. Perhaps if there were a greater understanding of what is possible, it would be easier to take steps to reduce the probability of being a target.

The lady felt she had been careful on her social networking page. No full name, no date of birth, no contact details. But this was a minor inconvenience. I noticed that the social networking site in question sometimes uses the user's full name ('firstname + lastname') in the website address (the URL) at the top of the browser. So, she had been careful but the site itself had given me a hook, a starting point.

I also knew her age and her star sign (because both were on her page), so I knew what year and month she was born in. Off to one of several genealogy websites that publish birth, marriage and death records of everyone in the UK (whether you like it or not) and after a few minutes of searching I had located her birth certificate details. That gave me her mother's maiden name too; very useful for proving you are who you say you are when talking to the high street banks and credit card companies who, despite the fact that it's publicly available online, still insist on using it as an important security word.

Armed with her full name and age it's over to the school reunion websites. Ah, there she is. An entry she put on one of those websites a couple of years ago and has neglected to remove even though after the initial excitement of being reunited with old friends she hasn't actually used it since. There she lists all her schools. She didn't move far, I can see the area she was born and the schools she went to on one of the online maps and they are all quite close.

Brought up a Catholic, too, I see, judging by the schools. All useful background context for the identity thief.

By looking at the electoral roll online it is also possible to get a sense of where she lives and works. Because she hasn't ticked the confusingly worded 'take me off the edited electoral roll' box I am soon able to find more details of her. Within a few hours information about her career, old boyfriends, where she works now and what she's thinking about her future are all downloaded.

But the problem to the identity thief is that none of this is tangible. Going into a high street store and trying to get a store card in her name won't work as they will ask for physical proof of identity, perhaps a utility bill or similar, and possibly a photo to prove it. I know her address so I could go round and trawl through her rubbish looking for an old bill. But I don't want to get my hands too dirty and I might get caught. Besides, she's probably got a shredder and uses it diligently, confident in the belief that she is thereby protected from identity theft.

However, have you ever looked at a utility bill? They tend to be standard A4 bits of paper. By using any utility bill, I can scan it, edit it with my details and within a short time I can create a near perfect utility bill. Finally I can go to one of several 'fake ID' sites to get a passable UK driving licence.

All that takes about an hour, and we have done several more tests of this nature. We find that if you stop people randomly on the street, collect their name, approximate age and star sign then on average for three out of ten people you can go on to collate enough information to take over their identity within an hour.

Moore's law of personal information

This ability to intrude into an individual's life using information found solely online is unprecedented and is a relatively recent phenomenon. Five years ago citizens did not face this situation. So what has changed in this period? The first is the rise of Web 2.0. Companies such as MySpace, Facebook, blogging sites, YouTube and Friends Reunited began to emerge in 2002 after the 'dotcom crash' of the preceding couple of years. This new wave differs from the first-generation Web 1.0 companies (Amazon, eBay and Egg) by being driven primarily by user-generated content. This means that the bulk of the content that makes up a Web 2.0 website is contributed by its individual users rather than the company itself. It might be pictures, an online diary, videos or just comments about a hotel you stayed at. The common thread is that it is all about what you say to the world.

Hundreds if not thousands of these sites, alongside perhaps 70 million 'blogs' (online diaries) have been created, relying on tens of millions of users publishing a deluge of their content – from pictures to videos.

The second point is the push towards e-government. The UK government in particular is striving to use the web to make services more accessible to citizens. One of the ways the government will do this is to make public sources of information readily accessible by making them available online. These range from millions of birth, marriage and death records, company directors' personal details, house prices, electoral roll and address records. That extends to planning applications, often with full plans of your house, plus your signature and mobile phone number – online, in the name of e-government. Recent analysis from Garlik estimates that in the region of 600 million individual records of personal information have been made publicly available online over the past few years in an effort by the UK government to be more accessible.

You could argue that all this information is already 'in the public domain', but there is a big difference between a piece of personal information sitting in a document in the local town hall and the same piece of information on the web available for inspection across the globe from West Africa to Eastern Europe at the click of a mouse.

With the fierce competition among Web 2.0 companies to expand their user bases and advertising revenue, and the continued drive towards e-government, this looks unlikely to slow down in the near future.

The third factor is perhaps the most important and that is the way in which personal information can be joined up to provide a level of insight into any individual that was not previously possible.

As you will have observed from the earlier example of how to collate a full picture of an individual online, it is the ability to tie together personal information from multiple sources, from public databases with user-generated and Web 2.0 content, that exposes us in a way that did not previously exist. It's all about understanding the relationships between the data. This is the world of 'mash ups', where one source of data is overlaid ('mashed up') with another source of data, to produce a new and interesting picture.

For example you can find out how much your local MP paid for their house by taking a list of all the UK MPs' home addresses and mashing it up with house prices and an interactive map of the UK. Sounds fun? How about if I do the same thing for you and all your friends and relatives? Is that harmless fun too? After all, the information is already 'out there', I am only combining it in new ways, as are companies dedicated to doing just this sort of thing.

In physics there is a phenomenon known as a 'phase transition'. After a period of time of heating a solid block of ice it will go through a transition and become a liquid. It's still made of the same particles but now it has different properties and needs to be handled in different ways. The world of personal information is undergoing its version of a 'phase transition'. There is so much personal information that has been made public on Web 1.0 and Web 2.0 and all of it can be knitted together in unexpected ways. A new environment has been created, which is profoundly different from what went before. And yet the current debate is often about applying or strengthening the 'old' rules in this new environment, without appreciating what has changed. In this new world of Web 2.0 we need to reconsider important notions such as privacy and identity to ensure that our understanding of them, in this new phase, still makes sense.

The King Canute strategy

We could address this new phase by adopting the King Canute strategy. We could go down to the water's edge as the tide of online personal information sweeps towards us and declare loudly, 'In the name of Privacy, we command you to stop!'

This approach is doomed to fail. Instead we must approach the challenge from a different perspective. We can assume that we are entering a world in which in five years' time there will be 10–20 times more personal information online about individuals than there is today. I assume that information will be combined, 'mashed up', in ways I can't even imagine at the moment. That is the world I expect to find myself in, whether I like it or not. It doesn't worry me, and it doesn't scare me. It's not better or worse than today's world.

It is just different – a different phase – and we need to be ready for it and learn how to thrive in that new environment.

Much of the debate emphasises the negative aspects of Web 2.0 – invasions of privacy or identity theft – yet there are many positive stories: rekindled relationships, opportunities seized and lives changed due to this new world of personal information.

I recently found my sister, after 30 years, who was lost to us in another country of over 20 million people. My search was founded on, and was only possible because of, some random personal information about me posted on a social networking site. As a result, lives have been changed; my children have met new cousins, my father has a daughter he thought he had lost forever and grandchildren he never knew, and I have completed a link in the chain of my life.

Staying private?

I don't bother to ask how I retain my 'privacy' in this not too distant digital world because I really do not know what 'retain my privacy' means. I do not seek 'complete power' or 'absolute control' over my personal information because I live in a real world of negotiation and navigation, not a world of black and white absolutes.

So the question I ask myself is this: how do I gain real power, for myself and my family, over my personal information in this digital world? In this new digital world, digital identity, the collection of personal information about me, a person in the online world, becomes as important as 'real world' identity. Who I am, what shape I am, and how big I am in the digital world really matters.

This is because others wanting to interact with me will make decisions and assumptions based on my digital identity. This is already starting to happen. When an executive is being recruited the company employing him will almost certainly 'Google' him to get a sense of what the world thinks of him. In social settings people check each other out online as a matter of course. Companies evaluate you continuously based on your digital profile. And as the amount of information mushrooms and combines in different ways, this will become standard and accepted practice.

So in many ways, however unfamiliar or uncomfortable a concept it may be, *promotion* will be as important as *protection* in this emerging world of digital information. How do you want to be seen by people who are looking at you?

As individuals we need help to understand this new world of personal information and we need tools, techniques and powerful levers to help us take advantage of it, to give us real power over our personal information, and what it means for us. Just as companies are emerging to extract and exploit personal information, so also companies are emerging to help individuals use their personal information to find that power.

Over the coming few years there will be large-scale initiatives aimed at consumers, specifically designed to give them power over their personal information. We are entering a different phase in the evolving digital world of personal information, not better, not worse, just profoundly different. The challenge for you as an individual is not to try to hold back the tide in the name of privacy but to learn how to swim safely, then jump right in and enjoy yourself.

Tom Ilube is Chief Executive Officer at online identity experts Garlik.

4 Drunken students, beauty queens and pole dancing

Peter Bazalgette

When David Cameron's brush with drugs at Eton was revealed last year he resolutely refused to comment. The leader of the Conservative Party and his well-drilled lieutenants justified their stance with a simple phrase: 'Everyone deserves a private past.' It was not long before another vice of the adolescent Cameron had been unearthed – his Oxford membership of the elitist Bullingdon club. There was the group photograph with boy David to prove it. He and his fellow peacocks were proudly on parade in their £1,000-a-head regalia.

Although we might all expect to be forgiven the odd youthful indiscretion, this was clearly thought by his advisers not to represent the required man-of-the-people image. And a Conservative well-wisher dealt with it rapidly by buying the copyright of the photograph so it could not be legally reproduced again. Of course, Cameron was at university in the 1980s, before the advent of MySpace, Bebo, Facebook and all the other confessional media that have mushroomed in the last five years. Imagine how different it will be for potential politicians of the future who are at school or university today. Take the New Jersey beauty queen, Amy Palumbo, who almost lost her crown when mildly suggestive photographs of her were lifted from her Facebook site. She had posted the images in the 'private' part of her entry, only for access to her accredited 'friends'. But one of them had a different view of what constitutes privacy.

The bulk of users employ their MySpace and Facebook entries for self-advertisement, social networking and the generally raw process of growing up. They are the first generation who can tell you precisely how many 'friends' they have. They are also the first generation whose sexual adventures, drug taking, immature opinions and personal photographs are shared electronically. Can you truly delete entries from social networking sites with the confidence they no longer exist on a server somewhere else? You cannot. And that is only your own entry. Typically the 'wall' on each site has more than a thousand 'postings' from other users – random, careless remarks recorded for posterity.

So we are a mere three or four years into a wholly new phenomenon: enabled by technology a generation is voluntarily surrendering its privacy on a hitherto unimaginable scale. I have carried out a highly unscientific straw poll of just one Facebook user. In a five-minute conversation I asked her for specific instances of personal revelation that might come back to haunt her circle of friends. Here are the results: photographs of marijuana smoking, naked runs and pole dancing… joining anti-women and anti-immigration groups and campaigns to save hereditary peerages (all ironic of course, but who's to know that in the future?)… extreme positions on Israel and Palestine plus leading a lobby to prevent the construction of a local mosque… sexual relationships, sexual conquests and declarations of sexual preferences… hobbies entered as 'drinking, whoring and fighting'… and so it goes on, the amusing and not-so-amusing social banter of students. Until, that is, it's dug up some years later and given the *Daily Mail* treatment. Already, the more astute employers are accessing this material to see what their applicants are really like. A survey last year revealed as many as one in five British companies are doing this. As are the authorities at Oxford University who, this summer, fined students whose personal photographs revealed their drunken antics at the conclusion of the examinations. The Facebook privacy settings had not guaranteed the confidentiality that the undergraduates casually expected.

There is some evidence that social networkers are beginning to be more wary about how much they reveal and there may well be landmark legal cases soon over 'friends' who behave more like enemies. Ashley Hurst, a media lawyer at Olswang, has observed that 'friends' who make free with Facebook images may be breaching the laws of both privacy and defamation. Facebook users may sign up to an agreement not to abuse the service, but the more dubious possibilities of social networking often prove irresistible. More serious still is the threat of identity theft. In August 2007, the IT security specialists, Sophos, demonstrated that 40 per cent of Facebook users will divulge personal information, such as email addresses and dates of birth, to complete strangers.

But voluntary, self-advertisement of personal details is only part of the story. 'Cyber bullying', where humiliating practical jokes and lewd exposés have been visited on teachers by pupils with video-enabled mobile phones, was condemned by the last education secretary. It was treated as an issue of bullying and backed up by a report from Goldsmiths College for the Anti-Bullying Alliance.[1] This set out seven methods of technological taunting that school children execute against each other, including text messaging, emailing, instant messaging and so on. But in reality this is a further privacy issue. The Italian government took action following a spate of similarly distressing incidents. Among these was the filmed bullying of a disabled child and the sexual harassment of a female teacher. Mobile phones are now banned in Italian schools. The British reaction has been to appeal to platforms to prevent the posting of such materials on the likes of YouTube. Either way, as users find ever more ingenious ways to employ their gadgets, society is several steps behind in its response.

Two interesting issues arise from this explosion of personal electronic traffic, either of which could necessitate a re-examination of the thinking that lies behind our privacy laws. First, is there a fundamental shift taking place in attitudes to privacy? Whether led or merely enabled by the technology, is the famous 'right to be left alone' becoming outmoded? If so, there would be profound implications for public policy. And second, even if this generation has a new attitude, what if they later change their mind? Could their consent subsequently be withdrawn, or are the relevant technologies becoming uncontrollable? The internet, CCTV, DNA, biometrics and digital camera mobiles now constantly challenge our historic expectation of privacy.

I became aware of a possible shift of attitude when examining the furore that originally surrounded the television show, *Big Brother*, which my company produces. The second country ever to stage it, in March 2000, was Germany. Beforehand the press made much of the 40 cameras and the 24-hour surveillance of the housemates. Catholic associations said *Big Brother* displayed a contempt for humanity. Politicians declared that it violated the articles of the country's constitution, protecting human dignity, and called for a ban. Television regulators took this as their cue and prepared to shut the production down, on the grounds that it infringed the right to privacy (for 'free development of personality') enacted in the German constitution in 1954. But in the event they allowed the show to go ahead. Despite the association of lack of privacy with fascism they recognised a crucial difference – these young people were consenting to the process.

As the television 'reality' format spread from country to country the same cultural conflict arose between the older and younger generations. Self-exposure by a generation seemingly relaxed about nudity was shocking enough in itself, but the public display of general, everyday social intimacies seemed even worse. In Italy Cardinal Tonini, a senior figure at the Vatican, said that videoing people, 24 hours a day, was like stealing their souls.[2] He particularly objected to the diary room being referred to as the confessional, something that should be private between the individual, the priest and God. In the US President Clinton attacked *Big Brother* in an interview with ABC News. When reminded that certain intimate events in his own Oval Office had become public he retorted: 'That's the problem. Privacy should be protected. My lack of privacy is a direct result of my position as President. But privacy shouldn't be auctioned off to the highest bidder. These people are prostituting themselves to media conglomerates. It's very troubling.'[3]

It was less troubling to Tim Gardam, the programme director at Channel 4 who originally commissioned *Big Brother* for the United Kingdom: 'In all its raunchiness it revealed the truth of a generation. It was the first programme that really laid open what all the marketing research, all the demographic research, all the cultural research was saying. You had a generation which was fundamentally different from generations before. They had no sense of propriety, no sense of modesty. They were open, honest and candid with each other.'[4] This is a trend also identified by Jonathan Freedland in the *Guardian* in 2002:

> *If we think hard about privacy, and ask what has really made it as endangered a species in modern Britain as courtly romance or stiff formality, the answer does not lie only in the realm of surveillance and monitoring. It's also about a cultural change, in which modesty, reserve and discretion – those sentries of privacy – have come to seem like values which are quaint or even vaguely repressed… Big Brother is watching us, to be sure. But we are also inviting him to take a look.*[5]

If there has indeed been a cultural shift in attitudes to privacy then it is not one that our middle-aged regulators and opinion formers have thus far picked up on. In fact, with assistance of the Human Rights Act and the judiciary, the laws on privacy have been considerably tightened up in Britain over the past decade. Recent legal victories by the likes of David Beckham and Naomi Campbell attest to this. And the ethics of privacy are being much more closely attended to than ever before in such fields as medical records. But if there were to be a genuine, permanent shift then it would paradoxically predicate a relaxation of privacy laws – society would actually place less importance on privacy in the future. This deserves investigation. It may be, on the other hand, that the events I have chronicled are mere youthful exuberance given currency by new sorts of technology and that today's carefree *Big Brother* housemates will become tomorrow's stern television regulators.

To try to gauge how this generation feels about privacy I commissioned the market research company YouGov to carry out a simple survey of attitudes to privacy.[6] Table 4.1 shows the questions they asked and the responses they received from a sample group of 2,274, divided into five age categories.

What can we conclude from this? That the population as a whole remains very concerned about privacy and easily values it above qualities such as freedom of speech and open access. You can also see that, while 18–24-year-olds prize freedom of speech rather more highly than older generations do, even within their own peer group privacy plus harm and offence rate well above freedom of speech and open access. So, despite the carefree enthusiasm with which some of the younger generation exploit social networking technology, when confronted with some of the dangers they are almost as concerned as older age groups.

I interpret this as a group that loves the powerful social networking that is now possible, but still has a clear sense of privacy. It relates less to a blanket desire for anonymity. We have seen from *Big Brother* that they are often happy to expose their relationships, or indeed their flesh. But they have chosen to do this. My impression is that their idea of privacy is that it should be available if they want it. Some might argue that if you flaunt your private life you surrender your future right to privacy. I disagree. To be attracted by self-exposure at a relatively early age does not mean you have no future right to privacy. You should be able to change your mind. Indeed,

Table 4.1 **Misuse of mobile phones and the internet have been in the news recently.**
(a) Considering the way that digital technologies such as phone cameras and sites like YouTube or MySpace are run, which of the following do you think should be the MOST important consideration?

	Total	18–24	25–34	35–44	45–54	55+
Privacy	**33**	31	33	29	31	36
Freedom of speech	**11**	18	18	10	10	7
Avoiding harm and offence	**43**	31	36	45	48	47
Open access for all	**6**	13	6	7	4	3
Don’t know	**7**	7	7	9	7	7

(b) And which of the following do you think should be the second MOST important consideration?

	Total	18–24	25–34	35–44	45–54	55+
Privacy	**33**	27	29	32	36	35
Freedom of speech	**20**	23	23	22	15	18
Avoiding harm and offence	**30**	27	31	26	30	32
Open access for all	**8**	12	9	9	9	7
Don’t know	**9**	11	7	11	10	8

Source: YouGov

with the way in which social networking is exploding in popularity among the younger generation, it is essential you be able to change your mind. The teenagers chattering away online are media literate, but they are not media wise.

How then should platform owners and legislators respond to this new situation? We are only in the second decade of the internet. The first saw the economic euphoria of the dotcom boom, later replaced with a somewhat more realistic view of who the financial winners and losers were. This second decade is witnessing a social euphoria instead. We are now astonished and excited by the social networks made possible by the World Wide Web. But it is time for this second wave of enthusiasm also to be tempered with a more sceptical attitude, one that would tie in with the results of the YouGov survey. A 2007 report from the Royal Academy of Engineering argues that the collection, storage and processing of personal data can be of great benefit, but that users' privacy needs to be protected.[7]

The Royal Academy of Engineers believes that many more safeguards could and should be designed into new technologies to ensure the integrity of our personal information. They are mostly concerned by identity fraud and the ease with which felons can gather, steal and abuse our personal details. But the development of the semantic web now provides a different threat. This is the means by which a trawl for information about an individual, held in many places, is assembled and presented as one coherent and convenient collection of data. Facebook announced in September 2007 that a listing on their site would be verifiable via search engines such as Google. In what sense have social networkers consented to this aggregation of data? Can consent for such dissemination be meaningfully withdrawn or the data deleted? This will become a major issue for personal privacy going forward. The 1998 Data Protection Act was guided by eight principles of good data handling, one of which was that data should not be kept longer than necessary. This is a precept marked more in the breach than the observance.

The Royal Academy recommends harsher penalties for those who flout the Data Protection Act. But prevention must be better than cure. So social network hosts need to develop new protocols to allow effective withdrawal of consent. The legal rule up to now, once consent has been granted, is that it is irrevocable. But this is a principle we will need to question in the future. And although we regard the internet generation as media literate, this is an area where it is looking increasingly naïve. So there is a need for greater education and awareness among the social networkers. Their instinct for candid revelation needs to be informed by the realisation that the results might be ineradicable. There is currently a lot of laudable work being done to prevent online child exploitation. Organisations such as the Child Exploitation and Online Protection Centre with their site www.thinkuknow.co.uk,[8] are working to improve the safety of young people from sexual predators. We now need to extend this sensibility beyond the specific area of child abuse.

A vast amount of work is being done outside the sphere of social networks to guard privacy. The National Health Service is currently piloting schemes where individuals have to consent to their medical records being made available for research. The new Human Tissue Act also covers the illegal gathering of information, prohibiting the analysis of someone's DNA without their consent. In time these systematic checks and balances may need to be adapted for the social sphere.

European regulators are now pressing Google, Microsoft and Yahoo! on their privacy policies. The companies have been keeping data for up to two years. They are being asked to reduce this substantially, despite the financial pressure on them to record and monetise the traffic they attract. Here the Royal Academy of Engineers' report has some interesting suggestions:

> *Postings to websites might be automatically destroyed after a certain period of time, unless the end user confirmed they wished to have the material retained. Postings to certain services could have an automatic delay before the material was made available to ensure a 'cooling-off' period between posting and publication.*[9]

The report goes on to float an even more intriguing suggestion:

> *Research could be pursued into the possibility of using Digital Rights Management technology to protect personal information… Applying this technology to information posted on the web could allow information to be posted for limited amounts of time, or would allow information to be publicly available on the web but not copied by others – meaning that the author of the information had control over the amount of time for which it was available, and could also rule out the possibility of the information being altered. Thus it could be used to protect the authors of blogs and the users of social networking sites.*[10]

In summary, when considering electronic privacy we should now include social networks in our policy making. We need to monitor the attitudes of users – the 'self-advertisers' – in more depth to see if they are truly more open and less private than previous generations. The initial evidence is that they still have an innate sense of privacy. If so, social networking needs to be governed by the same body of law, custom and practice that is developing to protect privacy elsewhere. The key elements would be to increase media literacy, enable the withdrawal of consent and ensure that obsolete data can be effectively deleted.

Peter Bazalgette was formerly Chief Creative Officer at Endemol and is a non-executive director of YouGov.

Notes

[1] See www.anti-bullyingalliance.org.uk/downloads/pdf/bullying&community_briefing2007.pdf (accessed 1 Apr 2008).

[2] See www.dw-world.de/dw/article/0,,1082665,00.html (accessed 20 Mar 2008).

[3] See www.thestage.co.uk/features/feature.php/7504 (accessed 5 Mar 2008).

[4] Quoted in P Bazalgette, *Billion Dollar Game: How three men risked it all and changed the face of TV* (London: Little, Brown Book Group, 2005).

[5] See www.guardian.co.uk/uk/2002/sep/07/privacy.jonathanfreedland (accessed 5 Mar 2008).

[6] See www.yougov.com/archives/pdf/BRO050101012_1.pdf (accessed 18 Mar 2008).

[7] Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of technological change* (London: Royal Academy of Engineering, 26 Mar 2007), available at www.raeng.org.uk/policy/reports/default.htm (accessed 2 Mar 2008).

[8] Website accessed 3 Mar 2008.

[9] Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance*.

[10] Ibid.

THE PUBLIC'S PRIVATE LIVES

5 Being watched

Peter Bradwell and Niamh Gallagher

In the song 'What's he building?',[1] Tom Waits' compulsive drawl obsesses over the behaviour of his reclusive neighbour. 'What's he building in there?… What's he *building* in there?' he repeats. Waits is playing the everyman, his suspicions piqued by the solitude and eccentricities of the guy next door. 'We have a right to *know*,' he implores, offering a typically biting comment on the fragility of neighbourhoods, the paranoia of a thousand households sharing the same postcode. On one level this is just the curtain twitching of traditional suburbia. But the way that identities and communities form and hang together makes such pointed curiosity, today, acutely relevant.

Shutting the door, drawing the curtains, disconnecting the phone, deleting the files and stashing the diaries – the realm of the private is at once comforting and essential. But the scent of the illicit or illegal is never too far away. In the connections between 'closeness' and affiliation with each other there sit expectations about what we want, or are entitled, to know of other people, and vice versa. The way we talk about privacy can tell us a lot about our social fabric, yet it is often seen as 'merely' a civil liberties problem, a predictable whine of the chattering classes or paranoid libertarians.

Here, we argue that privacy is far more than a problem for the individual, and that thinking in terms of 'Big Brother' misses important aspects of the privacy problem in light of how both the private sector and public services work. But Big Brother still tends to frame how we think of privacy. This does little to counter our deeply ambivalent attitudes to privacy. Our newspapers almost weekly cry Big Brother, traditionally referencing government surveillance but, in the more recent past, 'exposing' the databases that lie in the hands of the private sector. Seventy per cent of those surveyed for the Oxford Internet Surveys said going online puts a person's privacy at risk.[2] But still we shop online in increasing numbers. Around half of all households in the UK have a Nectar card. We still travel to the US despite EU–US passenger information sharing agreements, and border control fingerprinting.

This chapter will focus on why we think privacy is an important aspect of both private sector efforts to improve customer convenience, and public sector reform, specifically in the context of 'personalising' services. We argue that we need more democratic rules on personal information use, and to do that, we need a much better understanding of people's attitudes to privacy, and of organisational uses of people's information. We will then draw on focus groups designed to explore how and why people value privacy, and from ongoing research into personal information and public services.

Barry Schwartz argues in 'The social psychology of privacy' that 'weak social relationships, or relationships in the formative stage, cannot endure the strain of dissociation'.[3] This resonates in a world in which globalisation has enabled more far-reaching migratory flows, and in which there have been much talked about changes in the role of traditional associations such as class, race, nationality and political party. The new ways we engage with the world around us have changed how we come to decide who we are, what that means, and what we should and should not do as a result. The reference points of everyday life have changed, making our sense of who we are more fraught and placing more emphasis on the moments at which we work out who we are in relation to other people.

That makes privacy intimately connected with identity. As a result of these changes, we live, more than ever, through *being watched*. The means for self-determination – through which we compulsively seek the recognition that stakes out our social status – are predicated on our being seen. In an increasing number of contexts, from the associative clamour of Facebook through to the comprehensive profiling of supermarket loyalty card schemes, our interactions with people and organisations are predicated on their knowing about who we are and what we like. This is not a one-way relationship – the readiness to embrace social networking sites, the fascination with celebrity lifestyles, and the (possibly dwindling) love affair with reality television suggest an obsession with display. Being watched in this way is something we are, seemingly, often comfortable with – a function of our need for the recognition it affords.

But to say that we live through being watched does not mean that privacy is dead. Privacy still matters because it provides the space to withdraw from the gaze of others and to rest from the need to perform socially. Moreover, it matters *politically*, and democratically, because it is intimately connected with how we are seen, represented and treated by the people, organisations and institutions that hold influence and power over us. It grows in significance, but becomes more difficult to control, in an era in which identities form along unpredictable lines, with unpredictable consequences, and where the state has less of a claim to influence, determine or manage them.

Being invisible

The Invisible Man, by HG Wells, weaves a story of the seductive nightmare of becoming invisible. The blessing of being absented from the gaze of others quickly gives way to madness, as the invisible man recalls: 'I went over the heads of the things that a man reckons desirable. No doubt invisibility made it possible to get them, but it made it impossible to enjoy them when they are got.'[4]

Absolute privacy is to disappear, to mean and be nothing. It is one, but not the sole, form of invisibility. In Ralph Ellison's *Invisible Man*, the central character is subject to a different kind, resulting not from the active choice to disappear: 'I am an invisible man… because of a peculiar disposition in the eyes of those with whom I come into contact. A matter of the construction of their inner eyes, those eyes with which they look through their physical eyes upon reality.'[5]

He is speaking of the experience of a young black man in 1940s America. Whereas Wells writes about purposefully removing oneself from the gaze of others, Ellison deals with the differences in power that influence our ability to define who we are and what that means. His invisible man suffers from the indignity of being seen through, of being put in a place and judged, a place where his right to dispute, to engage and to negotiate is non-existent. His privacy becomes both meaningless and absolute, in the face of persistent and entrenched discrimination.

Ellison reminds us that privacy is not just about whether someone sees you – it is about *how* they see you.

In the context of the contemporary 'personal information economy', this is increasingly significant. We traditionally frame threats to privacy as threats to something tangible and fixed that is being eroded by, for example, new technology used by a malevolent panoptic conspirator – a 'Big Brother'.[6] But the discriminatory profiling that so much of modern life is reliant on is not captured in this traditional outlook. That is because, first, it misses our contemporary willingness, and need, to be 'on display'. Second, it misses the nature of discrimination, not carried out by a single authoritative force, but as a response to the need to sort and manage a population with complex and fluid identities. Peculiarly, the *absence* of Big Brother, in the traditional understanding, has contributed to surveillance, largely through digital profiling, being a centrally important feature of everyday life.

This condition of being watched and needing to be seen has changed what surveillance means, and it changes how we should approach privacy. The reliance on databases of information, and on our need to be recognised, structures our everyday lives.

In *addition* to guarding against the transgressions of large information holders – which remains an important task, encompassing governments, international organisations and businesses alike – we need to also focus on the many different arenas in which we are sorted and distinguished from each other. That means assessing the relationships between the watched and the watcher, relationships often marked by significant differences in power.

This suggests some key questions for the contemporary privacy debate:

- How can the practices of public institutions and the private sector differentiate the people they see as users, citizens or collaborators?
- How can they alter their services accordingly, and what are the consequences?
- How can these practices be made open and transparent, and why should we do so?

Who wants to know?

These questions are important ones not only to policy makers, but to people, something underlined by the focus groups we organised to support this collection.[7] The meaning of privacy might have changed, but the idea still holds emotional and personal force for teenagers and the elderly alike.

There's this fixed idea that government needs information for something evil, and if there's computers involved they always mess it up.

But if you've done nothing wrong you shouldn't mind giving it to them…

But it's private.

Participants in focus groups, June 2007

The things people considered private in our focus groups could broadly be split into two types. One was deeply personal: our relationships, our homes, our bodies and our possessions. The other was seemingly less personal: the services we use and how we use them – bank details, shopping habits, internet. These distinctions hold the key to understanding attitudes to privacy. Some of the confusion mentioned above can be put down to a lack of transparency in how information is used, who has access to it, and why they want it. But, importantly, any lack of transparency is compounded by changes in the distinctions between what is private and what is public. That complicates the lines we draw between the most intimate elements of our private realm, and the more extraneous pieces of information – such as our shopping habits, where we like to spend time, what we read and watch.

There are three aspects to this. First, it can be difficult to work out when and where we are being watched. There are new spaces in which our behaviour and information can be seen, and, therefore, judged. Being 'in private' while we are being watched – for example, while we drift across the internet – is partly a function of the rise of new technologies, intensive data collection by private companies and a government 'surveillance' culture. It means we experience new situations in which people can come to a decision about who we are. We find ourselves being watched through the logging of our behaviour online by internet service providers, or search engines, from the apparent privacy of our homes. Second, it can be difficult to work out the consequences; the paths our information follows are often opaque, and the precise role of the information holders can be difficult to grasp. For example, how can we be sure about where our passenger information goes when we enter the US? Who gets to see information about my behaviour on a website – what I buy, or how long I spend reading what, for example – and what do they do with it?

Context and *choice* are central in people's attitudes to the handling of their personal information; knowing when, where and how information is being used is the first step to making a judgement about how appropriate it is, and what can be done about it. But these changes to who is responsible for what, and to where we are seen and, potentially, under surveillance make that context more difficult to understand. So, when does being watched matter, why, and who decides?

'It's one thing to be watched, but it's another to be logged,' one focus group participant told us. The step from surveillance to categorising and profiling is a short one, if it exists at all, and yet the implications are crucial. David Lyon, elaborating on the significance of being seen, argues that 'human life would be unthinkable without social and personal categorization, yet today surveillance not only rationalizes but also automates the process'.[8]

The way these profiles are used not only describes the social terrain but, in turn, helps to sustain it through the structuring of organisations' responses to the needs, tendencies and interests of those profiled. David Lyon continues: 'Surveillance sorts people into categories, assigning worth or risk in ways that have real effects on their life chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice.'[9]

But, still: so what? If the price of surrendering more information is a service better suited to my needs, should I care? Altering the response to or service for people according to a profile of 'who they are' is not necessarily a bad thing. However, it becomes problematic, and leads to the 'deep discrimination' when we ignore the social context in which these profiles emerge. Sorting may be automatic – through the groupings and associations of customer relationship management software, for example – but the categories into which people are sorted are constructed, imbued with meaning and social implications.

We will look now briefly at two spheres where the everyday surveillance of personal information gathering and use is most prevalent – the retail industry and the public sector. Each tells us something about the level of control, choice and power we have over the profiles built about us. And both relate to how profiling not only offers choice, but also shapes our behaviour and experiences.

Our argument is not that the 'information' or surveillance society is necessarily *dis*empowering. Instead, we argue that thinking about privacy means finding ways to build democratic principles into information use, and to assert the power of individuals in their relationships with other people and institutions.

Customer convenience

The private sector, and perhaps most visibly the retail sector, rests its work on its ability to categorise people effectively. Through our willingness to provide them with the information they need, we are complicit in this process. People are usually inclined to share information if 'there's something in it for me' or 'if it makes my life easier', allowing supermarkets, department stores and online companies to develop enormous databases of information – charting individual and family habits, tastes and behaviours. We are nothing if not segmented.

The compelling pull of convenience helps to drive the growth of these databases. The private sector combines a sense of what the information is for with convenience: in the succinct words of one of our focus group participants: 'It gathers your information so it can offer you a better service.' It builds trust and business, while simultaneously categorising its customers and 'tailoring' its service to their needs. But this convenience operates as the product of surveillance only in particular circumstances – here, when the aims and context of a transaction or exchange are apparently clear, control is seemingly not exerted, and prejudicial judgements are apparently not made. The private sector, as it gathers information about customers in exchange for rewards, therefore emphasises the individual's *choice* and *consent*. It passes little comment in return.

But that hides some important problems with profiling in the private sector. First, there is a potential 'narrowing' of our experiences. For example, newspapers may choose to market to one group or the other, but not both; at the same, there lies an increasing potential for people to construct a personal cultural diet – with implications for how we live together and feelings of mutual belonging and responsibility. Second, the private sector does not have to address the value of people's decisions, or the social context that shapes them. Further, there is a risk in the longer term that as private and public roles merge, that information from our everyday lives is used to make important decisions we would not have anticipated – decisions that will deepen inequalities of access, aspiration and outcomes – involving, for example, increasingly targeted financial options for those on a lower income.

Personalising public services

Our great ambition now: a National Health Service that is also a personal health service.

Gordon Brown, Labour Party conference speech, 2007[10]

Where the private sector has built its work so successfully around the use of personal information, with the, sometimes tacit, consent of the public, a variety of factors have held back the public sector – with technological incompetence, a lack of clear strategies around joined-up working and technology, and concerns about privacy and responsibility among them.

Despite public concern both at government capacity to operate technological systems, and suspicions of government propensity for surveillance, the government is working to develop its IT systems to support secure and effective information sharing. Connecting for Health is perhaps the most visible example – a £12.4 billion project to develop nine major systems that will help doctors and the health system share their records, and make their service more efficient and 'personal'.[11] Choice and control, key words in discussions about privacy, echo the past decade of public services policy development in the UK, sitting comfortably with the rhetoric of empowering citizens and putting the 'user' in control. They are particularly prominent in the concept of 'personalisation' – an idea at the very heart of New Labour's philosophy of public services. Personalisation, broadly, means tailoring how a public service works to the needs of the individual.

Charles Leadbeater, writing for Demos in 2004, outlined five different meanings of personalisation, each becoming more radical in its implications for services.[12] The first two simply require an improvement in customer service among public service providers; the third gives the same users a more direct say over how their money is spent; the fourth has users as co-producers and co-designers of a service – allowing their active participation in service design and provision. The fifth and final possibility –

'self-organisation' – allows the public good to emerge from within society through the way public policy shapes individual decisions.

But what are the implications of personalised services for privacy? Like in the private sector, personalising public services is based on tailoring the offer based on respect for the needs of the individual. But Leadbeater identifies the bind faced by the state: 'Committed to protecting, even expanding, the sphere of private freedom it also is necessarily committed to shaping continuously, how people use their freedom in the name of public good.' This subtle tension between individual responsibility and state advice and support is increasingly important.[13] In order to offer support to its citizens, government requires a level of information; but however it chooses to use that information to respond to certain groups it is making a *political* decision. The relevance of our choices, behaviour and relationships grows as they are recorded, cross-checked and contextualised. In the way that it develops personalisation, it therefore embodies a particular model of the role of government in influencing our behaviour or deciding what support we need.

The last three types outlined by Charles Leadbeater call for a rebalancing of the relationship between the citizen and the state, and are based on a dialogue between both – involving sharing certain pieces of personal information (thus relinquishing control), in exchange for better services. Personalisation, in the more *radical* sense, is not about the state categorising people and then providing what it perceives them to need. Instead, it is based either on inviting users to be co-producers and co-designers of their services, or on empowering them more directly with resources and the support to use them. Both of these approaches see users as experts, bringing knowledge, skills and experience that even the best-intentioned providers cannot supply. An exchange of information – based on ongoing dialogue between user and provider – is transparent, and aims to build a sense of user-ownership of services.

It is this political decision that can get lost in the justifications of risk reduction and efficiency, and in the segmentation practices of the private sector. Each of the models of public service reform offers differing implications for privacy in the way they embody different perceptions about the role of government.

Many of the questions surrounding privacy have not changed: where, and on what basis, am I being judged, and why? Gathering information, sharing it, and using it to inform decisions or behaviours is not a neutral act, nor is it simply a question of administrative efficiency. The key to answering these questions lies in acknowledging that the process of segmentation is discriminatory. Privacy is not just about the politics of curtain twitching, but plays a central role in understanding how to make for wider-spread democratic engagement in the systems and institutions we live through and encounter.

Peter Bradwell and Niamh Gallagher are researchers at Demos. This chapter is drawn from their Demos pamphlet FYI.

Notes

[1] Tom Waits, 'What's he building?', Mule Variations, 1999.

[2] WH Dutton and E Helsper, *Oxford Internet Survey 2007 Report: The internet in Britain* (Oxford: Oxford Internet Institute, 2007).

[3] B Schwartz, 'The social psychology of privacy', *American Journal of Sociology* 73, no 6 (May 1968).

[4] HG Wells, *The Invisible Man* (London: Penguin, 2005).

[5] R Ellison, *Invisible Man*, 2nd edn (New York: Vintage, 1995).

[6] C Bennett and C Raab, *The Governance of Privacy: Policy instruments in global perspective* (Cambridge, MA: MIT Press, 2006).

[7] In June 2007 we ran four focus groups, with groups split by ages bands of 17–25; 26–35; 36–45; and 46+.

[8] D Lyon (ed), *Surveillance as Social Sorting: Privacy, risk and digital discrimination* (London and New York: Routledge, 2002).

[9] Ibid.

[10] See http://news.bbc.co.uk/1/hi/uk_politics/7010664.stm (accessed 27 Feb 2008).

[11] See www.connectingforhealth.nhs.uk/factsandfiction/ mythbusters/ the-cost-of-the-national-programme-for-it-is-spiralling (accessed 27 Feb 2008).

[12] C Leadbeater, *Personalisation Through Participation: New script for public services* (London: Demos, 2004).

[13] See, for example, C Leadbeater, J Bartlett and N Gallagher, *Making it Personal* (London: Demos, 2008).

6 A place of greater safety? Information sharing and confidentiality

Perri 6, Chris Bellamy and Charles Raab

[Soldier guarding the National Convention] '… can we offer you an escort, Citizen Deputy, to a place of greater safety?'
'The grave,' Camille [Desmoulins] said. 'The grave.'[1]

In Britain and in several other countries in recent years, the pursuit of greater safety has informed policy in growing numbers of fields. Improving probabilities of detecting crimes, achieving early intervention to prevent crime and reduce criminality, providing greater reassurance to anxious citizens that everything possible is being done to protect children, preventing people with the most serious mental health problems becoming a danger to others, ensuring that future violent and sexual offenders are monitored carefully, managing anti-social behaviour and the like, are goals of increasing importance to policy makers. Indeed, systematic risk assessment is now required in many fields, including those where people are considered to be a danger to themselves, as well as those where they present risks to the wider public.

The language of risk is now ubiquitous. In care for frail older people, for example, 'risk assessment', and not just the assessment of needs, is now routine in order to identify those who are susceptible to falls. In British public policy, the key to promoting safety is now the encouragement, through legislation, national policy guidance and a plethora of model protocols, of the sharing of personal information between agencies providing frontline services.

At first sight, it might seem surprising that information sharing should be thought the highway to safety. For sharing information carries no guarantee of its being acted on, still less of its being acted on appropriately. Indeed, for all that it has become commonplace to describe the horrible death of Victoria Climbié as a failure of information sharing, this is factually incorrect. In her wretched case, the relevant information was shared about Victoria's injuries, but in a form that failed to alert those who should have been alerted to her plight, or to draw the correct inferences from the information.

Similarly in the case of Ian Huntley, who killed two schoolgirls in the Cambridgeshire village of Soham. Information sharing may well have had a lesser significance for his employment as that village's school caretaker than is commonly thought. Information was not retained in the intelligence systems of Humberside police because the allegations against him were insufficiently evidenced to enable charges to be laid – let alone for the Crown Prosecution Service to advise that any be taken forward. Most of the cases did not concern children below the age of consent.

Nevertheless, ministers and many policy advisers remain firmly of the view that the sharing of more information about those classified as either at risk or else as presenting a risk will provide the critical infrastructure for more effective public protection. A central aspiration in policy has been, therefore, to remove blockages to the sharing of information. Chief among the barriers to information sharing, policy makers assume, is the widespread misunderstanding of the Data Protection Act 1998, which, when correctly understood, by no means prevents sharing where it would generally be warranted on public interest grounds.

Ministers' public statements typically present the issue of information sharing as one to do with finding a better 'balance' between effective inter-agency working and client confidentiality. In fact decisions about information are rarely matters of 'balance' at all. A decision whether or not to share information is taken precisely at the point where, by definition, no public service holds all the information that might be made available. That means decisions involved in sharing enough information to judge whether pooling it would be wise commit the service to one course of action. These are in fact dilemmas requiring a choice and a judgement, not problems calling for some judicious mix of sharing and confidentiality.

The dilemma is this. Any decision rule that would err on the side of avoiding the risks associated with not sharing information in a particular case, will sooner or later err on the side of sharing information – and perhaps of acting with inappropriately draconian intrusiveness – when in fact the person is not at risk. Indeed, it was only a decade before Victoria Climbié's case that social workers were excoriated for taking children into care in Orkney and Cleveland as a result of sharing information that had been wrongly interpreted to indicate high risk.[2]

The call for greater information sharing is not confined to contexts such as child protection and mental health where it may be shared on a case-by-case basis. The Labour government's programme also calls for greater 'bulk' sharing, or routine access by public service agencies to at least some of each other's information about clients – for example to check entitlements to service, to complete risk assessments or to cross-match records to detect possible cases of fraud.

Four public service contexts

It can therefore be said with some confidence that questions about information sharing between public services constitute some of the most difficult and urgent privacy challenges of this decade. Yet safeguarding privacy, understood as a human right, is not the only, or even the most pressing, reason for which we might care about confidentiality.

Confidentiality is often a critical means to the pursuit of service goals. For example in fields such as mental health, substance abuse and sexually transmitted infections, a strict confidentiality regime is necessary to persuade clients to present themselves and to be candid with professionals. In many human services, confidentiality protection helps to prevent stigma and to preserve employment and social relationships that may be critical to achieving service goals. In still other cases, agencies may worry that sharing information may lead another agency to take inappropriate action because they may fail to appreciate its full and proper context.

Sharing information often presents the greatest difficulties of principle when the decision to be made concerns sharing between services with different types of purpose. Table 6.1 shows some of the basic types of services between which sharing often raises the most fundamental operational problems, and sometimes ones of principle, too.

Table 6.1 **Four pure types of service context**

	Universal distribution	**Selective distribution**
Public benefit	**A** Personal direct taxes Social insurance payments Driving license registration Citizen registration	**C** Probation Youth offending Policing MAPPAs and CRB
Individual benefit	**B** Education General health services Social insurance benefits	**D** Child protection Services for older people Specialist health services Drug/alcohol abuse services

The problem is that services with different purposes have very different conceptions of their stewardship of client information, and these conceptions cause them to manage information in very different ways. We typically expect type A services to gather most information from clients themselves and to take information from other services only under specific legal powers. Type B services have generally been expected to keep information within their own 'family' or related health or education services and tend to be subject to professional protocols that codify duties towards clients.

Type C services have generally been required to show good grounds before requiring information from other services and to keep intelligence to themselves, especially where the information is 'soft'. Type D services may also deal in soft information but will tend to do so under professional confidentiality codes. In recent years, however, policy imperatives to share information, and especially to lower the thresholds for sharing with type C services, have blurred many of the boundaries between cells in Table 6.1. In the process, they have exacerbated the dilemma between risks associated with information sharing and confidentiality.

In response, the government has looked for *general* solutions to this policy problem. In 2000/01, the then Performance and Innovation Unit, now the Prime Minister's Strategy Unit, was commissioned to produce a report that finally appeared in 2002, entitled *Privacy and Data Sharing: The way forward for public services*.[3] Its recommendations for new legislation to create a general power for information sharing found little favour with government lawyers. When responsibility transferred to the Department for

Constitutional Affairs (now the Ministry of Justice) the department issued new legal guidance in November 2003, the burden of which was that existing powers provided all the cover required for any sensible sharing. It recommended that locally agreed protocols would suffice to govern information sharing in specific cases of inter-agency working. However, continuing scandals, which were widely attributed to information-sharing failures, led ministers to call for new initiatives to promote more extensive information sharing.

In late 2006, a 'vision statement' was published, promising much freer information flows but without providing much detail. Responsibility for publishing the statement was left to a cabinet committee, MISC 31. In the meantime, however, government brought forward new legislation creating information-sharing powers and duties to combat serious and organised crime, along with other proposals, including a children's database, a population register to underpin the national identity card scheme, a range of early years and even prenatal interventions to target those believed most likely, on the basis of long-range predictive modelling, to present future risks.

There are problems with both these approaches. The search for a single, general and overarching principle that could be set out in legislation seems likely to prove misguided, and it would, in any case, have to leave wide scope for discretion. The thresholds of probability and the severity of risk that would lead to information sharing in child protection cases are surely very different from those that are appropriate in detection of benefit fraud. In fields where willingness to present and to be candid with professionals is critical, disclosure rules have to be rather different from those in fields where financial entitlements are at stake.

In all these fields, decisions about sharing and confidentiality involve judgements about which staff within which agencies have a legitimate 'need to know' a specific piece of information, or to claim routine access to types of information. Such judgements also depend on how much, of which types of information, are proportionate to the risks presented by cases in different fields. However, these judgements cannot be made using algorithms, ie rules taking the form, 'if these circumstances obtain, always share [or do not share] this information with these other services'. No such algorithms are available, even for decisions about bulk sharing. Instead, claims about 'need to know' and 'proportionality' must be justified on the basis of arguable principle.

Dealing with the risks of risk assessments

'Risk assessment' for decisions of this kind, undertaken appropriately, must be *symmetrical*. That is to say, it should consider equally the risks arising both from sharing and from not sharing. Unfortunately, however, too much of the guidance presently given to practitioners encourages them to consider principally the risks arising from not sharing, on the assumption that these risks are generally worse. We argue instead that risk assessment should be conceived in terms of appraising the risks to the whole range of service outcomes including those arising from breaches of confidentiality, on the one hand, and the risks associated with not sharing, on the other.

Policy makers should also think about the ways public services could cultivate the skills and institutional capabilities for making and supporting these kinds of judgements. This is a very different policy problem from designing rules, and is a long way from resorting to simplistic calls for thresholds of probability and severity to be relaxed each time there is some service failure that may seem, at first glance, to be something to do with information sharing, or indeed, raising them, as was the response to the Orkney and Cleveland scandals.

Some professionals will, quite understandably, demand explicit rules to follow rather than be required to exercise personal judgement. This is particularly the case if they have reason to fear that, should conscientious and competent decisions turn out badly, politicians will expose frontline workers to personal blame and obloquy.

To illustrate this point, the cases of Victoria Climbié in Haringey and Caleb Ness in Edinburgh provide a powerful contrast. In the Climbié case, it was the frontline social worker, Ms Lisa Arthurworrey, who bore the brunt of the blame for the mistaken judgements made in that case, and she was placed on the register of those who should not be permitted to work with children. Yet there is evidence that she received totally inadequate training, support and guidance from her managers, and was given a case load beyond her capacity to cope. By contrast, for the errors made by social services in the Caleb Ness case, Les McKeown, the Director of Social Work in Edinburgh, resigned. The differences in the degree to which blame was individualised for catastrophic decisions will have proved very important in signalling to professionals in England and Scotland the need for defensive practice in relation to sharing information.

However, what constitutes practice that is defensible against blame is difficult for many professionals to call. There is no shortage of guidance for frontline staff on the legal aspects of information sharing. In almost every field of public services, central government bodies, professional institutes and local bodies have issued fat volumes of notes on the meaning of all relevant legal doctrines, from the principle of the paramountcy of the welfare of the child in child protection, through the legal powers of inspection for fraud detection officers, to the meaning of every relevant clause of the Data Protection Act, of the central concepts of the common law of confidentiality, of Article 8 of the Human Rights Act and much else besides. Locally agreed protocols on information sharing can run to over a hundred pages. In a large-scale study we conducted recently, we found to no one's great surprise that few professionals regularly consult any of these documents.

If there is a need for any more central policy intervention, it should surely not be designed to provide yet more guidance on the law, unless it be by way of handy summary. Rather, the focus should be on building competence through training, rather than producing yet more documents to clutter up the web. This training should be in the skills of symmetrical risk assessment, and the risks should be more holistically conceived. If there is to be more guidance, it should be aimed at managers rather than professionals, and should make the case for a less individualised and blame-oriented culture of management, and discuss practices that can most constructively be adopted when cases do go wrong, as inevitably they sometimes will, whatever decision norms are adopted. Most important, politicians should consider, before they reach for the easy option of blaming the frontline staffer or manager, what the consequences of devolving blame to lower levels may be for future decision making and public services in the relevant field.

The information sharing issue also raises some more general lessons about joined-up government. 'Joined-up' public services means, in practice, the joining up of purposes for which our personal information is collected, used and disclosed. In many cases, of course, this can be done sensibly and without contention. Few would doubt that any medical professional should, and in many cases commonly now would, alert other services if they saw evidence of neglect or violence in a child that was unlikely to be accidental.

It is also important to recognise, however, that we run great risks of undermining public services – independently of issues to do with privacy in its narrow sense – if we simply declare that all such services are obliged to use personal information they collect for their own purposes to further the goals of all public services, without exercise of judgement. Not only will the obvious imperatives of ensuring that clients and patients are willing to present and talk candidly about personal and social problems be undermined, but an issue of even more fundamental importance is at stake. Public trust in public services depends in no small measure on the degree to which people can understand and recognise the goals of these services as *delimited*, and recognise purposes for which they will use personal information as legitimately related to the core business of the service. As goals and purposes begin to sprawl and swell, their transparency, intelligibility and legitimacy is undermined.

At the heart of the issue there is a fundamental question about the causal relationships between opposing risks. At one meeting in Westminster not many years ago, we heard one child protection professional claim that if there were more cases of children being taken wrongly into care on the basis of sharing information that was over-interpreted, then that would be a sign that things were moving in the right direction, because it would indicate that fewer children who really are at risk are being missed: more cases of 'false-positive' judgement errors would be a price worth paying to save more children from abuse and neglect. This professional's emotional engagement with the plight of abused children cannot be faulted, but the reasoning in that remark is open to strong objection.

It simply does not follow that, because we are sharing even to excess and over-interpreting, we must consequently be guilty of fewer cases of insufficient sharing and under-interpretation of information. We could be misdirecting our efforts entirely. But, further, it is not at all obvious that the long-term cost of false-positive judgement errors would be a price worth paying for such an outcome. A system that routinely runs the risk of such errors will not indefinitely sustain public trust, as the legacy of the Orkney cases and the 'satanic ritual abuse' panics of 20 years ago showed. Politicians who call for 'more information sharing' and 'greater safety', and think that easy banalities about 'balance' and 'safeguards' cope sufficiently with the opposite risks, should think again.

Perri 6 is Professor of Social Policy, Nottingham Trent University; Chris Bellamy is Professor of Public Administration, Nottingham Trent University; and Charles Raab is Professor of Government, University of Edinburgh.

Notes

[1] H Mantel, *A Place of Greater Safety* (Harmondsworth: Penguin, 1992).

[2] It should be said that controversy continued for some time afterwards about the facts of some of those cases.

[3] Performance and Innovation Unit, *Privacy and Data Sharing: The way forward for public services* (London: Cabinet Office, 2002), available at www.cabinetoffice.gov.uk/upload/assets/ www.cabinetoffice.gov.uk/strategy/piu-data.pdf (accessed 3 Mar 2008).

7 The case of electronic patient records: is the privacy debate a smokescreen?

Marlene Winfield

Up until now, debate in the media about electronic health records has largely been conducted by doctors, speaking for themselves and also for their patients. Their concerns, at least as voiced, centre on risks to patient confidentiality. But they also often betray a lack of trust in their patients.

It is fair to say that the National Health Service (NHS), for the most altruistic reasons, has developed a parent–child relationship with patients. Any consideration of privacy and access to information needs to be seen against that backdrop. The eight-minute consultation can only work in one of two ways. Either the patient arrives fully briefed and ready to make the most efficient use of the eight minutes. Or the patient is a passive recipient of the clinician's wisdom – does as she is told and asks no questions.

Although possibly a satirical example, Essex GP 'Dr Copperfield', writing recently in *The Times*, illustrates a real school of thought among some clinicians:

> *Another pilot project allows patients to see their records and download their test results via the internet. Brilliant – when the scheme is rolled out across the country my patients can find out that they have an inoperable brain tumour from the comfort of their own home. At least it will save me the trouble of breaking it gently. When they sit down with their tear-stained scan result I can go straight in with 'Well, what can't speak, can't lie, can it?'*[1]

Contrast that with the findings of research the NHS Information Authority (NHSIA) commissioned from the Consumers' Association in 2003. In a survey of 2,000 adults, 63 per cent felt that being able to see their recent test results was an important benefit of electronic health records.[2] There is sometimes a presumption that the doctor knows best about not only medical advice, but also the way it is given and received. It is time that patients joined this debate rather than letting doctors speak for them.

I will be arguing here that we need to base our approach on the needs of the patient, and on trusting them to make informed decisions about their health. The privacy implications of NHS reform need to be seen in the context of this change in emphasis. If most people are 'privacy pragmatists', then the implications of connecting health records need to be based on understanding why the programme is happening, and what the benefits are.

The essay looks at how and why linking electronic medical records is so important to a patient-centred NHS. I suggest that some of the opposition to electronic health records can be understood as reticence towards better-informed and empowered patients – a challenge to the traditional relationship between doctor and patient.

The need for a strong patient voice

I work for NHS Connecting for Health as its patient lead, though the views expressed here are my personal ones. It is precisely because I am a patient that I joined this project to link all parts of the health service to share patient information, and share it with the patient.

For 15 years I ran a support group for British women injured by the Dalkon Shield, a faulty intrauterine contraceptive device that injured many thousands of women across the world in the 1970s. Over that time, I received hundreds of letters and telephone calls from women telling similar stories. They had the device fitted with very little information about how it worked or the danger signs. When they went back to their doctors reporting constant pain and excessive bleeding, they were told to wait until it settled down, or even to change their washing powder or take Valium.

Some of the less fortunate women wound up having emergency surgery for ruptured tubal pregnancies a little while later. Still more became infertile through chronic pelvic inflammatory disease. Some were left in chronic pain caused by scar tissue. In the worst cases, they became incontinent as well as infertile. Over 3,000 British women were compensated for their injuries by a worldwide trust fund set up by the US courts.

Three things became apparent to me as I listened to the women's stories. We didn't know enough about the device we were fitted with. Our doctors didn't know enough about potential problems and early warning signs. And there was no effective system for picking up patterns of problems as they emerged. All of these things could be significantly improved by better information sharing via electronic health records.

Though medicine is constantly developing and improving, it will never be a perfect science. Eminent paediatrician Sir Cyril Chantler has said that in the past medicine was simple, ineffective and relatively safe; now it is complex, effective and potentially dangerous. It must, therefore, make sense to increase the number of people able to be vigilant. Having badly informed patients is dangerous, especially when coupled with doctors who are not able to keep on top of every new development in all the medicines and medical devices they prescribe.

Privacy versus access to information

There will always be a tension between sharing information for good patient care and protecting individual privacy. If the NHS errs too far on the side of privacy, it comes at a cost to safety and the quality of care. But if it bends too far in the other direction, it risks eroding patient trust and also sometimes causing unintended harm.

In *The Future of Privacy*, Perri 6's research showed that the majority of us in most contexts are 'privacy pragmatists' – prepared to provide personal information for enhanced services or other benefits.[3] Up until now, that has certainly been true of patients in the NHS. In 2002 NHSIA commissioned the Consumers' Association to do research into patient confidentiality.[4] Under a third of 2,000 adults surveyed would prioritise NHS spending on systems to protect confidentiality, though that might have changed in light of recent data losses by other government departments. However, in 2002 those who had had problems such as lost records, letters going astray, or being mixed up with another patient were more likely to prioritise privacy.

In the NHSIA's research, one respondent, whom Perri 6 would call a 'privacy pragmatist', described an experience many will recognise:

If you go in for an emergency appointment… you've got to fill out this paper that's just been photocopied, and write down what is wrong with you. The receptionist looks at it and reads it out in front of everybody. And if you don't put down what's wrong with you, you don't get seen.

A 2003 report of patient surveys in primary care by the Picker Institute[5] found that 84 per cent of patients reported that they could be overheard by others while in the reception area of the surgery.

Another 'privacy pragmatist', when asked in the 2002 research who in his GP surgery had access to his medical records, replied, with tongue firmly in cheek:

Everyone in the surgery, apart from the cleaner – hopefully.

Weighing up the risks

The cost of not sharing patient information effectively can be seen in hospitals across the country every day. A prospective study of 19,000 people in 2004 concluded that one in 16 hospital admissions is the result of a bad reaction to medication – and that nearly three-quarters are avoidable. And of those admitted to hospital, 5,700 people will die[6] – the equivalent of around 19 jumbo jets crashing.

In a 2004 study, the National Audit Office found that apart from falls, the most common patient safety incidents in hospitals related to medication errors, record documentation errors, and communication failure.[7] A 2001 Audit Commission report concluded that most prescribing errors occur when the prescriber does not have access to accurate information about either the medicine or the patient.[8]

There are, of course, risks on the other side as well. Recent instances of government departments' laxity with computer discs containing personal data show all too well the dangers of not taking confidentiality seriously enough. In a recent report on the unlawful trade in personal information – of which health information is one part – the Information Commissioner wrote:

> *Investigations by the ICO and the police have uncovered evidence of a widespread and organised undercover market in confidential personal information… Among the 'buyers' are many journalists looking for a story… Other cases have involved finance companies and local authorities wishing to trace debtors; estranged couples seeking details of their partner's whereabouts or finances; and criminals intent on fraud or witness or juror intimidation.*[9]

The report gives the example of 'an abusive husband able to track down his ex-partner's whereabouts through her parents' medical records'.

People have a variety of reasons for not wanting their health information to fall into the wrong hands. People trying to avoid violent partners fear being traced through the NHS's demographics database. Those with a history of mental health problems say that it colours the way health professionals view their physical symptoms. Women who have terminated pregnancies feel certain staff will be biased against them. People with a history of alcoholism, mental health problems or drug abuse worry about employers finding out. People with certain long-term conditions fear that they won't be able to get mortgages or insurance. People with past sexually transmitted diseases worry about partners finding out. And it must not be forgotten that some of the 1.3 million people who work in the NHS will have concerns about what their colleagues might be able to see about them.

In addition to people with sensitive things in their records, there are those who object in principle to their information being stored on big government databases or who fear other parts of the state will misuse it. In some respects they are the most challenging for the NHS. Though they are a small minority, they are a vocal one, often better organised and able to speak more loudly than patients in general.

Better-informed patients

People in a few 'Early Adopter' primary care trusts are beginning to have 24-hour access to a summary version of their electronic health records, using a protected internet site. A small but growing number of GP surgeries are also offering their patients access to their full GP record over the internet. This is a significant change for patients, who are too often 'flying blind' when they make health decisions.

And there is more to come. Before long, people with long-term conditions will be able to monitor themselves, for example their peak flows, blood pressure and blood sugar levels, add the results directly to the record, and get instant feedback. They will also be able to add their treatment preferences to their record (such as advance decisions not to be treated) and their access needs (communication needs, dietary requirements, etc). A little further down the line, they could well have access to decision aids and an interactive care plan. They could use their records to give feedback on the treatment they've had. These things will really put meat on the bones of 'patient-centred care'.

Patients often tell me that they particularly look forward to having access to their health records over the internet if they are taken ill while travelling abroad. They will have the means to make information from it available online to anyone with internet access treating them anywhere in the world.

Better-informed staff

Even if people do not choose to access their own records or find it difficult, having this basic information available to authorised staff will improve their experience of being a patient.

I met a woman recently whose child has multiple health needs and many and often-changing medications. She told me that when her son goes into respite care, the home often does not have recent changes to his medication and must have proof in writing. So she spends stressful hours seeking written confirmation at a time when she wants to concentrate on settling her son in.

A friend emailed me recently after moving from London to Suffolk. She, her specialist and her GP had spent several years finding the right balance of medications for her thyroid problem, with all the mood swings and weight gain that entailed. She arrived at her new surgery to be told that the chances of her GP record following her were, in their experience, 'not high'. She wrote: 'My new GP needs to have a historic summary of my blood test results and medication levels in order to continue care and proper prescription. Not having access to information about my medical condition electronically makes no sense to me, and could result in a deterioration of my condition.'

A shared record of essential patient information would have greatly helped staff looking after a colleague nearing the end of the treatment for breast cancer. Her veins were 'shot' and the hunt for a useable one was agonising. Her care was shared between two hospitals. Each required a blood test before treatment but was unable to see the results of the one taken a few days earlier at the other hospital. While she is glowing in her praise for both hospitals, she reports that it was only when she 'begged and cried' that they took the (sometimes considerable) time to chase up the results from the other hospital by phone to save her having a painful and unnecessary repeat test.

Picking up trends

If, as Sir Cyril Chantler suggests, treatments are becoming more dangerous as they become more effective, then we need to improve our early warning systems of things going wrong. The electronic record offers a good opportunity. Data about treatments and outcomes can be anonymised and analysed for trends without the hit and miss of previous schemes that depended on doctors recognising and reporting adverse reactions. Had we been able to do this electronically in the 1970s, who knows how many women might have been spared the pain and suffering caused by the Dalkon Shield. It took a whole year for it to stop being used in Britain after it was banned in the US.

Is privacy a smokescreen?

A small group of doctors, especially general practitioners, have been vocal in their opposition to a nationally held patient information on the grounds of patient confidentiality. It is something all clinicians are naturally concerned about.

What the most vocal objectors hardly ever mention, though, are the problems today with paper records and existing computerised records. When recently a GP wrote in *The Times* that our GP records spilling out of Lloyd George envelopes were 'the envy of the world',[10] I wondered how in touch he was with the reality for his patients. On both safety and confidentiality grounds, it is high time we moved on.

We have a precious NHS with many caring and committed people doing their best under difficult conditions. Money and time are wasted when poorly informed patients and poorly informed clinicians struggle to make treatment decisions. Lives are sometimes lost or blighted by the errors that result – thousands each year according to the Audit Commission. Why would anyone want to continue down that road when we have the means to do better?

For patients, all aspects of medical care are a balance of risks and benefits. Electronic health records are no different. The risks have been well aired in the media of late, often inaccurately. For example, particularly inaccurate are assertions that the police and various government departments will be part of the sharing loop. Unlike now, when the police can put pressure on individual surgeries or trusts to release information, in the future there will have to be clear policies and procedures for information to be taken from electronic health records – and the process will be audited. That is not to say that there aren't risks, and each individual must weigh them against the benefits in their own circumstances.

The benefits of linked electronic records range from saving lives to saving people from additional stress in an already stressful situation. They also include giving patients the tools to better manage long-term conditions at home, the means to make known their treatment preferences, and the power that comes from being well informed. This context is often absent in stories about health records; the media know how to write only two stories about them: another large government IT project is failing or Big Brother is here. And though they are fundamentally incompatible, sometimes both are alleged at the same time!

Linked electronic health records, shared with patients, will make doctors and other clinicians more accountable to their colleagues and their patients for what they do and write down. It is likely that this, as much as their concern for patient confidentiality, may be sparking resistance in some quarters.

The 'privacy pragmatist' will have new choices

Much time and thought is being spent to enable the NHS to use its newfound capabilities wisely, to help it strike an appropriate balance between sharing information for good care and protecting people's privacy.

A number of safeguards are being introduced once the new systems are fully operational to provide more protection than exists now with either paper or existing computer records.

- Anyone wanting permission to use the new NHS Care Records Service will have to be sponsored to register to get a smartcard and passcode. Their smartcard registration will assign them a role or roles that will determine how much clinical information they are allowed to see. That means that someone booking appointments will no longer have access to a full patient record, for example.
- Staff will only be able to access records of patients the system recognises them as helping to treat. So gone will be the days when anyone in a hospital could look at any patient's records.
- The whole system is monitored and alarmed: anyone looking at a patient's record will leave a footprint (called an audit trail) and the patient can ask to see it.
- Anyone who tries to access a record against the access rules will trigger an alert to someone in charge of protecting patient privacy. Heads are more likely to roll when people do things they shouldn't.

Taken together, these controls will make it much more difficult for anyone outside the NHS to find people who actually have access to a patient's record who are willing to sell patient information (provided of course that the systems are up to standard). Apart from these new safeguards, over the next few years, various choices will become available to patients who want to put additional limits on who can access their information.

Those concerned enough to want to put additional limits on information sharing will be able to:

- choose not to have a nationally available summary created, or to have it created but not visible to anyone but themselves and their GP practice
- choose to maintain the status quo, with information being shared between organisations only by traditional means
- hide selected information from view when their records are shared
- put extra blocks on access to demographic information such as current address and current GP
- in extremis, not to have anything but basic administrative information held electronically

All training for professionals and NHS staff needs to reflect the new partnership with patients in relation to their health information. For example, health professionals will need to be trained to discuss with patients how information likely to be sensitive is recorded and shared.

The new world will throw up some significant challenges for patients and the NHS. People may profoundly disagree with things they see in their records but clinicians will not want anything deleted for medico-legal reasons. People who do not want any of their information held electronically may present real difficulties for those trying to provide them with care. What happens, for example, if they need an X-ray? Nearly all hospitals now use only digital imaging. While the NHS will try hard not to disadvantage people who make extreme information-sharing choices, it may not always be physically possible to provide the same standard of care as others get. And what will happen when, in a clinician's view, it is not possible to provide an acceptable standard of care because of someone's information-sharing choices?

Some of these challenges have always been there with paper records but they will be harder to fudge with electronic records. This is a real opportunity to come up with good answers. It is important that we proceed cautiously and learn as much as we can in the early stages. That is why an independent evaluation of early adopters of the Summary Care Record has been commissioned from University College London.

Conclusion

This essay started as a look at electronic health records. However, it has inevitably ranged wider because electronic health records are a means to an end, not an end in themselves. For patients, they offer an alternative to the Kafkaesque world where they rarely see information about them that clinicians share with each other – and are therefore disempowered. They offer an alternative to patients and staff 'flying blind', making important health decisions without crucial information. They usher in a world where patients have more say in the care they receive and how information about that care is recorded and shared.

There are risks to privacy with linked electronic records. As patients, we are aware of the potential for hacking into any linked computer system, of carelessness leading to lost information, and of identity theft. Even the considerable additional technological safeguards built into the new linked electronic health records can't guarantee 100 per cent safety. But there are privacy risks to paper records and existing computer records, not to mention well-documented risks to patient safety.

It is for each 'privacy pragmatist' to weigh up the pros and cons of fully participating in the new NHS Care Records Service. The decisions will be different for different people. Those who want to limit information sharing will have a number of options. Limiting sharing may have implications for the ability of the NHS to provide the safest and most efficient care – implications that need to be understood when decisions are taken.

The important thing for me as a patient is that the choice is mine. I no longer need well-meaning clinicians to speak for me. It is time they let me grow up, ask my views and trust in my judgement.

Marlene Winfield is National Patient Lead for NHS Connecting for Health.

Notes

[1] Dr Copperfield, 'Inside the mind of a GP. Dawn of the computer age', *The Times* (Body and Soul), 17 Feb 2007.

[2] Health Which? and NHS National Programme for Information Technology, 'The public view on electronic health records', NHS Information Authority, Oct 2003, see www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4055046.pdf (accessed 5 Mar 2008).

[3] Perri 6, *The Future of Privacy*, vol 2 (London: Demos, 1998).

[4] See NHS Information Authority in conjunction with the Consumers Association and Health Which?, 'Share with care – people's views on consent and confidentiality of patient information', final report, Oct 2002.

5 ‘Improving patients’ experience: sharing good practice’, Picker Institute, Summer 2003, available at www.picker.ch/download/newsletter/8.pdf (accessed 5 Mar 2008).

6 M Primohamed et al, ‘Adverse drug reactions as a cause of admission to hospital: prospective analysis of 18,820 patients’, *British Medical Journal* 329 (2004).

7 Department of Health, *A Safer Place for Patients: Learning to improve patient safety*, report by the Comptroller and Auditor General, HC 456 Session 2005–2006 (London: National Audit Office, 3 Nov 2005), available at www.nao.org.uk/publications/nao_reports/05-06/0506456.pdf (accessed 5 Mar 2008).

8 Audit Commission, *A Spoonful of Sugar: Medicines management in NHS hospitals* (London: Audit Commission, 2001), available at www.audit-commission.gov.uk/Products/NATIONAL-REPORT/E83C8921-6CEA-4b2c-83E7-F80954A80F85/nrspoonfulsugar.pdf (accessed 3 Mar 2008).

9 Office of the Information Commissioner, *What Price Privacy? The unlawful trade in confidential personal information* (London: The Stationery Office, May 2006).

10 ‘Medical records’, *Times Online*, 30 Dec 2006, available at www.timesonline.co.uk/tol/news/article1265068.ece (accessed 5 Mar 2008).

8 How personal medical data can improve the public's health

Robert Souhami

Research using data derived from medical records is one of the main methods for improving public health. It has saved and improved the lives of thousands of people. This form of research identifies causes of disease in the environment – cigarette smoking is a notable example. It suggests methods for controlling epidemics; the findings frequently demonstrate long-term beneficial or harmful effects of treatment and indicate ways in which effective healthcare can be delivered or improved. The UK has been one of the world leaders in this field for over 50 years. With the proposed national introduction of electronic healthcare records the opportunities for UK research to improve the health and lives of the population are now exceptional. No other country will be capable of providing data for research analysis on the same scale. But just at this moment of opportunity, changes in the laws concerning privacy, combined with confused interpretation and regulation of these laws and a conflicting and multilayered bureaucracy, have put such research at risk.

This form of research is quite different from other types of medical research that are interventional – such as clinical investigation or treatment trials where the patient and members of the investigator's team meet each other. This is research that uses information in medical records that was originally collected for some other purpose – usually the routine care of patients. Of course the researchers understand that private information is given in confidence during healthcare and that patients would not expect that it would be disclosed without consent. But some activities undertaken in the public interest may be damaged, or even prevented, unless the reasonable boundaries of such confidentiality are defined and understood.

Routine medical records have many advantages in public health research. They represent current practice; they cover all social classes and ethnic backgrounds; large numbers of records can be studied to detect rare events; and the findings can be quickly turned into practical recommendations for health. The researchers are not interested in outcomes, or details, of *individuals*, but in the health of *populations*. In formulating and presenting the results of the research no reference is made to individual patients but to general outcomes in the patient or disease group concerned. In other words, although the data have to be derived from individuals the subsequent results are generalised.

A straightforward example is the use of cancer registries. In many countries it is a legal requirement to register a diagnosis of cancer. These countries therefore know exactly how many cancers are occurring and can detect changes in incidence (the number of new cases in a given time). It is not a legal requirement in the UK but our registries include the majority of the population. Two examples serve to show the damage that can be done by not knowing the number of new cases. It is widely believed that in the UK the cure rates for cancer are inferior to those in France. Such a view, which worries the general public and patients with cancer, and influences policy, has no basis in fact because most cases of cancer are not systematically registered in France.[1] Although the death rate from cancer in France is known, in the absence of reliable data about incidence the national cure rates cannot be measured accurately. In Hyogo province in Japan, concerns over privacy led to the closure of the cancer registry. This decision tragically led to the failure to detect a rising incidence of mesothelioma (cancer of the lung due to asbestos exposure) and the registry was reinstated.

The routine passage of information about a cancer diagnosis to a public registry, which keeps the information securely and which uses it for population statistical purposes, is an example of the way in which the illness of an individual can be used to benefit society as a whole. And yet there are occasionally objections in the UK, on the grounds of privacy, to such a necessary activity. Indeed, in 2000 the General Medical Council stated that the transfer of such information to a registry may be against the law, thereby calling into question the registration of cancer in the UK. The GMC belatedly recognised, and retracted, this damaging advice, which was based on a controversial interpretation of the law.

It is of course legal to use medical data if the patient has given consent, or if the records have been completely and irreversibly anonymised. Unfortunately, consent or irreversible anonymisation are frequently either not possible, or would invalidate the research. It is extremely important to understand why this is so, and the following examples explain the problem.

It may be completely impractical to obtain consent. The research often involves linking the data from one source to that in another, unrelated, database. This may involve tens of thousands of individuals, the data often having been collected, both in time and place, at a considerable distance from the individuals and the events of interest and for different purposes:

Research testing the hypothesis that adverse conditions in pregnancy might increase the risk of cardiovascular disease years later in adult life used 15,000 birth records collected from 1911 onwards. At the time of the research the population had dispersed and 3,000 people had died. The study provided evidence for a link between low birth weight and hypertension and type II diabetes in adult life.[2]

Seeking consent may introduce biases that undermine the research, the process may cause distress, or the research may concern people whose illness means that they lack the legal capacity to consent:

There was uncertainty about whether termination of pregnancy increased the risk of breast cancer – thereby providing an argument against termination. But a probable bias was that women who had developed breast cancer might be more willing to disclose information about a previous termination (to help explain why they had a cancer) than women with no cancer and in doing so would establish a false association. The absence of risk was demonstrated when a data linkage study was performed without consent.[3]

There is a serious risk of double counting if data are irreversibly anonymised:

Following the thalidomide tragedy, registers of congenital anomalies were established to identify teratogenic exposures during pregnancy. The anomalies may present medically for the first time many years after birth, so data must be sought from genetic counselling services, midwives, paediatricians, *general practitioners and others. Unless the names are known, and can be checked, a single case may be recorded several times distorting the frequency and the risk.*[4]

Sometimes additional data may need to be added over many years in longitudinal studies of outcome. The detection of a rare but serious side-effect of a drug may only be suspected years after exposure. New data cannot be added if the records of those receiving the drug have been irreversibly anonymised.

These examples show that research in the public interest may sometimes need to use identifiable data without consent. This has created great difficulty for research as the legal framework, and its interpretation, concerning such use has changed. This is not just a problem for the UK, but it is especially important here because of our long-standing expertise in this form of investigation and the many important contributions that have been made. Of course, clinical researchers must recognise that changes in the privacy laws reflect public concerns about possible misuse of their personal information. These concerns largely centre on commercial and political use of data but medical research is caught up in the resulting legislation, even if it was not the primary target of changes in the law.

The law has become more complicated following the enactment of the Data Protection Act 1998, the Human Rights Act 1998 and the Health and Social Care Act 2001. In addition, the use of data is subject to the Common Law of Confidentiality. In spite of the wide areas of public life that this legislative framework is intended to cover, schedules and exceptions have been included to allow the use of data without consent in the public interest. The essential point is that the use of data in this way must be demonstrably proportionate to the risk involved to individuals and the likely benefit that may result. In more than 50 years there has not been a case concerning medical research use of records under the provisions of the common law.

A recent report of a Working Group of the Academy of Medical Sciences, which I chaired, considered that in spite of the difficulties with this complex framework, the law as it now stands was not intended to inhibit medical research in the public interest.[5] Our conclusion was that the problems that now beset the researcher in trying to undertake research are often caused by the confusing and contradictory assessments made by regulatory bodies that may be required to pass judgement on the legality of a research proposal.

Research proposals are usually developed by research teams in academic departments. Studies using population databases or large numbers of records are often collaborative, involving investigators in many different locations, sometimes in several countries. To fund the research, the proposal is usually submitted to a research funding agency and will have been approved by the ethics review committees of the institutions involved. Before funding, the science, feasibility and importance are assessed by a process of peer review. This is a highly competitive procedure – in aggregate, only about 30 per cent of proposals in biological sciences are funded in the UK. If a proposal for research using data passes through these hoops it will often then have to surmount hurdles which other medical research does not encounter. These take the form of one or more assessments by a variety of regulatory bodies. These include the Patient Information Advisory Group (PIAG), the Office of the Information Commissioner, the R&D offices of hospital and primary care trusts. Each of these structures may give different opinions on what they think is the legal position. In a multicentre study this process may take months or years. In the Academy study, researchers gave us numerous instances where it had been difficult or impossible to respond to the conflicting advice and interpretation.

Understandably, the regulators concerned with research use of data place preservation of confidentiality as the predominant factor in deciding on whether to permit research to take place. However, following its call for evidence the Academy received numerous examples of a wholly disproportionate assessment of the risks to any individual when judged against the potential benefits that the research might bring. If one or more of the regulators consider that there may be a legal impediment in the study this may delay, or prevent, the study from occurring. A frequent outcome is that so many additional administrative burdens are placed on the investigators that the financing and time allotted to the study will not support its continuation.

Although it is true that over the last 50 years there has been great benefit and no harm, it is clear that this truth will not suffice nowadays. There are already excellent standards of ethical review of research proposals and there is independent peer review of the science. Most research teams have high standards of data security and staff training. (It must be stressed that concern for *confidentiality* does not supplant the need for *data security*. The recent gross and inexcusable loss of data by government departments shows how important security is.) These standards must be of demonstrably high quality and for this reason the Academy suggested that guidelines be developed for these aspects of the research process so that the public can have confidence in the security of the data and its handling.

What does the public know of this process and the difficulties that are impeding research that may benefit them as individuals and their families? There have been very few reliable studies. Most enquiries have lumped together all research as one general activity and posed questions without explaining the specific context. One large-scale questionnaire enquiring generally into who should have access to medical records asked whether the respondent would be content to let their record be seen by 'a medical researcher'. Many of us would say 'no' to such an ill-defined question but might well answer 'yes' if we had been asked about confidential, secure, non-commercial use of the outcome of our illness that would allow long-term problems to be identified and services to be improved with no risk of personal identification.

Knowledgeable patient support groups are mostly strong supporters of research of this kind. But several important points must be considered in discussing public attitudes. Not all illnesses are equal in terms of sensitivity. Research on blood pressure has quite different connotations than that on sexually transmitted diseases, alcoholism, mental illness or child abuse. Furthermore the attitudes and responses of patients who have the disease may be quite different from when enquiry is made of the general public who have no experience of the anxieties that accompany serious illness and the intense desire for progress that many patients feel.

Whose opinion should then prevail? Many of us would perhaps answer that the attitudes that should carry most weight should be those of the people who are most affected. Even within patient organisations there may be problems of understanding that get in the way of informed discussion. Representatives of HIV-infected people are often, understandably, among those most concerned about records-linked research. But even in such a potentially sensitive area important issues of health cannot be avoided if, and when, they occur. Consider a possible scenario.

Let us suppose that a rare side-effect of one, but not all, drugs to treat HIV is an increased risk, after many years, of an uncommon cancer of the lymphatic system. (A similar long-term risk was found by records-based research, beginning in the 1970s, in patients with renal transplants treated with drugs to suppress graft rejection.) A way to detect this risk would be by matching the records of tens of thousands of treated patients with data derived from cancer registries. But the time elapsed, and the large numbers necessary to detect, with statistical confidence, a modest increase in risk of an uncommon disease, might well mean that informed consent could not reasonably be obtained. If you had HIV and were taking, or had taken, the drug in question, would you want this research to proceed – even if it was quite impossible to ask your personal permission but you knew there was no risk of disclosure?

So, more detailed research of attitudes is needed. This research must be focused and precise. Diseases should be considered separately, the details of the research made clear, and informed and considered responses should be sought from sections of the public that are likely to have different perceptions or interests. These include patients, the families of those affected, the general public, social and ethnic groups. Poor-quality research, sadly all too common, will inevitably generate confusion and misinformation.

How can patients and the general public be engaged in the opportunities, and obligations, to carry out research to improve the health of us all? The research mission of the NHS has almost no public face. The opportunities for research based on our own experience of illness, and the benefit it can bring, are seldom explained at the point when we use the service. Patients going to a teaching hospital know, because they are informed of the fact, that they may be asked to accept the presence of a medical student or nurse in training. But the same document given to patients seldom mentions the research mission of the hospital. Why not? Why cannot hospitals and practices help to spread the understanding of research for public benefit? If this isn't done, and public opinion is not well understood, there is a great risk that a highly vocal minority who insist on the primacy of the right to privacy, will drown out the desire of less emphatic citizens who wish to contribute to the public good. Getting ill is upsetting. If our experience of illness can be

used to help others most of us would surely want to participate. As citizens we know we have responsibilities as well as rights.
Robert Souhami is Emeritus Professor of Medicine at the University College London.

Notes

[1] F Berrino et al, 'Survival for eight major cancers and all cancers combined for European adults diagnosed in 1995–1999: results of the EUROCARE-4 study', *Lancet Oncology* 8 (2007).

[2] D Barker, 'The midwife, the coincidence and the hypothesis', *British Medical Journal* 327 (2003).

[3] MJ Goldacre et al, 'Abortion and breast cancer: a case–control records linkage study', *Journal of Epidemiology and Community Health* 55 (2001).

[4] ID Richards et al, 'A local congenital anomalies register: monitoring preventive interventions', *Journal of Public Health Medicine* 21 (1999).

[5] The Academy considers that a balanced interpretation of the legal provisions is necessary. Although the Academy did not recommend further changes in the law, there are several recurring areas of confusion in interpretation where greater clarity is needed. In particular, the public interest defence in the use of information hinges on the word 'necessary' in Article 8(2) of the Human Rights Act. This should not be taken to mean 'indispensable'. It is unclear if Section 60 of the Health and Social Care Act, which led to the establishment of the Patient Information Advisory Group (PIAG), supplanted the common law public interest defence or provided an alternative means of deciding if a proposal involved no breach of privacy.

REGULATING OUR PRIVATE LIVES IN AN OPEN SOCIETY

9 Sleepwalking into a surveillance society

Jonathan Bamford

Back in the early 1970s many were waking up to the potential of computers to have a powerful influence over ordinary people's lives – the power to store hitherto impossibly large quantities of personal information; the power to cross-reference information about individuals from different sources; the power to record this in a format aiding wider distribution than was ever possible before – all accompanied by the real risk that such power would not be used in a benign or beneficial way, but in a way that eroded individual freedoms. This was the real prospect of life imitating art, with the Orwellian vision of 'Big Brother'[1] becoming a nightmarish reality. A prerequisite to being able to build up this intrusive picture of people's lives is the capability to distinguish between one individual and another, to be able to identify them uniquely and attribute information to this identity.

The response to these privacy concerns included attempts to try to identify and codify standards for information handling that would enable the benefits of the emerging new technology to be realised while providing protection for individuals against unwarranted use of their information. These are what have become known as data protection laws.

If we cast our minds back to the time when these data protection standards and laws were developed, the information technology of the day was very different. The power of computing was based on expensive mainframe computers; the threat came from personal information being in the hands of a few well-resourced organisations and governments: a small family of 'Big Brothers'.

Today our 'computers' sit on our desks, in our laps, palms or pockets with devices as diverse as PCs to mobile phones. We are 'networked' unlike anything envisaged by most back in the 1970s. We take full advantage of our modern wired-up world where goods and services are available 24/7, where buying a book doesn't require a visit to a local bookshop but where it can be purchased with just the same ease from a retailer in Seattle, Shanghai, Stockholm or Sydney.

But with our modern world those with whom we do business want to have confidence in who we are, in order to protect themselves. Equally, individuals crave certainty in those whom they are dealing with to avoid falling prey to identity theft. All this involves the provision of identifying information, and we leave behind information about ourselves, our electronic footprints, as we go from transaction to transaction, from website to website: use of a credit card here, a mobile phone call there, the click of a mouse on a web url or on 'send' with an email. Our transactions are tracked, our interactions identified and our preferences profiled, all with potential for retaining and disseminating these to others, building up an increasingly intrusive picture of we live our lives. The 'surveillance society' is no longer science fiction.

Identity: its part in the bigger picture

We have undoubtedly moved into what has become known as the 'information age'. It is the linking of information to an identified or identifiable individual that is the precursor to other activities that may impact on them – identification of the individual either directly through traditional attributes of identity such as given name, date of birth and physical characteristics such as gender, eye colour and height or indirectly through identifiers allocated to them such as identification numbers, phone numbers, vehicle registration marks and credit card numbers.

In our parents' generation 'appropriate anonymity' was a fact of every day life. Many transactions took place face to face with payment by cash and although the individual may have been personally known to the service provider there was little in the way of centralised collections of personal information created. However in the modern 'wired-up' world, a variety of identity attributes are used to tie individuals to particular transactions involving a large number of other parties. Although identification attributes can vary depending on the degree of certainty a service provider needs to have about who they are dealing with, such as to ensure payment is honoured, there are still a large number of identifying particulars created. This not only produces a comprehensive picture of that individual's interactions with the service provider but also provides the links on which this information can be shared with others, building up a wider picture of an individual's activities. The day

of the data aggregator is with us and organisations offer lucrative identity verification services, and with this a vicious circle, as the greater the extent of the personal information and the more current it is, the greater certainty with which they feel they can vouch for that individual's identity. This is often known as the 'biographic footprint' and without it individuals can become disadvantaged as their identity is called into question.

However, identification does not end there; the technology now exists to tie identity to the very human tissue of an individual through biometrics. Automatic fingerprint, facial and iris recognition applications and DNA profiling and matching are increasingly commonplace and are no longer the preserve of the law enforcement community. Biometrics are being increasingly deployed in everyday life from international travel documents such as passports and visas to schools where fingerprint recognition is used to issue library books and to pay for school meals.

Identification and surveillance

The alliance between technological advances and the generation of more and more identifying particulars means that the component parts of the infrastructure of the surveillance society are now laid out before us and this is being assembled piece by piece. Each piece is justified in its own right by its advocates but when viewed as a whole the edifice could amount to the Orwellian vision, just nearly quarter of a century later than predicted. Increasingly the political response to terrorist outrages and fear of crime in the population is to deploy surveillance technology. In the United Kingdom there are now an estimated 4.2 million closed circuit television (CCTV) cameras observing and recording the population as it goes about its business.[2] When first introduced CCTV was essentially a passive tool, with images being viewed and acted on in response to events. Increasingly, digitised images are now being processed in a way that turns CCTV cameras into proactive tools with the capability to automatically identify and record an individual's movements. Automatic facial recognition software is now deployed with cameras not only with public sector schemes to identify and track known criminals but also in the retail sector to identify persons of concern entering shops.

Increasingly allied to CCTV cameras is vehicle registration plate recognition software, know as Automatic Number Plate Recognition (ANPR). This enables vehicle movements to be logged and by association the activities of the registered person associated with that vehicle. This technology is now deployed not only to look for vehicles of interest to the police but also to underpin traffic enforcement activities such as identifying speeding vehicles and whether a vehicle's owner has prepaid for driving in a road-use charging zone such as with the congestion charge in central London. The example of use of ANPR technology for catching speeding vehicles shows how new technology increases the ability to survey the population as it goes about its lawful business. ANPR speed cameras calculate average speed over a fixed distance by capturing the vehicle identification plate of all vehicles passing the first camera and a second camera some distance along the road.

The difference from traditional speed cameras is that there is a record of all vehicles passing through the two cameras not just the speeding ones. A vehicle movements database is built up. The London Congestion Charging Scheme also captures and retains details of all vehicles not just the vehicle details of those drivers who have not paid. Sensible application of data protection safeguards limits retention of the details of the innocent in this latter case although the law enforcement community sees such details as valuable should an incident occur and seeks long retention.

The huge advances in telecommunications with the use of the internet, email and mobile telephones as part of our everyday lives means that these can equally be used by those elements of society involved in criminal activity. Increasingly the law enforcement community wants telecommunication service providers to keep detailed records of who owns mobile phones, to whom SIM cards are sold and the phone numbers allocated to them. They also want providers to retain 'traffic' data showing phone numbers from which calls are made and received, email transactions and the URLs for websites visited.

While interception of telephone call and email content remains subject to strict legal safeguard (although much can still be judged from the title of a webpage visited or an email address), governments have moved to require telecommunication service providers to retain traffic details for longer than they ordinarily would for business purposes. In the UK the Anti-Terrorism, Crime and Security Act 2001 put in place such measures and one of the immediate responses by the UK government to the terrorist atrocities in London on 7 July 2005 was to use its position as the then President of the European Union to fast track work to establish a regulation requiring common minimum traffic retention periods in all EU member states. Although the fight against terrorism is cited as the reason for retention, once retained the potential is there to use it for less pressing policing activities.

Such legislative responses can erode safeguards contained in data protection and privacy legislation; other common examples include laws facilitating public sector data matching such as to detect fraudulent government benefit claims or other frauds against the public purse, data matching often being seen as the answer rather than preventing the fraud in first place by better administration.

In the UK other developments such as the extension[3] of the police's powers to take DNA samples and the removal of specific statutory requirements to delete these and fingerprint details where the police have no further interest in an individual are further evidence of a relentless acquisition of more and more identifying particulars about the population.

The list of public policy developments with a privacy impact does not stop there. Many current initiatives have dimensions that engage privacy concerns however well intentioned or desirable the initiative. Even a brief listing shows the range and extent. The Identity Cards Act 2006 creates a national identity register tied to individuals' biometrics, making possible the creation of a data trail as individuals use the card as they go about their day-to-day business. Connecting for Health is a project to create an electronic healthcare record in England with summary healthcare records available nationwide. There is an eBorders programme underpinned by wide-ranging legislative powers for border control agencies to acquire and share traveller information with each other.

Our road travel is subject to plans to increase the extent of road-user charging, engaging concerns about how vehicle users will be tracked and details of their journeys stored. The list goes on with many other developments in the public sector, be it increased information sharing to transform government or to catch those who commit fraud as with the Serious Crimes Act 2007. The developments are not just at home; the requirements of the US and other countries for passenger name record information to be provided by airlines, including substantial amounts of personal information in order to safeguard border and aviation security, impact across frontiers with details of millions of innocent passengers retained for long periods of time.

Are our privacy laws redundant?

The thirst for more and more information about individuals seems unquenchable but it would be unduly pessimistic to believe that data protection and privacy laws are at best anachronistic, and at worst completely useless. It is fair to say that data protection and privacy regulation has struggled to keep pace with the technological, economic and political changes that have driven the expansion in the breadth and depth of personal details held about individuals. Individuals are concerned about what happens to their information. Research conducted by the Information Commissioner's Office (ICO) in the UK shows that over half of individuals surveyed believe that they have lost control of how their information is handled and the need to protect their information is judged to be a matter that concerns them only second to preventing crime and issues mentioned above such as the NHS, unemployment, environmental issues and equal rights.[4]

Given public desire to be safeguarded against unwarranted use of their personal details, this begs the question whether the data protection laws themselves are deficient. In essence most data protection laws are technology neutral with no detailed references to particular technological applications within them. They set principles to be followed, rights for individuals, supervisory regimes and legal sanctions. The central principles remain as valid today as 30 years ago with safeguards against wider use, poor data quality standards, security arrangements and the need for transparency, data minimisation and individual access. The core data protection standards still appear to pass muster as a comprehensive set of desirable standards to protect individuals in the handling of their information, if applied correctly. Research undertaken by the Information Commissioner in the UK into public attitudes to CCTV[5] and other surveillance technology showed that when asked to come up with essential safeguards, the list generated closely matches the core data protection standards.

Trying to ensure that what appear to many to be complex data protection and privacy laws are applied in the context of new developments has become a challenge for the data protection regulatory authorities. In the UK the Information Commissioner used his powers to issue a code of practice specifically related to CCTV surveillance.[6] This was inspired by the need to try to apply the standards that had traditionally been required with computerised personal information to images relating to individuals. Although only published in 2000 this code is already showing its age as technology like ANPR advances, and a revised version has just finished a round of public consultation ready for publication in early 2008.

Incorporating safeguards at the outset does not yet always come naturally to those who develop policy and technology. This is despite the decades' long existence of data protection and privacy legislation. Core data protection safeguards such as data minimisation and finality of use are often overlooked in the rush to develop a new application. A solution is the deployment of privacy enhancing technologies (PETs) into new developments, using technological solutions to try to ensure appropriate privacy but this has yet to strike a chord with many despite the efforts of data protection authorities to promote them. Perhaps more fundamentally, many developing new applications do not even question whether there is a more privacy-friendly way to achieve the same objective; they are locked into the thinking of the past that substantial amounts of personal information is a necessity if you are dealing with people. Privacy impact assessments (PIAs) have a real role to play, particularly with the public sector developments, but in Europe these have yet to be embraced in the same way as in North America and Australasia. The Information Commissioner is redressing this balance and has commissioned work to produce a PIA handbook for use in the UK based on the best international experience available, which was launched in December 2007.[7]

Identity management is a good example of where old thinking dominates at the cost of personal privacy. Identity management is a crucial activity in our modern world as we do business with others who are not known to us or us to them, where service providers want to have confidence that they can trust the person they are dealing with and, importantly, that the individual can have confidence in what happens to their details. But the traditional approach of storing more and more details to substantiate identity held in a central collection for consultation by others does not necessarily achieve the objective and poses its own risks should security be compromised. This centralised approach to identity management is not the only option; there are other opportunities that may provide equally viable options such as user-centric and federated identity management among a number of privacy-friendly options.

However, each of these responses can address only particular elements. The effects on privacy go further than the informational privacy aspects, as is recognised in the PIA process, which goes beyond dealing with strict data protection compliance and goes on to consider societal impacts. Initial findings from ICO research commissioned to gauge public attitudes to surveillance was published in December 2007 and shows that the public is largely accepting of some element of surveillance as a product of how the modern world works but also trusts that there is something or someone in place to safeguard their interests.[8]

Whether subsequent widely reported security incidents, such as the loss of discs containing the personal details of 25 million people involved in child benefit claims by HM Revenue and Customs,[9] has altered the balance of public trust remains to be seen. It is clear that legislative safeguards can do only so much to address surveillance society issues. The two parliamentary inquiries into surveillance show the range of interests now engaged. The House of Commons Home Affairs Committee is addressing the issue from its perspective, which includes the law enforcement angle on surveillance, while the House of Lords Constitution Committee is addressing the issue from the constitutional perspective, which engages the important issue of the relationship between the citizen and the state.

Whatever aspects or approaches are adopted, addressing the challenges posed by the developing privacy risks cannot be left to chance. Acknowledging the need to rise to the challenges and concerted action to meet them is required. To this end the Information Commissioner has a dedicated surveillance society action plan, which has work streams ranging from understanding public attitudes to developing practical tools such as PIAs and codes of practice. It is vital that we move from debating whether we are living in a surveillance society to putting in place practical steps that will safeguard us against unwanted consequences. The Information Commissioner, having raised awareness of the issue at an international conference in London in 2006,[10] held a follow-up conference in Manchester in December 2007 entitled Surveillance Society: Turning Debate into Action, which was aimed at moving the agenda forward in a very practical way, addressing legitimate privacy concerns and, by doing so, helping to inspire public trust and confidence in the use of their information.

Privacy: an objective not a threat?

When considering the issue of surveillance and privacy from a data protection regulatory perspective, it is undoubtedly the case that the central principles of data protection law are as relevant today as they ever were, if not even more so. Information being used fairly, keeping it to a minimum, ensuring it is of the right quality and guaranteeing its security are crucial protections, which cannot be left to chance or the virtuosity of those who hold it. Its safeguards are vital in limiting the ambitions of those whose mantra is 'only the guilty have anything to fear'. As the recent security breaches have shown, more than just the guilty may have something to fear if personal information is not treated with proper respect and care. However, the rapid pace of technological progress has sometimes left behind data protection regulators who too often are trying to get data protection grafted on to an essentially privacy-intrusive way of operating.

Protecting privacy is seen by many as an obstacle to development rather than an objective. It is essential to change the mindset of those who crave more and more information about individuals and seek to employ the increasing power of technology and applications to deliver their objective of the need to consider privacy first rather than an as afterthought. They can embrace the use of tools like PIAs and privacy-enhancing technologies as real evidence of their commitment to protect privacy.

The first European-wide legal instrument on data protection, the Council of Europe Convention 108, points out that information power carries social responsibility. If those carrying this responsibility fail to discharge it and do not seize opportunities to treat appropriate privacy protection as an objective of new developments, not an obstacle to them, the consequences will be felt by all, as the very fabric of our society will have undergone an irreversible change. The public trust in those who hold and use their personal details will be lost and replaced with the chilling feeling that privacy and autonomy have disappeared with each and everyone of us a fully paid-up life member of the 'surveillance society'.

Jonathan Bamford is the Assistant Information Commissioner.

Notes

[1] G Orwell, *1984*, new edn (Harmondsworth: Penguin, 1990).

[2] C Norris, M McCahill and D Woods, 'The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space', *Surveillance and Society* (CCTV Special) 2, no 2/3 (2004), available at www.surveillance-and-society.org/articles2(2)/editorial.pdf (accessed 29 Feb 2008).

[3] Home Office, *Criminal Justice and Police Act 2001* (London: TSO, 2001).

[4] Information Commissioner's Office, *Annual Tracking Research Findings* (Wilmslow, Cheshire: ICO, 2007), available at www.ico.gov.uk (accessed 5 Mar 2008).

[5] ICO, *Public Attitudes to the Deployment of Surveillance Techniques in Public Places* (Wilmslow, Cheshire: ICO, 2004), see www.ico.gov.uk (accessed 5 Mar 2008).

[6] ICO, *CCTV Code of Practice* (Wilmslow, Cheshire: ICO, Jul 2000), see www.ico.gov.uk (accessed 5 Mar 2008).

[7] See www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html (accessed 25 Mar 2008).

[8] ICO Conference, Surveillance Society: Turning Debate into Action, Nov 2007.

[9] 'UK's families put on fraud alert', *BBC News Online*, 20 Nov 2007, see http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm (accessed 1 Apr 2008)

[10] London Initiative, 'Communicating data protection and making it more effective', 28th International Conference of Data Protection and Privacy Commissioners, 2–3 Nov 2006, see http://ico.crl.uk.com/files/ComE.PDF (accessed 29 Feb 2008).

10 Towards global privacy standards

Peter Fleischer

How should we update privacy concepts for the Information Age? The total amount of data in the world is exploding, and data flows around the globe with the click of mouse. Every time you use a credit card, or every time you use an online service, your data is zipping around the planet. Let's say you live in France and you use a US company's online service. The US company may serve you from any one of its numerous data centres, from the 'cloud' as we say in technology circles, in other words, from infrastructure which could be in Belgium or Ireland – and which could change based on momentary traffic flows. The company may store offline disaster recovery tapes in yet another location (without disclosing the location, for security purposes). And the company may engage customer service reps in yet another country, say India. So, your data may move across six or seven countries, even for very routine transactions.

As a consumer, how do you know that your data is protected, wherever it is located? As a business, how do you know which standards of data protection to apply? As governments, how do you ensure that your consumers and your businesses can participate fully in the global digital economy, while ensuring their privacy is protected?

The story illustrates the argument I will make in this essay. Businesses and governments, but most of all citizens and consumers, would all benefit if we could devise and implement global privacy standards. In an age when billions of people are used to connecting with data around the world at the speed of light, we need to ensure that there are minimum privacy protections around the world. But the majority of the world's countries offer virtually no privacy standards to their citizens or to their businesses, and the minority of the world's countries that do have privacy regimes follow divergent models. We can do better. Today, citizens lose out because they are unsure about what rights they have given the patchwork of competing regimes, and the cost of compliance for businesses risks cooling economic activity. Governments often struggle to find any clear internationally recognised standards on which to build their privacy legislation.

Of course there are good reasons for some country-specific privacy legislation. The benefits of homogeneity must be balanced by the rights of legitimate authorities to determine laws within their jurisdictions. We don't expect the same tax rules in every country, say some critics, so why should we expect the same privacy rules?

But in many areas affecting international trade, from copyright to aviation regulations to world health issues, huge benefits have been achieved by setting globally respected standards. In today's inter-connected world, no one country and no one national law by itself can address the global issues of copyright or airplane safety or influenza pandemics. It is time that the most globalised and transportable commodity in the world today, data, was given similar treatment.

So I would like to set out why I think international privacy rules are necessary, and to discuss ideas about how we create universally respected rules. I don't claim to have all the answers to these big questions, but I hope we can contribute to the debate and the awareness of the need to make progress.

Drivers behind the original privacy standards

First, a bit of history. Modern privacy law is a response to historical and technological developments of the second half of the twentieth century. The ability to collect, store and disseminate vast amounts of information about individuals through the use of computers was clearly chilling in relation to the collective memories of the dreadful mass misuse of information about people that Europe had experienced during the Second World War. Not surprisingly, therefore, the first data privacy initiatives arose in Europe, primarily aimed at imposing obligations that would protect individuals from unjustified intrusions by the state or large corporations, as reflected in the 1950 Council of Europe *Convention for the Protection of Human Rights and Fundamental Freedoms*.[1]

Early international instruments

Concerns about international data flows were already being addressed in a multinational context as early as 1980, with the awareness that a purely national approach to privacy regulation simply wasn't keeping abreast of technological and business realities. After a decade of uncoordinated legislative activity across Europe, the Organisation for Economic Co-operation and Development (OECD) identified a danger: that disparities in national legislations could hamper the free flow of personal data across frontiers. In order to avoid unjustified obstacles to transborder data flows, in 1980 the OECD adopted its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[2]

These OECD *Guidelines* became particularly influential for the development of data privacy laws in non-European jurisdictions. The *Guidelines* represent the first codification of the so-called 'fair information principles'. These eight principles were meant to be taken into account by OECD member countries when passing domestic legislation and include:

- collection limitation
- data quality
- purpose specification
- use limitation
- security safeguards
- openness
- individual participation
- accountability

A parallel development in the same area but with a slightly different primary aim was the Council of Europe *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* adopted in 1981.[3] The *Convention*'s purpose was to secure individuals' right to privacy with regard to the automatic processing of personal data and was directly inspired by the original European Convention on Human Rights. The Council of Europe instrument sets out a number of basic principles for data protection, which are similar to the 'fair information principles' of the OECD *Guidelines*. In addition, the *Convention* establishes special categories of data, provides additional safeguards for individuals and requires countries to establish sanctions and remedies.

The different origins and aims of both instruments result in rather different approaches to data privacy regulation. For example, while the *Convention* relies heavily on the establishment of a supervisory authority with responsibility for enforcement, the OECD *Guidelines* rely on court-driven enforcement mechanisms. These disparities have been reflected in the laws of the countries within the sphere of influence of each model. So, for example, in Europe, privacy abuses are regulated by independent, single-purpose bureaucracies, while in the US, privacy abuses can be regulated by many different government and private bodies (eg the Federal Trade Commission at the federal level, attorneys general at the state levels, and private litigants everywhere).

It is impossible to say which model is more effective, since each reflects the unique regulatory and legal cultures of their respective traditions. Globally, we need to focus on advocating privacy standards to countries around the world. But we should defer to each country to decide on its own regulatory models, given its own traditions.

What is happening now?

Today, a quarter century later, some countries are inspired by the OECD *Guidelines*, others follow the European approach, and some newer ones incorporate hybrid approaches by cherry-picking elements from existing frameworks, while the significant majority of countries still have no privacy regimes at all.

After half a decade of negotiations, in 1995, the EU adopted the data protection Directive 95/46/EC.[4] The EU Directive has a two-fold aim: to protect the right to privacy of individuals, and to facilitate the free flow of personal data between EU member states. Despite its harmonisation purpose, according to a recent EU Commission Communication,[5] the Directive has not been properly implemented in some countries yet. This shows the inherent difficulty in trying to roll out a detailed and strict set of principles, obligations and rights across jurisdictions. However, the Commission has also made it clear that at this stage, it does not envisage submitting any legislative proposals to amend the Directive.

In comparison with other international approaches, EU data privacy laws appear restrictive and cumbersome, particularly as a result of the stringent prohibition on transfers of data to most countries[6] outside the European Union, based around the Commission's view of 'adequacy' of protection in third countries.[7] The EU's formalistic criteria for determining 'adequacy' have been widely criticised: why should Argentina be 'adequate', but not Japan? As a European citizen, why can companies transfer your data (even without your consent) to Argentina and Bulgaria and other 'adequate' countries, but not to the vast majority of the countries of the world, like the US and Japan? In short, if we want to achieve global privacy standards, the European Commission will have to learn to demonstrate more respect for other countries' approaches to privacy regimes.

But at least in Europe there is some degree of harmonisation. In contrast, the US has so far avoided the adoption of an all-encompassing federal privacy regime. Unlike in Europe, the US has traditionally made a distinction between the need for privacy-related legislation in respect of the public and the private sectors. Specific laws have been passed to ensure that government and administrative bodies undertake certain obligations in this field. With regard to the use of personal information by private undertakings, the preferred practice has been to work on the basis of sector-specific laws at a federal level while allowing individual states to develop their own legislative approaches. This has led to a flurry of state laws dealing with a whole range of privacy issues, from spam to pretexting. There are now something like 37 different US state laws requiring security breach notifications to consumers, a patchwork that is hardly ideal for either US consumer confidence or US business compliance.

The complex patchwork of privacy laws in the US has led many people to call for a simplified, uniform and flexible legal framework, and in particular for comprehensive harmonised federal privacy legislation. To kickstart a serious debate on this front, in 2006 a number of leading US corporations set up the Consumer Privacy Legislative Forum,[8] of which Google forms part. It aims to make the case for harmonised legislation. We believe that the same arguments for global privacy standards should also apply to US federal privacy standards: improve consumer protections and confidence by applying a consistent minimum standard, and ease the burdens on businesses trying to comply with multiple (sometimes conflicting) standards.

An increasingly influential approach to privacy legislation has been developing in Canada, particularly since the federal Personal Information Protection and Electronic Documents Act (PIPEDA) was adopted in 2000.[9] The Canadian PIPEDA aims to have the flexibility of the OECD *Guidelines* – on which it is based – while providing the rigour of the European approach. In Canada, as in the US, the law establishes different regimes for the public and private sectors, which allows for a greater focus on each. As has also been happening in the US in recent years with state laws, provincial laws have recently taken a leading role in developing the Canadian model. Despite the fact that PIPEDA creates a privacy framework that requires the provincial laws to be 'substantially similar' to the federal statute, a Parliamentary Committee carrying out a formal review of the existing framework earlier in 2007 recommended reforms for PIPEDA to be modelled on provincial laws. Overall, Canada should be praised for encouraging the development of progressive legislation that serves the interests of citizens and businesses well.

Perhaps the best example of a modern approach to the OECD privacy principles is to be found in the *APEC Privacy Framework*, which has emerged from the work of the 21 countries of the Asia-Pacific Economic Cooperation forum.[10] The *Framework* focuses its attention on ensuring practical and consistent privacy protection across a very wide range of economic and political perspectives that include global powerhouses such as the US and China, plus some key players in the privacy world (some old, some new), such as Australia, Hong Kong, Japan, Korea and New Zealand. In addition to being a sort of modern version of the old OECD *Guidelines*, the *Framework* suggests that privacy legislation should be aimed primarily at preventing harm to individuals from the wrongful collection and misuse of their information. The proposed *Framework* points out that under the new 'preventing harm' principle, any remedial measures should be proportionate to the likelihood and severity of the harm.

Unfortunately, the coexistence of such diverse international approaches to privacy protection has three very damaging consequences: uncertainty for international organisations; unrealistic limits on data flows in conflict with global electronic communications; and ultimately, loss of effective privacy protection.

New (interconnected) drivers for global privacy standards

Against this background, we are witnessing a series of new phenomena that evidence the need for global privacy standards much more compellingly than in the last few decades. The development of communications and technology in the past decade has had a marked economic impact and accelerated what is commonly known as ‘globalisation’. Doing business internationally, exchanging information across borders and providing global services has become the norm. Many organisations and those within them operate across multiple jurisdictions. The internet has made this phenomenon real for everyone.

A welcome concomitant of the unprecedented technological power to collect and share all this personal information on a global basis is the increasing recognition of privacy rights. The concept of privacy and data protection regimes has moved from one discussed by experts at learned conferences to an issue that is discussed and debated by ordinary people who are increasingly used to the trade-offs between privacy and utility in their daily lives. As citizens’ interest in the issue has grown, so, of course has politicians’ interest. The adoption of new and more sophisticated data privacy laws across the world and the radical legal changes affecting more traditional areas of law show that law makers and the courts perceive the need to strengthen the right to privacy. Events that have highlighted the risks attached to the loss or misuse of personal information have led to a continuous demand for greater data security, which often translates into more local laws, such as those requiring the reporting of security breaches,[11] and greater scrutiny.[12]

Routes to the development of global privacy standards

The net result is that we have a fragmentation of competing local regimes, at the same time as the massively increased ability for data to travel globally. To be effective, privacy laws need to go global. But for those laws to be observed and effective, a realistic set of standards must emerge. It is absolutely imperative that these standards are aligned to today’s commercial realities and political needs, but they must also reflect technological realities. Such standards must be strong and credible, but above all they must be clear and they must be workable.

At the moment, there are a number of initiatives that could become the guiding force. As the most recent manifestation of the original OECD privacy principles, one possible route would be to follow the lead of the *APEC Privacy Framework* and extend its ambit of influence beyond the Asia-Pacific region. One good reason for adopting this route is that it already balances very carefully information privacy with business needs and commercial interests. At the same time, it also accords due recognition to cultural and other diversities that exist within its member economies.

One distinctive example of an attempt to rally the UN and the world's leaders behind the adoption of legal instruments of data protection and privacy according to basic principles is the Montreux Declaration of 2005.[13] This declaration probably represents the first official written attempt to encourage every government in the world to think collaboratively, and globally, about privacy protection. It is an ambition that must be praised, although little further was heard about the progress of the Montreux Declaration until the November 2006 International Privacy Commissioners' conference took place and the London initiative was presented.[14] The London Initiative acknowledged that the global challenges that threaten individuals' privacy rights require a global solution. It focuses on the role of the Commissioners' conference to spearhead the necessary actions at an international level. The international privacy commissioners behind the London Initiative argue that concrete suggestions must emerge in order to accomplish international initiatives, harmonise global practices and adopt common positions.

One privacy commissioner who has expressed great interest in taking an international role aimed developing global standards is the UK Information Commissioner. The *Data Protection Strategy* of the ICO published at the end of June 2007 stresses the importance of improving the image, relevance and effectiveness of data protection worldwide and, crucially, recognises the need for simplification.[15]

The way forward

The key priority now should be to build awareness of the need for global privacy standards. Highlighting and understanding the drivers behind this need – globalisation, technological development and emerging threats to privacy rights – will help policy makers better understand the crucial challenge we face and how best to find solutions to address them.

The ultimate goal should be to create minimum standards of privacy protection that meet the expectations and demands of consumers, businesses and governments. Such standards should be relevant today yet flexible enough to meet the needs of an ever-changing world. Such standards must also respect the value of privacy as an innate dimension of the individual. To my mind, the APEC *Framework* is the most promising foundation on which to build, especially since competing models are flawed (the US model is too complex and too much of a patchwork, the EU model is too bureaucratic and inflexible).

As with all goals, we must devise a plan to achieve it. Determining the appropriate international forum for such standards would be an important first step, and this is a choice that belongs in the hands of many different stakeholders. It may be the OECD or the Council of Europe. It may be the International Chamber of Commerce or the World Economic Forum. It may be the International Commissioners' Conference or it may be Unesco. Whatever the right forum is, we should work together to devise a set of standards that reflects the needs of a truly globalised world. That gives each citizen certainty about the rules affecting their data, and the ability to manage their privacy according to their needs. That gives businesses the ability to work within one framework rather than dozens. And that gives governments clear direction about internationally recognised standards, and how they should be applied.

The early initiatives to create global privacy standards have become more urgent and more necessary than ever. With data flowing across the internet and across the globe, this is a reality we have to face together.

Peter Fleischer is Global Privacy Counsel for Google.

Notes

[1] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol No. 11* (Rome: Council of Europe, 1950), available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (accessed 29 Feb 2008).

[2] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal*

Data (Paris: OECD, 1980), available at www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed 29 Feb 2008).

3 Council of Europe, *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (Strasbourg: Council of Europe, 1981), available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (accessed 29 Feb 2008).

4 European Parliament and Council of Europe, 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data', 24 Oct 1995, available at http://eur-lex.europa.eu/ smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (accessed 29 Feb 2008).

5 Commission of the European Communities, 'Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive' (Brussels: CEC, 2007), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/ com_2007_87_f_en.pdf (accessed 29 Feb 2008).

6 European Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries', available at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (accessed 29 Feb 2008).

7 In terms of core European standards, the best description of what the EU privacy authorities would regard as 'adequate data protection' can be found in the Article 29 Working Party's document WP 12. This document is a useful and detailed point of reference to the essence of European data privacy rules, comprising both content principles and procedural requirements. See European Commission, *Working Party on the Protection of Individuals with Regard to the Processing of Personal Data* (Brussels: EC, 1998), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf (accessed 29 Feb 2008).

8 'Consumer privacy legislative forum statement of support in principle for comprehensive consumer privacy legislation', see www.cdt.org/privacy/20060620cplstatement.pdf (accessed 29 Feb 2008).

9 Office of the Privacy Commissioner of Canada, *Personal Information Protection and Electronic Documents Act* (Ottawa: Public Works and Government Services Canada – Publishing, 2000), available at www.privcom.gc.ca/legislation/02_06_01_e.asp (accessed 29 Feb 2008).

10 Asia-Pacific Economic Cooperation Electronic Commerce Steering Group, *APEC Privacy Framework* (nd), available at www.apec.org/apec/news____media/fact_sheets/apec_privacy_framework.html (accessed 5 Mar 2008).

11 Consumers Union, 'Notice of security breach state laws', last updated 2007, available at www.consumersunion.org/campaigns/Breach_laws_May05.pdf (accessed 29 Feb 2008).

12 Article 29 Data Protection Working Party, *Opinion 8/2006 on the Review of the Regulatory Framework for Electronic Communications and Services, with Focus on the ePrivacy Directive*, 1611/06/EN, WP 126 (Brussels: European Commission, 2006), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf (accessed 29 Feb 2008).

13 Montreux Declaration, 'The protection of personal data and privacy in a globalised world: a universal right respecting diversities', 27th International Conference of Data Protection and Privacy Commissioners, 14–16 Sep 2005, available at www.edoeb.admin.ch/dokumentation/00444/01023/01025/index.html?lang=en&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVp3Uhmfhnapmmc7Zi6rZnqCkkINog3yEbKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w== (accessed 29 Feb 2008).

14 London Initiative, 'Communicating data protection and making it more effective', 28th International Conference of Data Protection and Privacy Commissioners, 2–3 Nov 2006, see http://ico.crl.uk.com/files/ComE.PDF (accessed 29 Feb 2008).

[15] ICO, *Data Protection Strategy: Consultation draft* (Wilmslow, Cheshire: ICO, Jun 2007), available at www.ico.gov.uk/upload/documents/library/corporate/notices/ico_dp_strategy_draft.pdf (accessed 29 Feb 2008).

11 The naked machine: privacy and security in an age of terror

Jeffrey Rosen

Since the terrorist attacks of 9/11, I've become convinced that it is possible to design laws and technologies that protect privacy and security at the same time.[1] But it not clear that a political consensus exists, in the US and Britain, to demand that these well-balanced laws and technologies are, in fact, adopted. My interest in this topic was provoked by a challenge from my friend Lawrence Lessig of Stanford University. Not long after 9/11, we were appearing on a panel about privacy and security, and I denounced the proliferation of surveillance cameras in Britain – a technology that threatened privacy without, according to the British government's own studies, having any discernible effect in detecting violent crime or terrorism. Lessig politely but firmly called me a Luddite. Technologies of security will proliferate whether you like it or not, he suggested, and he encouraged me to learn enough about them to be able to describe the architectural and legal choices that could ensure they are designed in ways that protect privacy rather than threaten it.

After studying the laws and technologies adopted in the US and Britain since 9/11, I've become increasingly convinced that Lessig was correct and that each of them can be designed in ways that strike sensible balances between privacy and security. But after describing what these sensible balances might look like, I'd like to ask why these well-designed laws and technologies have not been adopted routinely. Conceptions of privacy vary dramatically among different cultures, and the very different cultural expectations about privacy in Europe and the US have vastly complicated the attempt to achieve comprehensive and balanced regulations.

Let me begin by giving two examples of the kind of technological design choices I have in mind. The simplest example is a high-beam X-ray machine originally tested in London and at Orlando International Airport. Let's call it the 'naked machine', for that's more or less what it is. An electronic strip search, the naked machine reveals not only metal but any plastics or foreign objects concealed under clothing.[2] But it also reveals the human body completely naked.

The naked machine doesn't have to be designed in this way. Researchers at the Pacific Northwest Laboratory identified a simple programming shift that can project the images of plastics or explosives onto a nondescript mannequin, and scramble the images of the naked body into a nondescript blob.[3] With this simple adjustment, the 'blob machine', unlike the naked machine, guarantees just as much security while also protecting privacy. And a version of the blob machine rather than the naked machine was recently deployed at Phoenix International Airport.[4]

Not all the technological choices are so simple, but I'm convinced that most of the technologies of security proposed since 9/11 can be designed in ways that look more like the blob machine than the naked machine. Consider the evolution of the Computer Assisted Passenger Profiling System, or CAPPS II, a controversial data-mining scheme tested by the Transportation Security Agency. In its original incarnation, the CAPPS II system proposed to unite government databases with consumer data held by private data warehouses such as ChoicePoint and Acxiom. Using the same neural network technology used by credit card companies to identify credit card fraud, the initial proposals for CAPPS II proposed to examine passengers' living arrangements and travel and real estate history, along with a great deal of demographic, financial and other personal information, to determine whether or not individual passengers resembled the 9/11 terrorists. Based on their risk index, the CAPPS II program proposed to label travellers as 'green', 'yellow' or 'red' security risks, and subject them to correspondingly intrusive scrutiny.[5]

In its original form, CAPPS II was a naked machine-like technology that raised two important objections – it was unlikely to increase security and it posed grave threats to privacy. The security objection is that terrorism is not the kind of activity that follows predictable patterns – the next attack is unlikely to resemble the last one. Unlike people who commit credit-card fraud – a form of systematic, repetitive and predictable behaviour that fits a consistent profile identified by millions of transactions – there is no reason to believe that terrorists in the future will resemble those in the past. There were only 11 hijackers on 9/11, and those who followed them the next year weren't Saudi Arabians who went to flight school in Florida; they included Richard Reeves, the English citizen who hid a bomb in his shoe, and who had a Jamaican father and an English mother.

By trying to identify people who look like the 9/11 hijackers, the profiling scheme is looking for a needle in a haystack, but the colour and the shape of the needle keep changing. 'Some terrorism experts are sceptical about terrorist profiling,' indicates a 1999 report prepared by the Library of Congress for US intelligence agencies. 'There seems to be general agreement among psychologists that there is no particular psychological attribute that can be used to describe the terrorist or any "personality" that is distinctive of terrorists.'[6] For this reason, the US Secret Service, which once looked for people who fit profiles of stereotypes of presidential assassins, has abandoned its personality profiles and now looks for patterns of motive or behaviour.[7]

Moreover, because the sample of known terrorists is so small, attempts to identify suspects with electronic profiles are bound to produce a high number of 'false positives' – that is, passengers whom the system wrongly identifies as likely terrorists – and the costs of the system are likely to outweigh its benefits. To illustrate why data-profiling systems are likely to be ineffective in looking for needles in haystacks, Christopher Guzelian and Mariano-Florentino Cuéllar of Stanford Law School note that, at one point, doctors used to recommend monitoring large numbers of people for signs of latent diseases such as diabetes or ovarian, lung or skin cancer. But because of the inaccuracy of profiling systems in identifying symptoms that occur very rarely in the population at large, the medical establishment has concluded that the benefits of monitoring are outweighed by the costs, which include not only false positives – or people wrongly identified as being sick – but also false negatives – or people wrongly identified as being healthy.[8]

In the case of terrorism, of course, the prevalence of potential terrorists in the population as a whole is unknown. But imagine a profiling system that was set up to identify the 11 hijackers of 9/11. Searching for 11 individuals in a population of 300 million would yield exponentially more false positives: even assuming the profiling system is 99 per cent accurate, because of the low prevalence rate, 3,000,000 (that's 0.01 × 300 million) of those identified as potential terrorists by the system would be wrongly accused. Such a system would bring the nation's airports to a halt. In other words, only 0.000363 per cent of the people who tested positive in a nearly perfect system actually would be positive – a success rate so low that the system would have to be stopping a nuclear bomb on the benefits side and imposing little more than a pat-down on the costs side to be justified.

But, in fact, of course, no data-mining system has proved to be 99 per cent accurate in predicting terrorist behaviour, because the new attacks so rarely resemble the previous ones. A system with only 1 per cent accuracy would falsely accuse nearly all innocent travellers of being terrorists and correctly identify only a fraction of terrorists while missing nearly all of the real terrorists. No rational evaluation of costs and benefits would support the adoption of such a hopeless system as an effective tool for national security. For this reason, efforts to use dataveillance as a way of predicting terrorist behaviour in the population at large, rather than investigating individuals who have been identified as terrorists by other means, seems empirically dubious.

In its original form, the CAPPS II system also posed grave threats to privacy. The designers of the system proposed to include in its database not only the passenger data that airlines currently maintain as part of the Computer Assisted Passenger Profiling System, or CAPPS – such as travel history, address and telephone number – but also publicly available marketing data that is currently maintained by private companies. This could include living arrangements, household income, pet ownership, personal buying habits, and even lists of the books we buy and the music we listen to.

In addition, some of the companies contacted by the government hoped to include personal data whose use is currently restricted by law, including records of individual credit card purchases of fertiliser or flight school lessons, for example, or international telephone calls to Afghanistan. Because CAPPS II, as originally proposed, included no controls on the use of this data, it would have been possible for the government to scan a traveller's consumer behaviour and telephone calls, share unusual behaviour with law enforcement agencies, and prosecute him for low-level offences that had nothing to do with terrorism. This raised a danger of politically discriminatory prosecutions of the kind that President Nixon engaged in when he scanned the tax returns of Vietnam protesters and threatened them with exposure. It was the effort to avoid this kind of Nixon effect that led Congress to pass the Privacy Act of 1974.

Happily, the CAPPS II system was redesigned in ways that look far more like the blob machine than the naked machine. Two important design modifications are worth noting.

First, the system is now limited to the goal of 'authenticating' that individual airline passengers are who they say they are, rather than trying to identify them as possible terrorists based on their consumer profiles. By focusing on authentification rather than identification, the system avoids the dangers of false positives that arise from predictive data mining and is likely to be a more effective technology of security.

Second, as for privacy, the system now includes controls on the secondary uses of data. In its initial announcement, the administration proposed to share personal data from the CAPPS II system with national and international police to allow the prosecution of any civil or criminal violations. But critics objected that this could create widespread abuses, allowing the administration to scour the personal data of millions of people, uncover relatively minor offences, and threaten its critics with vindictive prosecutions. In response to these criticisms, the Transportation Security Agency agreed to restrict officials from sharing personal data with law enforcement agencies, except in the cases of individuals who had an outstanding federal warrant for a violent crime.

This was a welcome and important victory for privacy. It recognises an insight that some European countries have adopted in designing technologies of security. The German wiretap law, for example, allows intelligence authorities to use wiretaps for domestic surveillance only when there is factual basis to suspect that one of a list of crimes involving a threat to national security has been or is about to be committed. The German law says that evidence obtained through wiretapping can be used only in the investigation and prosecution of the specified national security crimes or certain other serious crimes; if the intelligence officers find evidence of low-level crimes, they may not share it with law enforcement officers or introduce it in court.[9]

Because of Germany's distinctive history with the Nazis and the Stasi, the German intelligence services have been constrained by a special sensitivity to privacy. Unlike Germany, however, the US has no comprehensive regulation of the sharing of information by commercial databases in the private sector. As a result, the victory of CAPPS II may prove to be illusory, and much of the data mining originally proposed by the government may be contracted out to private organisations whose use of the data is unconstrained. To construct an effective blob machine-like regime of data mining, the US would need a combination of public and private sector regulation of the kind that libertarians in Congress are reluctant to embrace. A bipartisan coalition of civil libertarian liberals and libertarian conservatives has proved effective in resisting the executive's most dramatic proposals for government surveillance after 9/11. But because of its suspicion of private sector regulation, the same coalition has been unwilling to consider the kind of complicated compromises and controls on the use of data by the public sector that an effective blob machine technology would require.

Although the blob machine and the CAPPS system represent important victories for a sensible balance between privacy and security, there have been many important defeats as well – defeats such the expansion of National Security Letters in the USA Patriot Act, which allow the government to seize any data merely by asserting its relevance to a terrorism investigation. National Security Letters could have been designed with controls on the sharing of data between intelligence officers and law enforcement offers, but they were not – and as a result, the Inspector General of the FBI found that they were gravely abused.

The expansion of the use of security cameras in the US represents another defeat for privacy. Right after 9/11, Washington DC proposed to create a 'British-style' surveillance system for the city, despite the British government's own survey of the empirical evidence, which concluded that the proliferation in cameras since the 1990s had had no effect on violent crime[10] or terrorism. (The cameras may be more useful in identifying the perpetrators after an attack, although in most cases, it appears that major terrorist suspects would have been identified without them.) Initially, the political debate about cameras evolved differently in England and the US.

Despite the support of community leaders in Washington, who demanded more cameras as a way of making their constituents feel safer, the vigorous coalition of libertarian conservatives and civil libertarian liberals that had opposed the cameras before 9/11 converged again to oppose the expansion of their use. After several hearings before the City Council, where the case against the cameras was forcefully presented, the Metropolitan Police Department retreated from its original plans. It abandoned an early draft of its proposed regulations, which had promised to use the cameras to deter and/or eliminate crime in residential and commercial areas. In the face of libertarian opposition, the department promised to use the cameras only in exigent circumstances and not for general crime deterrence, unless legislation was enacted to the contrary. The regulations also pledged that the cameras would be turned on only for limited time periods, at the direction of the Chief of Police, and that recorded images would ordinarily be erased after ten days.

The City Council endorsed the regulations, but it also unwisely funded a so-called pilot programme to allow cameras to be put up in Washington neighbourhoods and to study their effect on general crime prevention, detection, deterrence and investigation. And in 2006, after a British political activist was murdered in Georgetown, the council reversed its decision and endorsed an expansive surveillance system without the previously adopted restraints on the use of the images. In New York City, the debate was similar: the City initially resisted proposals by the former head of the New York Police Department to expand surveillance after 9/11, but in the wake of the London tube bombings, the mayor embraced an expansive surveillance system, which will soon be implemented. The surveillance debate in the US and Britain, ultimately, suggests that people are more concerned about feeling safe than adopting oversight mechanisms for surveillance cameras that can protect privacy and security at the same time.

I'm increasingly convinced that political and cultural constraints may make effective regulation of technologies of security difficult to obtain. There are no generally shared intuitions about privacy: different countries respond to different dangers in different ways. To put the problem in brief: Americans tend to be much more concerned about government surveillance while Europeans tend to be more concerned about privacy invasions by the private sector, but because of the complicated technological interplay of public and private surveillance, any effective regulatory scheme has to take account of both concerns. Contrast American and European attitudes about financial information.

Europeans are far more sensitive than Americans about disclosing financial information, steeped as they are in the aristocratic tradition that respectable people don't discuss money in public. And European law reflects this squeamishness. The traditional rule in France made it a violation of privacy rights to reveal another person's salary, and for hundreds of years the French nobility successfully resisted laws requiring public registration of their mortgages. In France and Germany today, consumer credit reports are available only in the case of people in financial difficulties. In Germany, consumers seeking credit must explicitly authorise lenders to share information about them, and before any information can be shared, the privacy interest of the borrower must be balanced against the commercial interests of the lender.[11]

Financial reporting is not the only area in which Americans' cultural ideas about privacy differ dramatically from those in Europe. If visitors from Europe are scandalised by the casual way Americans discuss their salaries with strangers, they are also surprised by Americans' discomfort with public nudity on beaches or with female bathroom attendants in men's restrooms. At the same time, Europeans are far more trusting of government, and willing to allow it to regulate personal choices in ways that Americans would find intolerable – such as the naming of infants, for example. And these cultural differences are reflected in dramatic differences in law. European law protects not only consumer data and credit reporting but also email privacy in the workplace, discovery in civil cases, and the distribution of nude pictures on the internet, while US law allows dramatic violations of privacy in all of these areas.

'Why is it that French people won't talk about their salaries but will take off their bikini tops?' James Whitman of Yale Law School asks in a path-breaking article entitled 'The two western cultures of privacy'. 'Why is it that Americans comply with court discovery orders that open essentially all of their documents for inspection but refuse to carry identity cards?'[12] Whitman's answer is succinctly expressed in his subtitle: 'dignity versus liberty'. When Europeans think about privacy, they are most concerned about personal dignity and the right to control one's public image – a right threatened primarily by the mass media, the internet and commercial data warehouses. By contrast, US conceptions of privacy are focused on personal liberty and the right to be free from state surveillance, threatened primarily by government intrusions into the home.

The European conception of privacy as a protection for dignity rather than liberty, Whitman argues, stems from its aristocratic tradition of protecting personal honour. For most of European history, this was a hierarchical tradition: for some people to have honour, it was necessary for others not to have it, and for people to be treated with the honour to which they were entitled by their station, everyone had to know his or her place. But over the course of the nineteenth century, the defence of personal honour and interpersonal respect began to migrate from something that high-status people expected to defend through law. And during the twentieth century, the legal protections against personal insult were increasingly 'levelled up',[13] as Whitman puts it, and extended to all citizens, not only high-status ones. Repeatedly, however, the legal protections for personal honour in Europe clashed with two freedoms that Americans take for granted – property rights and freedom of the press.

The cultural differences between European and American conceptions of privacy have important legal implications for their attempts to balance privacy and security. Europeans tend in general to be less suspicious of centralised government authority than Americans. As Kim Lane Scheppele of the University of Pennsylvania has noted, Europe's greater deference to government authority led countries like Germany and France to adopt surveillance measures after 9/11 that in some ways went farther than the USA Patriot Act. In 2002, for example, Germany adopted a sweeping law that increased the power of its security agencies in important ways. The government was authorised to create a central database with personal information about foreigners, including fingerprints and religious background. The law also authorised German national identification cards to include biometric data, such as fingerprints. And it explicitly endorsed data mining along the Total Information Awareness model, requiring government agencies to turn personal information over to the federal police.[14]

The great variation between the European and the US response to 9/11 reflects our different historical conceptions of privacy and state authority, but it also poses a challenge to policy makers: in an age of integrated databases and the internet, it may be costly to have very different rules about what sort of information can be shared among and between intelligence agencies, law enforcement officials, and the private sector in the US and Europe. It is now conventional wisdom, in fact, that increased information sharing is the best way of preventing terrorism, but information sharing between the public and private sectors may be difficult if the Americans are focused on the dangers of state surveillance and the Europeans are concerned about protecting the dignity of the consumer. At the same time, in the age of the internet, attempts to protect the rights of Europeans to control the distribution of their images in the name of dignity may be thwarted by the refusal of cyberspace to respect national boundaries.

Is there any possibility for privacy advocates to expand the cultural understandings of privacy in Europe and the US, so that the Europeans come to care more about liberty and the Americans more about dignity? When it comes to the protection of privacy, legal values tend to reflect and follow social understandings, rather than the other way around. Perhaps those who hope to import European understandings of privacy into the US, and vice versa, should focus on changing social understandings of privacy rather than on passing new laws. But can social understandings of privacy be changed easily to accommodate both honour and liberty? Not necessarily.

An unsettling possibility for privacy advocates is that as Europe becomes more and more like the US – that is, more market driven, less hierarchical, more democratic and more distant from its aristocratic past – the popular consensus about the importance of protecting dignity will atrophy and eventually collapse under the weight of market forces. A society where citizens refuse to respect their own privacy is not one where privacy will be long respected; and the US experience suggests that citizens in an individualistic market democracy may perceive too many market rewards for exposure to respect their own privacy for long.

As European traditions of dignity are withering in the face of US-style assaults of the market, US traditions of suspicion of government may be threatened by the persistent anxieties of an age of terrorism. It's not hard to imagine, in the face of future attacks, the bipartisan libertarian coalition being overwhelmed in the face of public demands for security above all. Unrestrained by libertarian minorities, the public in a public opinion state will sacrifice privacy to security at every turn.

All this reminds us that privacy – understood as a protection for dignity or as a bulwark for liberty – is not an especially democratic virtue. It is a virtue historically demanded and enjoyed by aristocratic minorities and extended, in Europe and the US, to a broader population that often was indifferent to its benefits and demands. Dignity requires a degree of self-restraint on the part of citizens – good manners, reticence, self-respect and a willingness to respect the dignity of others; while liberty requires a degree of civic engagement – only informed and educated citizens can check the excesses of the state. Neither dignity nor liberty can easily be achieved in a nation of anxious exhibitionists, more concerned about attracting attention than deflecting it. To defend privacy, in other words, citizens in democracy have to care about privacy, and it's increasingly clear that many of us do not.

Jeffrey Rosen is a law professor at George Washington University and the legal affairs editor of the New Republic.

Notes

[1] This essay is adapted from J Rosen, *The Naked Crowd: Reclaiming security and freedom in an anxious age* (New York: Random House, 2004); and J Rosen, 'The silver bullet: protecting privacy and security through law and technology', *Proceedings of the American Philosophical Society* 151, no 3 (Sep 2007).

[2] K Maney, 'The naked truth about a possible airport screening device', *USA Today*, 7 Aug 2002.

[3] M Hamer, 'All-seeing scan spares your blushes', *New Scientist*, 17 Aug 2002.

[4] P Giblin and E Lipton, 'New airport X-rays scan bodies, not bags', *New York Times*, 4 Feb 2007.

[5] R O'Harrow Jr, 'Air security focusing on flier screening: complex profiling network months behind schedule', *Washington Post*, 4 Sep 2002.

[6] RA Hudson and the staff of the Federal Research Division of the Library of Congress, *Who Becomes a Terrorist and Why: The 1999 government report on profiling terrorists* (Guilford, CT: Lyons Press, 1999).

[7] Ibid.

[8] C Guzelian and M-F Cuéllar, 'When terrorists are the needles and America is the haystack', unpublished draft on file with the author.

[9] CM Bradley, 'The exclusionary rule in Germany', *Harvard Law Review* 96 (1983).

[10] BC Welsh and DP Farrington, *Crime Prevention Effects of Closed Circuit Television: A systematic review*, Home Office Research Study 252 (London: Home Office Research, Development and Statistics Directorate, Aug 2002), available at www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf (accessed 29 Feb 2008).

[11] JQ Whitman, 'The two western cultures of privacy: dignity versus liberty', *Yale Law Journal* 113 (2004).

[12] Ibid.

[13] Ibid.

[14] K Lane Scheppele, 'Other people's patriot acts: Europe's response to September 11', *Loyola Law Review* 50 (2004).

12 The culture of control

Simon Davies

Mass surveillance, together with the consequent erosion of personal privacy, has become an enduring theme throughout the spheres of media and politics. Privacy protection, in the guise of data protection, has permeated technological and legislative development across the world. Formerly arcane issues such as encryption, transborder data flows and predictive profiling have captured the public imagination and sparked headlines in every newspaper. Throughout the past quarter century, no other fundamental right in the arena of public policy has generated such turbulence and controversy.

Since 2003 the number of parliamentary inquiries, legal challenges, media stories and academic papers on the subject of privacy has risen to an unprecedented extent. Indeed, privacy protection in its many forms can now be seen as an industry in its own right, employing many thousands as regulatory staff, advocates and writers.

Despite these dynamics privacy is fatally disadvantaged for two primary reasons. First, the concepts of embedded surveillance and perfect identity in our information systems have gained acceptance faster than the concepts of embedded privacy and anonymity. Second, governments in charge of large information systems have the luxury of writing the rules. Exemptions in favour of surveillance are written into law on the basis of a stated ‘public interest’, while requirements for the protection of privacy rarely have such a weighty pedigree.

Public interest exemptions from data protection laws have resulted in wholesale violations of privacy. The imposition by financial services regulators and insurance companies of statutory and non-statutory reporting and audit requirements creates a further imbalance. While acknowledging the importance of privacy as a fundamental right, data controllers argue that surveillance is necessary to maintain law and order and to create economic efficiency, and that privacy rights in general must remain subject to constraints of fiscal and public interest. Thus despite the burgeoning activity in privacy regulation, surveillance continues to expand while privacy laws continue to degrade.

It is possible that the current interest in privacy stems from the broader concern over loss of human autonomy. The number of people each year who are restrained or disciplined by legal, administrative and judicial mechanisms is a thousand per cent greater than 20 years ago. Legislation regulating conduct in public has increased 15-fold in the same period. The requirement for 'permission' to initiate group activities has soared. It can now be argued successfully that individual freedom is no longer conditioned by what is expressly prohibited in law, but instead is circumscribed by what the law expressly permits. In this context privacy takes on a libertarian aspect and thus becomes the standard bearer for the general issue of freedoms.

That we are entering an age of the 'surveillance society' is without dispute. In 1999 Privacy International estimated that almost a million people in the UK alone conduct at least a degree of surveillance as part of their employment. In the same year, the organisation also undertook a study to find out how much information was being held on each of us. The findings were quite remarkable, concluding that details of each economically active adult in the developed world were located in an average of around 500 major databases, creating enough processed data to compile a lengthy reference book on each person. When Privacy International conducted the survey again in 2002 at the request of the *Guardian* newspaper, the organisation found that the number of computer systems processing information on the average citizen had shot to more than 700.[1]

It is equally true that the government has largely abandoned any responsibility for protection of privacy – or, at least, abandoned any responsibility to keep surveillance in check. While it is true that many government departments are obsessed with data protection compliance, they are less interested in controlling surveillance. The Health and Social Care Act removes the traditional right of patients to control their own health information, transferring the ownership of this data to the Secretary of State. The Identity Cards Act 2006 will place all key personal information under the control of the Home Secretary. Legislation since 1995 has permitted a range of public authorities the right to share information on every UK resident. Each of these laws progressively undermines the provisions of the Data Protection Act, a law designed (albeit to a minimum standard of protection) to preserve citizen rights over personal information.

This trend is symptomatic of a broader arrogance within government – one that has lubricated the wheels of control. Former Cabinet Secretary Lord Butler knew this when he launched into a remarkable attack on the Blair style of government, accusing it of control-freakery and intellectual paucity. He bemoaned the decline of Parliament, the obscene power of the whips and the puppeteer role adopted by the Executive.

Butler was among good company. A brief review of the investigations conducted by parliamentary oversight committees provides ample evidence that the government has permitted a wholesale and systematic abrogation of its responsibility not just to privacy but also to the democratic process. Increasing anxiety expressed by the Human Rights Committee has been all but entirely ignored. The Public Administration Select Committee has expressed continuing disappointment about a range of concerns from the conduct of government inquiries to the way ministers answer questions. The Constitution Committee has given up on hoping to effect any change on government thinking.

Once independent oversight is removed the ethos of surveillance can flourish. It also occurs through a more systemic process. A huge shift has taken place since the 1980s in the way governments view the ordinary citizen. In the past, surveillance was based on the targeting of specific individuals or groups. Now, systematic surveillance proactively profiles millions of people at a time. In their often-futile quest to second-guess the bad guys, authorities have chosen to treat everyone as a potential suspect. Instead of working to build a profile on particular suspects, authorities now use template criminal profiles that are matched against the entire population. This is the way, for example, that airline passengers are screened.

This trend has been evident for decades. In 1988 privacy guru David Flaherty was writing and teaching about the growth of surveillance societies and postulating that part of the cause lay with the inability of regulators to face up to the challenges of a turbulent policy domain. For almost 20 years the idea of a surveillance society has been well known to academics, even though the expression in the twenty-first century is exciting and fashionable.

The effect of the surveillance society, whether intended or not, is a push to normalise human behaviour with the motivation of promoting 'good' and socially responsible conduct. Deviants, when identified, are penalised in myriad ways never before imagined. With escalating regulation, deviation is increasingly probable, and with increasing surveillance deviation is easier to detect. A shrinking 'zone of normality' has been constructed. Individuals may step outside this domain, but they will be more vulnerable, exposed and observed than ever before. Little wonder that the libertarian instinct gravitates to privacy.

Some people argue that this trend is justified. They say privacy cannot be sustained in an age of organised crime and terror, and that public interest exemptions to privacy law are legitimate and necessary. This view assumes a benign approach by law makers and data controllers in which wise people gather in sensitive dialogue over such questions. The reality should give rise to a far more cynical view. To be blunt, privacy is widely perceived as a nuisance. In theory at least it limits data flows, prevents the sale of valuable data to third parties and stops entities from establishing surveillance simply for the sake of surveillance. And were it not for the institutional vandalism of this right the law might very well have offered those protections.

For advocates, the value of privacy as a boundary between the intrusion of state and society and as a right of an individual to say 'go away' is self-evident. To many millions of people who express anxiety at privacy invasion in its many forms such a view is equally self-evident. The interesting question that emerges is why the surveillance society has been permitted to grow at such a pace.

It is superficially tempting to imagine that the cause of mass surveillance and loss of privacy is due to the increasing power and capacity of modern IT systems. However, there are four additional factors. First, individuals – while consistently expressing anxiety about privacy invasion – are overwhelmed by the processes required to enforce protection of their privacy. Resistance to the use of conventional encryption techniques is one example. Second, privacy and data protection regulators are frequently fatalistic, timid or under-resourced, resulting in management that is based on reaction rather than advocacy. Third, many protections – whether legal or technological – are frequently undermined by options to discard privacy through inducement, exemption or coercion.

The fourth and final reason is perhaps the most disquieting. The ancient idea of privacy as a public interest in its own right (similar to the right of free expression) has been all but extinguished. Instead of being viewed by authorities as a right and proper means of determining the autonomy of the individual set against the values of society, privacy is now interpreted as a 'selfish' right or at best a 'group' right relating to specific populations (such as those using the roads in the case of road-user charging or those wishing to shop on the high street in the case of public CCTV). The result has been to exorcise from the public imagination any instinctive notion that privacy is a fundamental right.

The means of achieving this important change are subtle but obvious. The imagery, context and language surrounding both privacy and surveillance have been substantially altered.

The idea of 'the good, law-abiding and honest' citizen has been eliminated. Successive governments have engineered an environment in which all citizens must be watched at all times. The ancient burden of proof – the presumption of innocence – has been reversed. This phenomenon has come about partly because it is not acceptable to 'single out' particular groups or classes, even if they may be known historically to be the cause of particular problems. However, it is primarily due to a flourishing philosophy that only those with something to hide would have something to fear from surveillance. The maxim 'no one is above the law' has become 'no one is above suspicion'.

Indeed the UK, like Australia and the Netherlands, has mastered this new governance. The Children Act 2004, for example, provides for the profiling and analysis of all children to detect which infants may be potential criminals. The Regulation of Investigatory Powers Act 2000 makes provision for the universal archiving of all communications records (phone, email and internet visits) for possible later use by authorities. A raft of new laws on border security, travel and immigration controls assume that all travellers, UK nationals and others, are potential criminals and should be subjected to constant tracking and profiling. Financial regulations increasingly assume that innocence on the part of bank customers is dependent on a constantly narrowing zone of normal account behaviour determined by constant analysis.

The Dutch syndrome, like that in the UK, is symptomatic of a trend across the world. Once a confident and freedom-loving society with a deep liberal pathology and libertarian inspiration, the Dutch nation has been largely transformed into a control culture. In the space of 30 years it has moved from a place where a mass movement paralysed the national census, to a place where government could, without controversy, institute the most extensive wiretapping infrastructure in the Western world. From its comfortable position as a global melting pot of cultures it has become a reactive and sometimes xenophobic surveillance society. In doing so it has set a lead for many countries in Europe.

A similar trend has emerged half a world away in Australia. Less than 20 years ago a fiery individualist spirit sparked a vast campaign of popular opposition to the government's proposed national identity card. Fuelled by recollections of the nineteenth-century 'Eureka Stockade', tens of thousands marched in the streets to oppose an initiative that government had figured was an entirely reasonable proposal. The card fell, and so – very nearly – did the government.

Half a generation later, the Australian people have capitulated to controls once undreamed of. Smoking has been banned in all public places (including beaches), restaurants are prohibited from giving their customers 'doggy bags' (their leftovers from dinner) and all bank accounts, geographic movements and personal details are routinely scrutinised by government. Again, hardly a syllable of dissent is expressed.

France, Germany, Russia and countries throughout the Asian region are taking the same route. Only in the US is there a slight deviation. There, constitutional protections limit such activities by the federal government, but the states and the private sector are out of control.

These dramatic cultural shifts have occurred throughout the world. It can be postulated that they have transpired because of the combined influence of an oppressive mass of legal requirements, routine surveillance and an equally oppressive mass of judicial sanctions. It is also likely that cultures have changed because of clever marketing of control initiatives.

Simon Davies is Director of Privacy International.

Notes

[1] S Andrews, *Privacy and Human Rights 2002* (Washington, DC: Electronic Privacy Information Center, and London, UK: Privacy International, 2002), see www.privacyinternational.org/survey/phr2002/ (accessed 5 Mar 2008).

13 The architecture of privacy: space, power and human rights

Markus Miessen and International Festival

It is just over ten years ago since Hotmail was first released. A decade later, it is handling approximately 100 million emails a day, covering 230 million users. Text messaging on mobile phones appeared around the same time; ten years on the worldwide volume of SMS is estimated to be in the hundreds of billion messages. Amazon and eBay were created in 1995. Google was unleashed in September 1999 from a garage in Palo Alto, and in the spring of 2007 it claimed to handle 300 million queries per day; more than 100 billion per year.[1]

Considering the same ten years in relation to concepts of privacy, it is quite easy to argue that adjustments are small in perspective as we adapt incrementally to a proliferation of communication tools and the opportunities they bring. Most are more than happy to adjust: social networking sites were unheard of a short time ago; now, we do not blink before putting photographs and details of our lives online. But, given these tools' ubiquity, these adaptations have profound implications. As recent newspaper headlines about the potentially pernicious side-effects of our online openness suggest, the public is getting increasingly jittery about what exactly we have given up when we invite the world to ponder our identity as well as gaze at last eve's party pics.

There are some fundamental principles underlying privacy. Privacy is about relationships between people: it relates to the ways that boundaries are drawn between us, them, me and you. The way we value our privacy helps to produce our sense of who we are and what others mean to us. But as we shall see in the next section, it is those very relationships that have changed; our affiliation and 'closeness' to the people around us has become more contested – disrupting our sense of where we stand socially.

If privacy is a function of new ways of behaving, communicating and organising, but the principles behind it remain the same, then the question remains: what has happened to privacy? This essay attempts to answer this by approaching privacy as a socio-spatial concept. As is the case through the boundaries between home and street for example, the space around us comes to reflect the priorities of privacy: who we choose to let 'in' to spaces and who we choose to keep out. Through stipulations about minimum overlooking distance and the often mandatory half metre between pavement and front door, such considerations are in fact at the heart of the UK planning system. This is no trivial matter; the way spaces are organised is not only a result of, but helps to shape, relationships between people and groups, and influences how people understand their identity, position vis-à-vis others and culture of everyday life.

Privacy as process

Discourses around privacy tend to idealise a privacy that is an immutable right. But it is important that we avoid addressing privacy through a question of *what*, and to think in terms of the 'particular': of when, how, for whom, to which end and through which mechanisms privacy is valuable. We need to respect a priori how context-specific privacy is. That means thinking not of a 'thing' to be defended – a space we can retreat to, a set of information we should never have to give away – and instead looking at privacy as a process of negotiation. We don't just enjoy privacy, we perform and reproduce it every day. From this it follows that, in relating it to the protection and empowerment of the individual, we need to understand privacy not as a right to a thing, but rather as a right to be part of that performance and negotiation. Rather than something set in stone, the human 'right' to privacy is bound up in the right to self-determination.

This negotiation of privacy happens every day. Every morning on the way to work, thousands of us 'produce' privacy by opening a book, reading a newspaper, working on a laptop, or listening to MP3 players. The space that is created is often not physical, but has physical effects. Privacy, on the crowded train or bus, for example, is about creating anonymity, and on occasion a sense of security. It means being able to influence where we set out boundaries between others and ourselves.

This is an inherently political endeavour. There are moments where established understandings of the boundaries of privacy have been disrupted and exposed as such. The act of disrupting or giving up privacy can be understood as political if we consider that the privacy we are granted or demand is the result of social or economic interests. For example, the feminist emphasis on the personal as political took aim at a sphere that was considered private: the home. In highlighting domestic behaviour, the home became the point where privacy reinforces a particular relationship of power.[2] The ability to challenge the established principles of privacy is as important as the ability to set them up.

Privacy as process can be a tool to demand that the society around us remains open to renegotiation – that the relationships that constitute that society are fluid and contestable. But at the same time, it can be a tool through which influence and power can be wielded – where it is deployed as a *reactive* tool, reinforcing prejudice and legitimising crimes against humanity. At its most extreme, this is evident in the examples of Abu Ghraib and Guantanamo Bay. In this essay, we will use these examples to show that this architectural expression of a society's approach to underlying principles of privacy can have severe, violent consequences. Such excesses have to be seen against the background of a moment of 'crisis' in which globalisation and technological change have destabilised established norms, values and expectations regarding privacy. This could be a moment of opportunity in which societies can formulate, demand and express an approach to privacy that is *productive* and always under negotiation. We argue that planners, architects and spatial practitioners need to be involved in the debate over privacy because their work embodies choices made about the relationships that privacy speaks of.

Crisis? What crisis?

What exactly has changed in the recent past that throws our idea of privacy into this state of crisis? The technological advancements we spoke of above are products of an age in which people have the ability to communicate and organise like never before. The progressive triumph of globalising market capitalism has seen an emphasis on flows of people, finance and ideas. Integral to this has been a progressive commercialisation of resources that were formerly publicly guaranteed. This has opened up new market spaces, for example in telecommunications – driving technological innovation but also dramatic change in the relationship between person and public domain, state and market. Coincident with that has been a roll-back of the direct power of the state, or institutions that mediate between individuals and representative collective interests. While these trends have often sought to emphasise the empowerment of individuals, there has been a loosening of the ties between people and these types of institutions.

It is no surprise that the concept of precariousness has often accompanied these stories of global change. Let us follow the example of Isabell Lorey's argument on precariousness.[3] In the 1960s, the archetypical 'precarious' person was a somebody who stepped out of (or was ejected from) a strongly homogenous society and thereby produced 'alternative' communities. These stood in a marginal relationship to the rest of society. As she and others such as Chantal Mouffe argue, the 1980s saw precariousness becoming a more generalised condition, a feature of everyday life. Suddenly, hitherto relatively stable notions of work, family and cultural networks became precarious. People's relationships to their jobs changed, and certainty with regard to their sense of who they are became harder to find. At the same time, 'mainstream' culture and society has become increasingly fragmented – the rising significance of the 'Long Tail',[4] for example, and the declining consumption of mass media suggest a society turning towards the niche. Precariousness is becoming mainstream.

Since precariousness is now a shared societal condition, it conditions the ways in which citizens negotiate moments of privacy in daily life. The task we must set is to recognise opportunities for a radically different form of privacy that intervenes and works *with* the social context – the way that we understand each other – rather than simply reacting to 'threats' alone. Our job should be to work out how the relationships that we connect to privacy are (and can be) produced and reproduced to benefit genuinely from this opportunity moment.

In this moment of flux, there are potentially different incentives for government, private sector and the general public that could drive how privacy is approached and produced. The current condition of precariousness makes this a key moment in which to consider privacy, because the crisis moment can either prompt an empowering renegotiation of relations, or instead a profoundly threatening trend. This latter, reactive aspect is a powerful force. As we shall see, it can prompt a reaction against those deemed ‘outside’ or threatening to the remaining ideals of togetherness and commonality – those who invade our privacy and disrupt our fraught and increasingly unattainable sense of security and stability.

This also implies that the institutions that profess to provide such protection are relevant, something especially evident in the light of increasingly prominent security concerns. Just as we question their accountability to democratic control, we ought to continuously interrogate what spatial syntax they produce and its implications for those who are co-producing spatial outcomes. In sum, this is a moment in which we can, or should, re-establish a collective ability to engage in the process of negotiating the relationships on which privacy depends, and through which it is inscribed in space.

The privacy we want, and the privacy we get

But what are the influences and interests that pull and shape how privacy is produced? We focus here on two areas: corporate or private sector interests, and the interests of the state. Their actions are a necessary product of their need to manage populations, albeit for different ends. Through the operating of both, space and the places around us come to reflect how privacy is valued. Far from being something imposed on us by overt force, this happens partly through gradual seduction.

From a corporate perspective, the present state of flux is positive. Corporate economies support fragmentation, movement and breaks, as a means to continuously re-contextualise demands. Insight in our private sphere is evidently favourable, because it allows for a tailoring of products and offers to individuals’ perceived aspiration, want or need. But it is too hasty to consider that corporate economies are interested in full transparency or the wholesale abolishment of the private sphere. Instead their interest lies in a highly dynamic and heterogeneous private sphere, as long as it remains open to measurement with sophisticated marketing tools.

On the one hand, businesses need access to our private realm; they need to learn about what we do and who we are. But at the same time, people's compulsion to consume is based in and dependent on the very private sphere, on the idea that marketised goods reflect our inner self – that they help us craft, define and communicate 'who I am'. Hence the privacy enunciated by corporate economies is simultaneously expanding and contracting; without (at least the illusion of) private and individual selves, the 'dividual'[5] of companies' samples, data and targeted products become meaningless.

This is not just true for products; the same process has been at work in urban space at large. Fuelled by the increasing aesthetic reflexivity of urban populations, resulting in the more conscious crafting of lifestyles, such identities – aggregated from individual to recognisable and marketable groups – get inscribed into space. What is striking about present-day urban space is not the extent to which we have accepted intrusions in our privacy with CCTV cameras, but the extent to which public space is segmented according to lifestyle groups and communities of interest. This process has eclipsed the general public, annihilating that classic element of urban sociology, the 'anonymous crowd'. The flaneur is no longer the ultimate individual but an urban 'dividual', member of one of many 'commodity publics', catered for by themed urban spaces, the physical equivalent of the highly self-selecting social dynamic that forms the core of Facebook's success.[6]

These influences work in a moment in which the relationships that privacy embodies are seemingly up for grabs. The moment of crisis constitutes a dissolved or dissolving 'grammar' that opens the possibility of a productive change in how we understand how the world fits together. That is an opportunity for society to become more open, as ideas and groups can become actively involved in negotiating the terms and conditions that are henceforth to apply – until the next renegotiation.

Although the boundaries between private and public sector are blurring, the state plays a distinct and significant role in shaping and influencing how privacy is valued. For this essay's purposes, we are interested in how the state, in its role as the mediator between individual and collective interests, influences the public's perceptions and attitudes to the distinctions between public and private. In particular, its role in protecting public security has come to the fore.

Privacy and punishment reinvented

We cannot be blind to the risks that are simultaneously immanent in this moment of flux. Major disasters set the stage for capitalist forces to assert their hegemony in previously unconceivable ways by sweeping aside previously existing constraints of 'traditional' society, often side-stepping democratic concerns in the process, the crisis moment has also produced markedly undemocratic, reactive practices and spaces.

A serious analysis of the relationship between space and power raises many questions about how far spatial conditions have influenced and continue to affect conscious violations of human rights. Post 9/11 in particular, one can trace an increasing habit of politicians to convert the tools of spatial planning in order to create microclimates which do not obey any legal framework, subverting existing notions of both individual privacy and public scrutiny. There is evidence that spatial planning has been used as a mechanism to convert spaces into strategic weapons of punishment that reflect prejudices and the interests of dominant ideologies and institutions. At this point, people's ability to influence the public–private realm disappears; the decisions about us and them are instead presented to us as fait accompli.

In 2005, the Italian philosopher Giorgio Agamben reinterpreted the US 'war against all evil' as a symbolic gesture that envisions an alteration of the political landscape.[7] Two months after the September attacks in 2001, the Bush administration – in the midst of what it perceived as a state of emergency – authorised the indefinite imprisonment of non-citizens suspected of terrorist activities. This policy, according to Agamben, should be understood as the 'state of exception', a powerful strategy that enables the transformation of a contemporary democracy into a civil dictatorship. Agamben argues that the state of exception, instead of a provisional measure, has become part of the everyday fabric of society. This has moulded the current precariousness and crisis moment into a reactive situation in which barriers and boundaries are reinforced in an attempt by the state to reassert a particular notion of stability and security.

In the post 9/11 world, we are told that in 'times of war' rules and rights are no longer applicable and have to be 'temporarily' suspended. In some instances military judges replace civil courts and, in the name of national security, the president – as the civil leader of the military – embodies unrestricted powers. The underlying principle of justification is whether or not a particular action is taking place in the name of national interest – with this very interest defined by the power that pursues it. In this context, the term 'terror' is being pollinated with 'war'. Consequently, 'war' allows for all civil rights to be suspended.

In this context, it is not surprising that those imprisoned in Camp X-Ray and Camp Delta (Guantanamo Bay, Cuba), the detention centre at Bagram airport (Afghanistan), Abu Ghraib prison (Iraq) and numerous third-country penitentiaries have been deferred into territories that lack human rights monitoring, influenced by the infamous White House directive that 'terrorist' suspects do not deserve the rights given to prisoners of war under the Geneva Conventions.

This method of creating extra-legal territory also includes the technique known as 'extraordinary rendition'. In April 2005, Human Rights Watch released a summary of evidence of US abuse of detainees in Iraq, Afghanistan, Cuba and other programmes of secret CIA detention.[8] The US government openly admits that they seek diplomatic assurances from states where torture is a common phenomenon, an absurd pragmatism of one state requesting that another make an exception to its general policy of using torture with respect to just one individual. This has deeply disturbing implications. Proactively proposing the creation of such territorial and legal islands of protection illustrates the imperative function of space, and comes close to accepting the ocean of abuse that surrounds it.

When Giorgio Agamben, both prior to and post 9/11, discussed the principles of Western society, he rendered a threatening image that is gaining momentum but is consistent from legal documents all the way back to the Roman Empire. Influenced by Hannah Arendt's work on totalitarianism and the institutional form of rights,[9] Agamben traced a historic process towards his primary thesis: there is an unforeseen solidarity between democracy and totalitarianism. According to the Roman legal system, the one who threatened the existing order of the Republic was treated as a public enemy, the ultimate outsider, as 'Homo Sacer' – the one without rights – who was stripped of his human attributes, reduced to nothing but a living being who could be executed with no further ado. Logically, the individual's right to privacy is obliterated: his 'bare existence' is that of an animal whose privacy is irrelevant.

The videos and photographic footage that came out of Iraq's Abu Ghraib prison illustrate graphically the urgent relevance of Agamben's theory: the stripping of rights, and bodily violations, the naked bodies piled on top of each other and its sadistic choreography blend into a scene that resonates with the fatal imagery of the twentieth century. Within this, there seems to be a strong link to what Michel Foucault described as the premodern 'ceremonial of punishment': 'some prisoners may be condemned to be hanged… others, for more serious crimes, to be broken alive and to die on the wheel, after having their limbs broken; others to be broken until they die a natural death.'[10] Starting from such medieval practices, Foucault illustrates how far in present-day societies physical punishment has become the most hidden part of the penal process. In the twentieth century, he argues, the spectacle of punishment has shifted to the trial. But if there is no trial, such as seems to be the case now that the 'the rules of the games have changed', there is no scene. We are witnessing the disappearance of public sentencing, and with that we lose accountability, and justice. We are left with the occasional leaks of a sinisterly private spectacle of abuse.

Another spatial expression of the state of exception, the naval base Guantanamo Bay in Cuba, is essentially a territory in which prisoners can be held indefinitely beyond scrutiny of US courts – some of them since 2001. It is the 'legal equivalent of outer space';[11] since it is not considered US territory, those imprisoned there have none of the rights of someone brought to US soil. Amnesty International has compared the territory with Soviet concentration camps known as Gulags, where resistance was legal proof of the need for 'treatment'.

The spatial construction of Camp Delta consists of a maze of fences, razor wire and guard towers. Walls are made from chain link and cells are protected from the elements by corrugated metal sheets. Prisoners spend most of their time in their cells, sitting on the floor or lying on foam sleeping mats. At night the entire territory is lit up so the guards can see the prisoners' every move. This extreme of security is the extreme absence of privacy. The construction of additional detention units was completed by mid April 2002, and done by Brown & Root Services (BRS) – a subsidiary company of oil venture Halliburton – approximately five miles from Camp X-ray. Each detention unit is 8 feet long, 6 feet

8 inches wide and 8 feet tall and constructed with metal mesh on a solid steel frame.[12] Each detainee is provided with a foam sleeping mattress, a blanket, and a half-inch-thick prayer mat.

It is precisely these conditions that have been meticulously designed in order to alter the behaviour of inmates and cause symptoms such as chronic depression, suicide, interpersonal rejection, psychiatric disorder and trauma. Spatial components are being used as a tool to both punish and coerce. As soon as the aim is achieved – ie the detainee confesses – the spatial conditions are altered. Detainees who are willing to comply and confess have the opportunity to become a 'level one' detainee and live in Camp Four, where prisoners are housed in communal settings. Spatial design in the service of mental breakdown and humiliation has become part of the everyday fabric.

Through Bentham's Panopticon, Foucault explains the subtle form of psychological control of inmates in the private–public microclimate of a prison. It seems this has turned into a scenario in which there is neither political control on the micro-scale he described, nor a fully operative legal framework able to deal with this parasitic relationship between politics and space.

From permanent exception to everyday opportunity

Although the 'camp' should by no means be understood as a possible answer to some of the political questions that are continuously being raised by the 'architects of power', at least the camp offers a spatially defined framework, which can be judged and debated as a tangible space. The state of exception has led to the spaces of exception, where the performance of privacy takes place under lawless conditions not seen on such a scale since the Second World War. Tomorrow's politics should reach out for an architecture of human rights. That architecture would be one that did not shy away from the complicity of space in affecting the individual's public–private interface, but was open about the relations created, and democratic in their continuous renegotiation.

The crimes regarding the organisation of the built environment through the deliberate misuse of spatial components, isolating human targets by withdrawing them from any evident physical environment while dehumanising the individual, are in desperate need of further analysis. This calls for the involvement not just of politicians or human rights groups, but also of architects and planners trying to dismantle and understand the physical relationship between space and power. Guantanamo and Abu Ghraib are showcases for the extreme extents to which physical planning is capable of ethical failure.

We experience this every day in cities where conditions aren't nearly as stark. But we should be equally attentive to the socio-spatial strategies of intrusion, segregation and exclusion from the right to self-determination about the boundaries between the self and the world around us. The private sector offers continual reaffirmation of the self; the state promises an elusive sense of security. In an age of precariousness, the actions of market and state offer the public a reassurance of identity and security, in return for the relinquishing of privacy. We have to insist on playing our part in this ongoing re-negotiation, lest we be reduced from performers in a play, to mere spectators of an increasingly sinister spectacle.

Markus Miessen is a German, London-based architect, researcher, educator and writer.

Notes

[1] See http://searchenginewatch.com/ showPage.html?page=2156461 (accessed 25 Mar 2008).

[2] J Rosen, *The Unwanted Gaze* (New York: Vintage, 2001).

[3] I Lorey, 'Governmentality and self-precarization: on the normalization of cultural producers', Jan 2006, available at http://transform.eipcp.net/transversal/1106/lorey/en (accessed 29 Feb 2008).

[4] C Anderson, *The Long Tail* (London: Random House, 2007).

[5] G Deleuze, 'Postscript on the societies of control' (transl. M Joughi), *October* 59 (1992 [1990]).

[6] I Johar, 'Public space is dead, long live public space', in M Mean, J-A Sanchez de Juan and J Beunderman (eds), *BCL/LDN 2020* (London: Demos, 2007).

[7] G Agamben, *The State of Exception* (Chicago: University of Chicago Press, 2005).

[8] See, for example, http://hrw.org/english/docs/2005/11/07/usint11995.htm (accessed 29 Feb 2008).

[9] H Arendt, *The Origins of Totalitarianism* (New York: Schocken Books, 1951).

[10] M Foucault, *Discipline and Punish: The birth of the prison*, trans Alan Sheridan (Harmondsworth: Penguin, 1979).

[11] See http://books.guardian.co.uk/reviews/politicsphilosophyandsociety/0,,2104014,00.html (accessed 29 Feb 2008).

[12] See www.globalsecurity.org/military/facility/guantanamo-bay_delta.htm (accessed 29 Feb 2008).

14 Regulating privacy

Gareth Crossman

At Liberty we try and avoid the use of phrases such as 'Orwellian' and 'Big Brother' when describing privacy, surveillance and data sharing in the UK. We're concerned it can lead to allegations of wild-eyed paranoia. It seems that we might have been overcautious. In 2007 even senior police officers such as the deputy chief constable of Hampshire, Ian Readhead, seem worried that we are edging towards the world of *1984*. On the BBC show *Daily Politics* he said that the spread of CCTV cameras is leading the country into 'an Orwellian situation'.[1]

He is not alone. In October 2006 the Information Commissioner Richard Thomas described the UK as a 'surveillance society'. He said it as a statement of fact.[2] Since then select committees in both Houses of Parliament have launched enquiries into surveillance while the main opposition parties rarely miss an opportunity to lambaste the government with allegations of contempt for individual privacy and an unhealthy obsession with snooping.

It was not always like this. In the aftermath of 9/11, expressing a concern about surveillance was seen as being soft on terrorism and crime. Vox pops on the BBC website agreed that ID cards were an essential weapon in the war on terror. Only those with something to hide had something to fear. Privacy was a right easily trumped by national security. While these arguments might still be rolled out on occasion today, the range and quantity of those keen to voice their disagreement is on the increase.

But is it too late? Some are now warning that privacy as we understand it is a concept that will seem alien a generation from now, that we are either regressing into the Stasi-esque world of *The Lives of Others* or heading towards the cyber-futurism of *Minority Report*. Whether melodramatic or not, in 2007 we are subject to levels of state and private sector intrusion and surveillance unimaginable ten years ago.

This is not necessarily always a bad thing. Surveillance techniques need to adapt to deal with modern criminality while data sharing can make life more convenient and improve access to public services. What has been missing in government policy in recent years is a sense of proportionality limiting privacy intrusion so that it is targeted and appropriate. This overarching principle can be applied across the range of privacy-relevant subjects. It is helpful to look at some of these in more detail before looking at possible ways of redressing the balance.

Privacy intrusion by the state is generally summarised as 'surveillance'. This word means many things to many people. There are several broad categorisations that can help definition. 'Mass informational surveillance' covers the retention and dissemination of database information. This would cover databases such as the National Identity Register (NIR), created by the Identity Card Act 2006 (IDCA) and the children's index set up by the Children Act 2004. 'Mass visual surveillance' relates to the use of CCTV cameras. 'Targeted surveillance' refers to the use of intrusive powers such as communication interception by means of the framework created under the Regulation of Investigatory Powers Act 2000 (RIPA). The central distinction between these types of surveillance is that targeted surveillance is commonly used as part of intelligence-led investigation into illegal or unlawful activity. Mass visual and informational surveillance does not take place in anticipation of a specific investigation into impropriety but will often be claimed to have some crime detection or (in the case of CCTV) crime prevention purpose. Information is retained and disseminated in anticipation of being of use for investigation. Mass informational surveillance will also take place for purposes unrelated to investigation such as assisting access to public services.

Mass and targeted surveillance techniques have usually been distinct. However, in the last few years this distinction has been blurred by the increasing use of 'data-matching' and 'data-mining' processes. These techniques are based on the use of automated processes that analyse or match seemingly innocuous data in order to throw up anomalies or inconsistencies. When used in relation to information about people this is more commonly known as 'profiling'. The blurring of distinction arises from the fact that there is no human- or intelligence-led initiation of suspicion. Human investigation will follow *after* initial matching or mining.

Although not strictly surveillance the retention of DNA on the National DNA Database (NDNAD) should also be mentioned. The

UK has five times as many people on its database as any other country. DNA retention is not informational surveillance in that the 'data' (at present) serve a specific single purpose, which cannot be applied elsewhere. DNA retention is, however, of concern to an increasing number of people.

In privacy terms possibly the most profound societal shift in the last ten years has been the proliferation and use of mass informational databases. We have become so used to instant informational access, particularly from online sources such as Google, that it is easy to forget how recently things have changed. It is also easy to see how concerns about mass informational systems used by the state can be seen as Luddite. Looking at the legislative frameworks behind mass database programmes can be telling, however. What the Identity Card Act 2006, the Children Act 2004 and the recently enacted UK Borders Act 2007 (which will require anyone from outside the European Union to have a 'biometric information document') share is enormous scope for both the information contained and the bodies with access to be increased. The ability to increase powers is generally left to the 'positive resolution' process whereby extensions are given limited debate and parliamentarians can only vote for or against the order as a whole.

When systems are in place it makes logistical, practical and financial sense to use and expand these powers as much as possible. Liberty has always maintained that the uses put forward justifying the ID card scheme, from crime to unlawful immigration and terrorism to identity fraud, fail to stand up to scrutiny. However, whatever use is made of them events will inevitably occur which will result in an extension of powers. If, for example, the NIR had been in operation at the time of Ian Huntley's conviction for the Soham murders, the mood of public outrage was such that there would have been political pressure to place details of convictions or 'soft' non-conviction police intelligence onto NIR entries.[3] The experience of the previous Second World War identity cards suggests that extra purposes would soon be found as that scheme saw an increase in uses from three to 39 in 11 years.

Pressure to increase the scope of use of the NIR could arise from a need to make it of genuine use in combating serious crime or terrorism. After the July 2005 attacks, the former Home Secretary, Charles Clarke, publicly accepted that ID cards and the NIR would not have prevented the attacks. This makes sense as it is safe to assume that British intelligence and policing agencies have gathered information on anyone that they believe could constitute a risk to national security.

The reality is that anyone who does give reason for concern would become subject to a level of targeted surveillance that would collate information going way beyond what would be contained on the NIR. It is not feasible that the NIR entry would add information to that possessed by the security services. This leads to a worrying possibility; in order to be of any use whatsoever in combating terrorism, the NIR *must* contain more information. This would need to be of a type that would separate those who present no, or minimal, risk to national security from those who might pose a serious risk. In other words, to be of any use in combating terrorism, data contained on the NIR must be increased in order to allow some degree of profiling and categorisation.

Profiling of information through data matching or data mining is increasingly being seen as a legitimate policing technique. The Serious Crime Act 2007 places data matching for fraud purposes on a statutory footing. So far profiling of persons has remained too contentious and divisive a proposal for the government. However, following the 7 July 2005 bombings and the plot to blow up a series of transatlantic flights in August 2006 there were calls from a number of commentators to introduce profiling for public transport users and airline passengers, respectively. Profiling may be the future of surveillance.

Of course many informational databases can serve useful purposes. In theory the children's index set up under the Children Act 2004 could be a useful resource for identifying children at risk from neglect and abuse. Unfortunately, making the index apply to every child in the UK and allowing broad scope to enter detail on the index increases the potential for both familial privacy intrusion and counterproductivity. In particular, so much information might be entered onto the index, especially by social workers who are worried by the consequences of failing to register information, that soon the woods cannot be seen for the trees and children genuinely at risk are overlooked.

As DCC Readhead's words attest, CCTV is a frequent target for allegations of state 'Big Brotherdom'.[4] However, there are few who argue it has no uses. Since the poignant images of Robert

Thompson and Jon Venables in a Merseyside shopping centre leading Jamie Bulger to his death seized the nation in 1993 it has been common currency that CCTV helps fight crime. Of course CCTV has crime detection uses. It also, as in the case of the 7 July bombers, has proved to be of use in piecing together a retrospective picture of events leading to a major crime. Its use as a crime prevention tool is debatable. Street lighting is a more effective way of reducing crime. At best CCTV can be one part of a local crime strategy.

To an extent debates over effectiveness, while interesting, are not the principal issue with CCTV. It is here to stay. Of greater significance is its unregulated nature. The relevance of the Data Protection Act 1998 (DPA) is limited for two reasons. First, a decision by the House of Lords in the case of *Durant* means that footage from many systems not specifically targeted on an identifiable subject (ie most public systems) are not covered by the DPA. Second, the DPA contains a series of principles about processing data but is of little assistance in providing any detail for more practical matters such as locating and signposting cameras and the handling, disseminating and disposal of footage. Bodies such as the Information Commissioners Office (ICO) and the Local Government Information Unit (LGIU) have published detailed codes of practice on CCTV use. However, these are for guidance and carry no sanction for breach. In terms of enforceability CCTV remains very much the Wild West.

NDNAD used to be relatively uncontentious. When set up in 1995 it was used for the storage and use of DNA samples of those convicted of certain offences, mainly involving sexual assault or violence. Since 1999 successive acts of Parliament have rolled back the grounds for the taking and permanent retention of DNA so that anyone can have their DNA retained on the NDNAD for the rest of their lives after being arrested for a recordable offence (generally those for which a person could be sent to prison). A recent Home Office consultation has suggested that this could be again extended to cover non-recordable offences allowing for permanent DNA retention for the most minor traffic offence.

Coupled with ever-expanding grounds of retention is the difficulty in removing samples on the database. There is a general discretion to remove but no statutory basis for making determinations. Thus, decisions tend to be operational ones made by individual forces and discretion seems very sparingly used. People arrested and then not proceeded against routinely find that the sample is retained. This practice makes DNA retention increasingly rub up against the concerns of 'Middle England' as middle-class parents whose children have minor brushes with the law find out that youthful indiscretion can lead to permanent retention. Suddenly the NDNAD becomes much more than a necessary tool for capturing violent criminals and sex offenders.

Of course violent and serious crime detection is most assisted by the more intrusive forms of targeted surveillance such as communication interception. The framework for intrusive surveillance is set out in the highly complex Regulation of Investigatory Powers Act 2000 (RIPA). Even those who are familiar with its workings can struggle with RIPA, which was referred to by David Blunkett when Home Secretary as 'this horribly complicated legislation'. RIPA creates five different tiers of surveillance ranging from interception of communications as most intrusive down to access to communications data, which is the record (but not content) of phone calls, mobile calls, emails and website visits. Use of RIPA is staggering with 439,000 warrants for communications access alone being granted between 1 January 2005 and 31 March 2006. The authorisation process ranges from self-approval for communications data by the myriad of public bodies able to apply for it to warrant signed by a government minister for interception of communications.

Executive authorisation is a long way from independent judicial oversight, which is totally absent. Anyone believing the UK's system is likely to compare favourably with that of the US might be surprised to know that no interception of communications can take place within the US without court authorisation. Suspicions that this might in fact be occurring resulted in the deputy press secretary at the White House, Dana Perino, going on record in November 2006 to say: 'There is no domestic surveillance [in the US] without court approval.'[5]

The oversight structure is also lacking. Three separate Commissioners between them review the use of RIPA power but their functions are mainly restricted to reporting after the event. The Investigatory Powers Tribunal does provide recourse to those who believe they have been improperly subjected to surveillance.

However, the success rates of the 150 or so applicants who have cases heard annually is not staggering. In December 2006 the tribunal's one and only finding of unlawful surveillance determined that Police Chief Superintendent Ali Dizaei had his telephone unlawfully tapped.

This somewhat whistle-stop run through a broad range of privacy and surveillance issues might be seen as painting a somewhat negative and pessimistic picture. To an extent this is true. Part of the problem is that the legislative framework in place to protect privacy is lacking. The human rights principles embodied in the Human Rights Act 1998 (HRA) make specific provision for privacy protection through Article 8. In common with most of the rights guaranteed in the HRA it also provides a comprehensive framework allowing for appropriate limiting of privacy rights when in accordance with the law, for a legitimate purpose, and proportionate. The problem with the HRA is that it is mainly tailored to protect individual 'victims'. It is not best suited for providing protection against the societal-wide impact of mass data sharing and surveillance.

The DPA is far more suited to the protection of data privacy. However it is nearly ten years old and originated from a directive dating back to 1995. Its ability to provide proper limitation to data-processing, data-matching and data-mining techniques in 2007 can be questioned.

For example the DPA contains eight principles, which all data processing must comply with. One of these allows processing only for one or more specified purposes. However, there is no limit on those purposes so long as they are registered with the ICO. This means multiple registrations could allow potentially unlimited uses. The ICO is limited in its ability to act against excessive processing. Its powers in relation to processing are essentially administrative rather than regulatory. What enforcement powers the ICO does have tend to be used after the event and rely on cooperation of the data controller.

There are many problems with the nature of privacy protection. There are, however, a number of steps that can be taken which might at least partially redress the balance. At the top of the list is new data protection legislation. This could help provide effective regulation of CCTV and update the data protection regime to provide proper enforcement powers to the ICO.

Effective powers for the ICO is only part of the story. It also needs to be properly resourced to proactively ensure that data protection is taken seriously. Good practice and inter-agency cooperation are more important in ensuring this than new enforcement powers. This is of particular relevance to the operation of mass informational database systems when privacy protection is frequently about the appreciation of public bodies as to what is proportionate.

Formalisation of a rigorous weeding regime to remove from the NDNAD DNA samples from those who are not convicted of offences of sex or violence would immediately make the retention of DNA more equitable and less contentious. The introduction of a degree of judicial oversight in RIPA authorisation along with a more rigorous scrutiny from commissioners would greatly enhance the accountability of intrusive surveillance.

This is just a quick summary of some of the steps that could be taken. None are radical or revolutionary. For a government of whichever persuasion willing to listen to the growing expressions of public concern about privacy intrusion they could represent an opportunity to make political capital while helping to make privacy once again a meaningful concept.

Gareth Crossman is Director of Policy at Liberty.

Notes

[1] See www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/21/npolice121.xml (accessed 19 Mar 2008).

[2] See http://news.bbc.co.uk/1/hi/uk/6108496.stm (accessed 5 Mar 2008).

[3] As it was, the Bichard Inquiry into the killings made the commendable suggestion that a positive vetting process be introduced.

[4] See www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=456487&in_page_id=1770&in_page_id=1770&expand=true (accessed 26 Mar 2008).

[5] See L Cauley, 'NSA has massive database of Americans' phone calls', *USA Today*, 5 Nov 2006, see www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (accessed 19 Mar 2008).

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

A **'Collective Work'** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

B **'Derivative Work'** means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

C **'Licensor'** means the individual or entity that offers the Work under the terms of this Licence.

D **'Original Author'** means the individual or entity who created the Work.

E **'Work'** means the copyrightable work of authorship offered under the terms of this Licence.

F **'You'** means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work,or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive,perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

A to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

B to distribute copies or phonorecords of, display publicly,perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised.The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

A You may distribute,publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display,publicly perform, or publicly digitally perform.You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder.You may not sublicence the Work.You must keep intact all notices that refer to this Licence and to the disclaimer of warranties.You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement.The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licencor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

B You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation.The exchange of the Work for other copyrighted works by means of digital filesharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

C If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works,You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

A By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

B except as expressly stated in this licence or otherwise agreed in writing or required by applicable law,the work is licenced on an 'as is'basis,without warranties of any kind, either express or implied including,without limitation,any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental,consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

A This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence,however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

B Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

A Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

B If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

C No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

D This Licence constitutes the entire agreement between the parties with respect to the Work licensed here.There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You.This Licence may not be modified without the mutual written agreement of Demos and You.

This project was supported by:

BT

The transformation of our social lives and the increases in surveillance and technological innovations have led us to believe that privacy is in the midst of a very public death. But privacy is not dying, nor can we let it do so. Privacy protects a set of deeply significant values that no society can do without; it is about the lines, boundaries and relationships we draw between and among ourselves, communities and institutions. Privacy appears threatened because our perception of what it means has radically changed.

This collection argues that we get the privacy culture we deserve. Our appetite for a connected society means we have yet to determine why we still care about privacy. These essays explore the underlying challenges and realities of privacy in an open society, and argue for a new settlement between the individual and society; the public and the state; the consumer and business. To achieve this, we need collective participation in negotiating the terms and conditions of twenty-first century privacy.

Charlie Edwards is Head of the Security Programme at Demos. Catherine Fieschi is Director of Demos.

ISBN 978-1-84180-192-6 £10