A Report on the Surveillance Society

For the Information Commissioner

By the Surveillance Studies Network

Appendices

September 2006

Appendix 1: Further Reading

The following list of further reading is not intended to be comprehensive, but to provide ways in to further research on surveillance. For more specific references or background information please consult the footnotes in the main report or the individual expert reports.

1. Edited Collections

Key edited books with chapters covering a wide range of surveillance subjects covered in this reports:

Ball, K. and Webster, F. (eds.) (2003) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Era*. London: Pluto Press.

Haggerty, K. and Ericson, R. (2006) *The New Politics of Surveillance and Visibility*, Toronto: University of Toronto Press.

Levin, T. Y., Frohe, U. and Weibel, P. (eds.) (2002) *CTRL [Space]: Rhetorics of Surveillance from Bentham to Big Brother.* Cambridge, MA and London: MIT Press.

Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, London and New York: Routledge.

Lyon, D. and E. Zureik (eds.) (1998) *Computers, Surveillance and Privacy.* Minneapolis: University of Minnesota Press.

2. Popular Books

Major general books on surveillance written in an accessible style or designed for a mass audience:

Cavoukian, A. and Tapscott, D. (1995) *Who Knows? Safeguarding Your Privacy in a Networked World*, Toronto: Random House.

Davies, S. (1996) *Big Brother: Britain's Web of Surveillance and the New Technological Order*, London: Pan Books.

Garfinkel, S. (2001) *Database Nation: The Death of Privacy in the 21st Century.* Cambridge, MA: O'Reilly.

O'Harrow, R. J. (2005) *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society.* New York: Free Press.

Parenti, C. (2003) *The Soft Cage: Surveillance in America from Slave Passes to the War on Terror.* New York: Basic Books.

Parker, J. (2000) *Total Surveillance Investigating the Big Brother world of e-spies, eavesdroppers and CCTV*, Piatkus.

Rosen, J. (2004) *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age.* New York: Random House.

Whitaker, R. (1999) *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York: The New Press.

3. Academic Books

General books on surveillance written for a mainly academic audience or using more theoretical approaches

Bogard, W. (1996) *The Simulation of Surveillance: Hypercontrol in Telematic Societies.* Cambridge: Cambridge University Press.

Coleman, R. (2004) *Reclaiming the Streets: Surveillance, Social Control and the City*. Cullompton, UK: Willan.

Dandeker, C. (1990) *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day.* Cambridge, MA: Polity Press.

Ericson, R. V. and Haggerty, K.D. (1997) *Policing the Risk Society.* Toronto: University of Toronto Press.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison.* New York: Pantheon

Garland, D. (2001) The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: University of Chicago Press.

Gilliom, J. (2001) *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy.* Chicago: University of Chicago Press.

Lyon, D. (ed.) (2006) *Theorizing Surveillance: The Panopticon and Beyond.* Cullompton, UK: Willan.

Lyon, D. (2003) *Surveillance after September 11.* Cambridge: Polity Press.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*. Cambridge, MA: Polity Press.

McCahill, M. (2002) The Surveillance Web: The rise of visual surveillance in an English city, Cullompton: Willan.

McGrath, J. (2004) *Loving Big Brother: Performance, Privacy and Surveillance Space.* London: Routledge.

Marx, G.T. (1988) *Undercover: Police Surveillance in America.* Berkeley, CA: University of California Press.

Monmonier, M. (2004) *Spying with Maps: Surveillance Technologies and the Future of Privacy*. Chicago: University of Chicago Press.

Norris, C. and Armstrong, G. (1999) The *Maximum Surveillance Society: The Rise of CCTV*, Oxford: Berg.

Rigakos, G. (2002) *The New Parapolice: Risk Markets and Commodified Social Control.* Toronto: University of Toronto Press.

Rule, J.B. (1974) *Private Lives and Public Surveillance: Social Control in the Computer Age*, New York, NY: Schocken Books.

Staples, W.G. (2000) *Everyday Surveillance: Vigilance and Visibility in Postmodern Life.* New York: Rowman and Littlefield.

Staples, W.G. (1997) *The Culture of Surveillance: Discipline and Social Control in the United States.* New York: St. Martin's Press.

4. Expert Reports

Borders

Andreas, P. and Snyder, T. (eds.), *The Wall Around the West: State Borders and Immigration Controls in North America and Europe*. Lanham MD: Rowman and Littlefield.

Bigo, D. and Guild, E. (eds.) (2005) *Controlling Frontiers: Free Movement into and within Europe*, Aldershot: Ashgate.

Salter, M. (2003) *Rights of Passage: The Passport in International Relations.* Boulder, CO: Lynne Rienner.

Torpey, F. (2001) *The Invention of the Passport: Surveillance, Citizenship and the State.* Cambridge: Cambridge University Press.

Zureik, E. and Salter, M.B. (eds.)(2005) *Global Surveillance and Policing: Borders, Security, Identity*. Cullompton, UK: Willan.

Citizenship and Identity

Caplan, J. and Torpey, J. (eds.) (2002) *Documenting Individual Identity: The Development of State Practices in the Modern Word*, Princeton, NJ: Princeton University Press.

Garton-Ash, T. (1997) *The File: A Personal History*. London: Harper Collins.

House of Commons Select Committee on Science and Technology (2006) *Identity Card Technologies: Scientific Advice, Risk and Evidence*, http://www.parliament.uk/parliamentary_committees/science_and_technology_committee/sag.cfm

Lyon, D. (2004) 'Identity cards: social sorting by database,' OII Internet Issue Brief No. 3 . http://www.oii.ox.ac.uk/research/publications.cfm

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

Consumption

Elmer, G. (2004). *Profiling Machines: Mapping the Personal Information Economy.* Cambridge, MA: The MIT Press.

Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO: Westview Press.

Lace, S. (ed.) (2005) *The Glass Consumer: Life in a Surveillance Society*, Bristol: The Policy Press.

Turow, J. (2006) *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge MA: MIT Press.

Crime and Justice

Gill, M. and Spriggs, A. (2005) *Assessing the impact of CCTV*. London, Home Office Research, Development and Statistics Directorate.

Goold, B. J. (2004) *CCTV and Policing: Public Area Surveillance and Police Practices in Britain.* Oxford: Oxford University Press.

Newburn, T. and Hayman, S. (2001) *Policing, CCTV, and Social Control: Police Surveillance and Suspects in Custody*. Collumpton: Willan Publishing.

Norris, C., McCahill, M. and Wood, D. (eds.) (2004) *The Politics of CCTV in Europe and Beyond.* Special Issue of *Surveillance and Society,* 2(2/3), http://www.surveillance-and-society.org/cctv.htm

Painter, K. and Tilley, N. (1999) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention.* Cullompton: Willan.

Infrastructure and Built Environment

Coaffee, J. (2003) *Terrorism, Risk and the City: The Making of a Contemporary Urban Landscape*. Aldershot UK: Ashgate.

Graham, S. (ed.) (2004) *The Cybercities Reader*, London: Routledge.

Graham, S. and Marvin, S. (2001) *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition.* London: Routledge.

Institute for the Future (2004) *Infrastructure for the New Geography*. Menlo Park: California. IFTF.

Kang, J. and Cuff, D. (2005) 'Pervasive Computing: Embedding the Public Sphere,' *Washington and Lee Law Review* 62(1): 93-146.

Medicine

Armstrong, D. (1995) 'The Rise of Surveillance Medicine,' *Sociology of Health and Illness,* 17(3): 393-404.

Cole, S. (2001) *Suspect Identities: A History of Fingerprinting and Criminal Identification,* Boston; Harvard University Press.

Nelkin, D. and Tancredi, L. (1994) *Dangerous Diagnostics.* Chicago: University of Chicago Press.

Laurie, G. (2002) *Genetic Privacy: A Challenge to Medico-Legal Norms,* Cambridge: Cambridge University Press.

Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database*, London: The Wellcome Trust.

Public Services

Bellamy, C. and Taylor, J. (1998) *Governing in the Information Age*, Buckingham: Open University Press.

Cabinet Office (2005) *Transformational Government – Enabled by Technology* (Cm 6683), London: Cabinet Office, Available at: http://www.cio.gov.uk/documents/pdf/transgov/transgov-strategy.pdf#search=%22Transformational%20Government%20%E2%80%93%20Enabled%20by%20Technology%20%22

Snellen, I. and van de Donk, W. (eds.) (1998) *Public Administration in an Information Age: A Handbook*, Amsterdam: IOS Press.

Parton, N. (2006) *Safeguarding Childhood: Early intervention and surveillance in later modern society*, Basingstoke: Palgrave-Macmillan.

Performance and Innovation Unit, Cabinet Office (2002) *Privacy and Data-Sharing: The Way Forward for Public Services*, London: Cabinet Office, Available at: http://www.strategy.gov.uk/downloads/su/privacy/downloads/piu-data.pdf#search=%22Privacy%20and%20Data-Sharing%3A%20The%20Way%20Forward%20for%20Public%20Services%2C%22

Regulation

6, P. (1998) *The Future of Privacy, Volume 1: Private Life and Public Policy*, London: Demos.

Bennett, C. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, NY: Cornell University Press.

Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: MIT Press.

Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill, NC: University of North Carolina Press.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill: University of North Carolina Press.

Telecommunications

Bamford, J. (2001) *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency.* New York: Random House.

Keefe, P.R. (2005) *Chatter: Dispatches from the Secret World of Global Eavesdropping*. New York: Random House

Crampton, J. (2004) *The Political Mapping of Cyberspace*. Chicago: University of Chicago Press.

Diffie, W. and Landau, S. (1998) *Privacy on the Line: The Politics of Wiretapping and Encryption*, Cambridge, MA: MIT Press.

Lessig, L. (1999) *Code and Other laws of Cyberspace*, New York, NY: Basic Books.

Workplace

Ball, K.S. (ed.) (2002) *Work*. Special issue of *Surveillance and Society* 1(2), http://www.surveillance-and-society.org/journalv1i2.htm

Frenkel, S. *et al.* (1999) *On the Front Line: The Organization of Work in the Information Economy*. Ithaca: Cornell University Press.

McKinlay, A. and Starkey, K. (eds.) (1998) *Foucault, Management and Organization Theory: From Panopticon to Technologies of Self*. London: Sage.

Stanton, J.M. and Stam, K.R. (2006) *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust*. Medford, NJ: Cyberage Books.

Zuboff, S (1988) *In the Age of the Smart Machine*. New York: Basic Books.

5. Key Reports

A selection of important advisory, consultancy and research reports:

ACLU (American Civil Liberties Union) (2004) *The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society*. Washington DC: ACLU. http://www.aclu.org/FilesPDFs/surveillance_report.pdf

European Parliament Scientific and Technological Options Assessment Committee (STOA) (1999) *Development of Surveillance Technology and the Risk of Abuse of Economic Information* (5 Vols), Luxembourg: STOA. Available from: http://www.europarl.europa.eu/stoa/publications/studies/default_en.htm

SWAMI (2006) *Safeguards in a World of Ambient Intelligence: Report on the Final Conference: Brussels March 21-22, 2006*, Information Society: Technologies. http://swami.jrc.es/pages/documents/Deliverable5-ReportonConference.pdf#search=%22swami%20report%22

Privacy International / Electronic Privacy Information Center (EPIC) (Annual) *Privacy and Human Rights: An International Survey of Privacy Laws and Developments.* Available from: http://www.privacyinternational.org/

UrbanEye Project (2001-2004) *Working Papers* http://www.urbaneye.net/results/results.htm

6. Selected Websites

A very brief selection of research, campaigning and information sites…

CASPIAN (Consumers against supermarket privacy and numbering) http://www.nocards.org/

Roger Clarke's Dataveillance and Information Privacy Home-Page http://www.anu.edu.au/people/Roger.Clarke/

Electronic Privacy and Information Centre http://www.epic.org/

Liberty http://www.liberty-human-rights.org.uk/

New York Surveillance Camera Players http://www.notbored.org/the-scp.html

Notags.co.uk http://www.notags.co.uk/

Privacy International http://www.privacyinternational.org/

Statewatch http://www.statewatch.org/

The Surveillance Project http://www.queensu.ca/sociology/Surveillance/

Surveillance and Society http://www.surveillance-and-society.org/

UrbanEye Project http://www.urbaneye.net/

Appendix 2: Surveillance Encounters 2006

Surveillance encounters in the 2006 scenario.

- Travel: Family subject to passenger screening on the way out of Gatwick because of the time at which they bought their tickets, their seating requests and their connections with Pakistan.
- Borders/body: Subject to biometric checks on entry into US.
- Borders: Quicker entry for Gareth who has a UK passport. Slower entry for non-EU passport holders.
- Mobility: Intervention after CCTV picked up Geeta being knocked over by the luggage.
- Mobility/infrastructure: Use of SatNav which alerted the family to the presence of red light and speed cameras.
- Crime/infrastructure: No hats to be worn in the shopping centre
- Consumer: The use of a credit card linked to a supermarket chain because of money off vouchers received based on a spending profile.
- Consumer: Yasmin’s loyalty card scheme was linked to different retail outlets and generated a more comprehensive profile about her
- Consumer/Crime: Bank fraud monitoring of credit card spending patterns
- Consumer: Junk mail based on consumer profile or postcode
- False positives: The dog received junk mail; the ANPR system wrongly identified the number plate
- Crime: Sara’s school consulting on random drug testing of pupils
- Mobility: RFID access card scheme at Sara’s school
- Body: cashless card system which enables parents to monitor Toby’s eating habits
- Body: Drug testing in sport.
- Crime/Infrastructure/Public services: Enhanced street lighting, CCTV and electronic access control in council properties like the one Geeta lives in.
- Body/health: motion detectors in the homes of the elderly.
- Crime: ANPR able to cross check other police databases.
- Mobility: Tracking mobile phones on the internet.
- Public services/Crime: Intensive supervision and surveillance programme for persistent offenders, curfew orders, public-private partnership.
- Public services/Crime: Multi agency monitoring of vulnerable and risky children in particular areas to prevent them becoming offenders.
- Workplace: RFID access control linked to other databases regarding reward.
- Workplace: Intensive call centre work monitoring and intense reporting of performance.
- Workplace: Internet monitoring and worker privacy. Monitoring superseding other more social managerial processes.
- Body/health: Disease screening for vulnerable or at risk populations.
- Consumer: Spam and internet fraud based on harvesting of consumer lists.
- Public services: Background checks on benefits claimants.
- Workplace/consumption/infrastructure: differential customer queuing in the call centre.
- Consumer/Crime: Credit card cloning.

- Workplace: Both Yasmin and Asabe were unaware of the extent of monitoring undertaken on them.
- Consumer: Managing a personal credit profile held by Experian.
- Crime/mobility: Oyster cards and police access to the data.
- Infrastructure/crime/mobility: the extent of CCTV surveillance in London.
- Health/Safety: Computer vision in swimming pools.
- Infrastructure/mobility/consumer: with mobile phone cameras – the means of surveillance is distributed.
- Crime/body: Biometric information taken on arrest.

Appendix 3: Questions to Help Determine the Ethics of Surveillance

From: Gary T. Marx (1998) 'Ethics for a the New Surveillance', *The Information Society*, 14(3): 174

A. The Means

1. Harm: Does the technique cause unwarranted physical or psychological harm?
2. Boundary: Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, or spatial border)?
3. Trust: Does the technique violate assumptions that are made about how personal information will be treated, such as no secret recordings?
4. Personal relationships: Is the tactic applied in a personal or impersonal setting?
5. Invalidity: Does the technique produce invalid results?

B. The Data Collection Context

6. Awareness: Are individuals aware that personal information is being collected, who seeks it, and why?
7. Consent: Do individuals consent to the data collection?
8. Golden rule: Would those responsible for the surveillance (both the decision to apply it and its actual application) agree to be its subjects under the conditions in which they apply it to others?
9. Minimization: Does a principle of minimization apply?
10. Public decision-making: Was the decision to use a tactic arrived at through some public discussion and decision-making process?
11. Human review: Is there human review of machine-generated results?
12. Right of inspection: Are people aware of the findings and how they were created?
13. Right to challenge and express a grievance: Are there procedures for challenging the results, or for entering alternative data or interpretations into the record?
14. Redress and sanctions: If the individual has been treated unfairly and procedures violated, are there appropriate means of redress? Are there means for discovering violations and penalties to encourage responsible surveillant behavior?
15. Adequate data stewardship and protection: Can the security of the data be adequately protected?
16. Equality-inequality regarding availability and application:
    a. Is the means widely available or restricted to only the most wealthy, powerful, or technologically sophisticated?
    b. Within a setting is the tactic broadly applied to all people or only to those less powerful or unable to resist?
    c. If there are means of resisting the provision of personal information are these means equally available, or restricted to the most privileged?
17. The symbolic meaning of a method: What does the use of a method communicate more generally?
18. The creation of unwanted precedents: Is it likely to create precedents that will lead to its application in undesirable ways?
19. Negative effects on surveillants and third parties: Are there negative effects on those beyond the subject and, if so, can they be adequately mediated?

C. Uses

20. Beneficiary: Does application of the tactic serve broad community goals, the goals of the object of surveillance, or the personal goals of the data collector?
21. Proportionality: Is there an appropriate balance between the importance of the goal and the cost of the means?
22. Alternative means: Are other, less costly means available?
23. Consequences of inaction: Where the means are very costly, what are the consequences of taking no surveillance action?
24. Protections: Are adequate steps taken to minimize costs and risk?
25. Appropriate vs. inappropriate goals: Are the goals of the data collection legitimate?
26. The goodness of fit between the means and the goal: Is there a clear link between the information collected and the goal sought?
27. Information used for original vs. other unrelated purposes: Is the personal information used for the reasons offered for its collection and for which consent may have been given, and do the data stay with the original collector, or do they migrate elsewhere?
28. Failure to share secondary gains from the information: Is the personal data collected used for profit without permission from, or benefit to, the person who provided it?
29. Unfair disadvantage: Is the information used in such a way as to cause unwarranted harm or disadvantage to its subject?

Appendix 4: Expert Reports

1. Borders, by Louise Amoore
2. Citizenship and Identity, by David Lyon
3. Communications, by Nicola Green
4. Consumption and Profiling, by Jason Pridmore
5. Crime and Justice, by Clive Norris
6. Infrastructure and Built Environment, by Stephen Graham (with David Murakami Wood)
7. Medicine, by Ann Rudinow Saetnan
8. Public Services, by Charles Raab
9. Workplace Surveillance, by Kirstie Ball

Expert Report: Borders

Louise Amoore
Department of Geography, Durham University, UK.
Louise.amoore@durham.ac.uk

Introduction

The control and management of borders has historically been central to the security and sovereignty of the nation-state. The verification, authorization or refusal of people, money and goods crossing these borders – via passports, visas, exchange controls, customs and immigration and so on – has defined much of what we consider to be the sovereignty of a political jurisdiction.[1] Surveillance of the border has long been essential to the drawing of physical territorial lines around a political jurisdiction. Yet, in the aftermath of 9/11 we are seeing an intensification of political interest in the surveillance of the border as a means of fighting the 'war on terror'. For those charged with considering the privacy, data, information and civil liberties implications of surveillance, the post 9/11 border poses a number of important questions.

The first is how the border itself is undergoing significant transformation through new surveillance practices. Put simply, the monitoring and regulation of border surveillance practices now has to confront multiple new manifestations of the border. Whereas traditionally the borders 'at the edge' of nation-states have been thought of as the territorial geographical lines delineating political jurisdictions, contemporary dataveillance, because it integrates electronic data and surveillance, potentially allows the border itself to become more mobile.[2] When surveillance of the border is conducted via data mining and the profiling of suspicious or risky people, finance or goods, it is conducted far in advance of an actual physical border crossing, and often also long after a border is crossed.[3] For example, the UK government's e-borders programme has the stated objective "to identify and separate from the mass of legitimate traffic crossing our borders, that which poses a risk". This discrimination between legitimate and illegitimate traffic is done through the "routine capture of information in advance of arrival".[4] This example captures a key dynamic of change in border surveillance: the surveillance practices historically carried out at the territorial line of the border are superseded by ***pre-emptive*** practices that screen ***in advance***.

The second major question relating to surveillance practices at the border is the question of political jurisdiction over borders. Many of the emerging practices of border surveillance involve agencies and actions that cut across political jurisdictions or those that are offshore and out of the direct reach of national systems of regulation. For example, at the time of

[1] Mark Salter, *Rights of Passage: The Passport in International Relations* (Boulder, CO: Lynne Rienner, 2003). David Newman, 'Boundaries, Borders and Barriers: Changing Geographic Perspectives on Territorial Lines', in M. Albert, D. Jacobson and Y. Lapid (eds), *Identities, Borders, Orders: Rethinking International Relations Theory* (Minneapolis: University of Minnesota press, 2001).
[2] Michael Levi and David Wall, 'Technologies, Security and Privacy in the Post 9/11 European Information Society', *Journal of Law and Society* 31:2 (2004): 194-220. Roger Clarke, 'Dataveillance: Delivering 1984', in L. Green and R. Guinery (eds) *Framing Technology: Society, Choice and Change* (London: Routledge, 1994).
[3] Louise Amoore and Marieke deGoede, 'Governance, Risk and Dataveillance in the War on Terror', *Crime, Law and Social Change* 43:1 (2005): 149-173.
[4] UK Home Office, 'Partial Regulatory Impact Assessment: Data Capture and Sharing Powers for the Border Agencies' (London: HMSO).

writing the controversy over the Society for Worldwide Interbank Financial Telecommunication's (SWIFT) extradition of confidential financial transaction data to US authorities illustrates how cross-border financial surveillance challenges regulatory structures. Headquartered in Brussels, with offices in many locations around the globe, and comprising banks and financial authorities worldwide, SWIFT's accountability to particular regulatory structures is likely to be subject to intense political negotiation and juridical contestation. It is far from clear, for example, which specific governments SWIFT includes in its routine extradition of financial data and under what conditions and controls. In the consideration of border surveillance practices in this report, the border crossings of finance and goods are considered to be as important as the mobilities of people. Not only the surveillance of people at borders, but also the surveillance of cross-border financial transactions and commodities has a concrete impact on the life chances, liberties and rights of individuals and communities.

Finally, the ongoing international debates as to the apparent trade-off between security and civil liberties are particularly pertinent to border surveillance. Inherent within everyday practices of border surveillance are questions of rights to mobility, access to the global economy, inclusion and exclusion. The climate of heightened national security concerns is intensifying the drive to 'social sorting' at the border.[5] Where people can verify their identity and authenticate their activities, arguably their experience of crossing borders is one of expedited travel. The trade-off here is the submission of personal data, biometrics and access to private information. At many air, sea and land ports of entry it is now common, for example, to see 'fast track' lanes for expedited crossing. Such privatized spaces of 'trusted traveller' experience, though, do raise questions of data protection and privacy. Moreover, the growth of expedited border security sorts people and transactions into categories of risk that allows greater surveillance to be applied to those who do not or cannot enter the private spaces.

In this report, these three key questions will inform the analysis across many of the different categories of border surveillance discussed. We will see that current and emerging trends in border surveillance are significantly transforming the character of the border itself, the regulatory powers and authority of political jurisdiction over the border, and the everyday experiences of the included and excluded individuals and communities.

Key developments

1. *Surveillance and risk profiling at the border*

From the protection of land borders to the policing of cross-border financial flows, from airport security to the screening of containers at sea ports, risk assessment has become the defining feature of border surveillance. Of course, post 9/11 border risk management is not entirely new and there is ample historical evidence of risk profiling prior to 9/11.[6] However, what is novel about contemporary border surveillance practices is its ***pre-emptive*** approach to risk.[7] Where past border surveillance practices had a broadly ***preventative*** approach to risk, issuing or denying access on the basis of individual credentials, current and emerging practices have turned to technologies and data-mining in order to pre-empt potential risks. The important point here is that pre-emptive risk profiling shifts surveillance practices toward

[5] David Lyon, *Surveillance After September 11* (Cambridge: Polity, 2003). David Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (New York: Routledge, 2003).

[6] Didier Bigo, 'Security and Immigration: Toward a Critique of the Governmentality of Unease', Alternatives (27): 63-92. P. Andreas and T. Snyder (eds), *The Wall Around the West: State Borders and Immigration Controls in North America and Europe* (Lanham: Rowman and Littlefield, 2000).

[7] François Ewald, 'The Return of Descartes' Malicious Demon: An Outline of a Philosophy of Precaution', in Tom Baker and Jonathan Simon (eds), *Embracing Risk: The Changing Culture of Insurance and Responsibility* (Chicago: University of Chicago press, 2002).

the screening of the actions and transactions of the general population.[8] Contemporary border surveillance involves the compilation, classification and categorization of data on, for example passenger manifests or financial transactions, on an unprecedented scale. Consider, for example, the implications of the USVISIT[9] border control system for a UK citizen crossing the US border. For all visa waiver countries the USVISIT system involves the integration and mining of some 30 databases, from previous entry and exit data to social security records and information on exchange students. Privacy advocates and civil liberties groups such as the American Civil Liberties Union (ACLU), Electronic Privacy Information Centre (EPIC) and Privacy International have raised a number of key concerns relating to USVISIT's dispersed surveillance of the general population. As one EPIC lawyer put it in an interview: "these technologies are assumed to provide a complete picture of who someone is, leaving people having to dispute their own identity".[10] The challenge for regulatory bodies and advocacy groups is that apparently mundane information about daily activities is now being seen as key to border security. Pre-emptive decisions are taken about the potential risk of an individual or group long before they reach a physical border. If refused entry, as EPIC, PI and others suggest, citizens are left to challenge data-led decisions that are opaque and diffuse.

2. *Outsourced border surveillance*

Perhaps the most significant challenge for the public regulation of information, data and privacy is the extent to which border surveillance practices have become privatized. The evidence is that the outsourcing of state border security to private commercial companies – IT multinationals, major weapons and military hardware manufacturers, consultants, risk analysts, banks, identity management and biometrics corporations – is a burgeoning practice. Let us look briefly at some examples. In 2004, IBM won a £15 million contract for 'Project Semaphore', the first phase of the UK government's e-Borders programme. Project Semaphore, in a similar programme to USVISIT will integrate databases on airline passengers entering and leaving the UK. Together with 'Project Iris', also trialled by IBM, the programme will link biometric data to integrated databases that can identify anomalous patterns of behaviour. IBM is one example of a vast array of companies who now have a designated 'homeland security practice' offering data management, biometric and identity services to governments. Other notable players are Accenture who lead the $10 billion Smart Borders Alliance in the US; Oracle, whose ubiquitous identity management systems are now being used by the UK and US as 'homeland security solutions'; consumer electronics and telecoms companies such as Ericcson, who are contractors for the US Strategic Border Initiative (SBI); and Unisys and Microsoft, whose databases for the Schengen Information System (SYSII) were due to be implemented in 2006. The outsourcing of border surveillance practices to the private commercial sector raises a number of challenges for everyday privacy.

First, how is the boundary between commercial databases and public and state security to be regulated? Many workers in the UK, for example, have their employment data embedded in the Oracle system. Is there potential for function creep from the commercial, employment and consumer domains to the border security applications? This is a particularly important issue when many of the costs of war on terror surveillance can be displaced onto commercial entities such as airlines, money transfer agencies and credit card companies. There is some evidence now that the dominance of a particular firm in commercial applications of a technology (for example fingerprint secure entry systems for workplace security) is a key factor in their success in the border security procurement process.

Second, how are private companies to be made accountable for errors and false hits in their database systems? Currently there is extremely limited access for citizens who find

[8] Marianne Valverde and Michael Mopas, 'Insecurity and the Dream of Targeted Governance', in Wendy Larner and William Walters (eds) *Global Governmentality: Governing International Spaces* (London: Routledge).
[9] United States Visitor and Immigrant Status Indicator Technology, in place at all land, air and sea ports of entry from 2004.
[10] Interviews conducted by author at the Electronic Privacy Information Center, Washington DC, November 2004.

themselves on a 'smart border' watch list. While multiple agencies and authorities can access the system or place information on the system, there is restricted capacity to remove or correct data. Post the Madrid and London bombings, for example, the EU Justice and Home Affairs Council have consulted on the integration of the Visa Information System (VIS) and EURODAC databases and the move to matching entry and exit data. This will require a complex network of agencies across the public and private sectors and, potentially, will routinely extradite data to member state's law enforcement agencies. Privacy International and EPIC have raised questions surrounding the lack of accountability and transparency in smart border systems such as e-Borders and USVISIT.

Finally, there are substantial questions surrounding the accountability of elected governments to their citizens and the 'offshore' nature of many of the private contractors of border surveillance. In effect, commercial banks of data such as credit card transactions or mobile phone records that are held by multinational corporations can be 'offshore' and beyond the direct reach of a political jurisdiction. Recent examples of multinationals extraditing information will raise specific challenges for public scrutiny and regulation, particularly when a company holds the commercial data *and* has a contract for border surveillance.

3. *Identity at the border: biometric technologies*

There as been much hype and hyperbole surrounding the new biometric technologies deployed in border controls. It is worth contextualising biometric technologies in a history of the verification and authentication of identity.[11] After all, the signatures on passports or visas are a form of biometric identifier. The important thing here, then, is to carefully establish the new developments in biometric border surveillance practices. In the context of the war on terror, biometric techniques already in commercial use or on the threshold of applicability were fast tracked and heralded as the key to winning this new kind of war.[12] The US Patriot Act, in a framework that has implications far beyond US soil, established a set of practices for biometric applications that afforded their almost unlimited use in the investigation and identification of terrorist activity. It is likely, for example, that the UK debates about privacy, civil liberties and biometric ID cards will be superseded by the requirement for biometric data in passports in order to comply with US regulations. Though we might not describe this as direct international collaboration on biometrics, it certainly indicates that technological convergence and global travel will push toward new 'norms' for identification and verification. The allure of the biometric in border surveillance is the appearance of an 'anchor' for identity in the human body, to which data and information can be secured. In effect, the claims that can be made for data mining and data integration are limited if the identity linked to that data cannot be verified or confirmed. The biometric identifier – iris scan, digital fingerprint, facial scan, voice biometric or hand scan – becomes the access gateway to the data held. It is this convergence of data-mining and information integration with biometric identifiers, allowing new forms of social sorting and classification at the border, that poses specific challenges for privacy and civil liberties groups.

Of course, the promise of the biometric technologies is not being delivered quite as anticipated. The biometric technologies for the USVISIT programme, for example, were downgraded from planned iris scans to digital fingerprints for logistical reasons. Similarly, the biometrics elements of the UK's e-Borders programme have been subject to problems of implementation. As a result, the biometrics elements of routine border surveillance practices are relatively underdeveloped. However, in terms of the impact on public experiences of surveillance, it is likely to be more everyday forms of biometric identifier that are of greatest significance. For example, the proposed use of gait recognition technologies in 'new border'

[11] Gareth Jones and Michael Levi, 'The Value of Identity and the Need for Authenticity', *Report for the DTI Office of Science and Technology Foresight Panel* (London: DTI, 2000).
[12] Louise Amoore, 'Biometric Borders: Governing Mobilities in the War on Terror', *Political Geography* 25: 2 (2006): 336-351. Kelly Gates, 'Biometrics and Post-9/11 Technostalgia', *Social Text* 23: 2 (2005): 35-53. Irma Van der Ploeg, 'Biometrics and the Body as Information', in David Lyon (ed.) *Surveillance as Social Sorting* (London: Routledge, 2003).

spaces such as London's Waterloo station suggest not only an expansion of surveilled border spaces but also an extension of surveillance via the body. Such developments pose new problems for regulation and public accountability.

4. *Self-surveilled borders: trusted traveller schemes*

While biometric border surveillance applications have been beset by difficulties in large-scale general programmes, they are rapidly proliferating in privatized border crossing schemes. The ATA's trusted traveller programme, Air France's PEGASE scheme, and Schiphol's Privium Plus, for example, signal a move to expedited border crossing schemes. In effect, these schemes offer a system of pre-screening that allows people enhanced mobility across border spaces. In the examples of the airport schemes, the individual makes an application, submits a payment and biometric identifier (most commonly an Iris scan) and is subject to a security check via database. In such schemes the actual point of border crossing becomes something of a smooth space with little role for the border guard or other checks. These developments are perhaps seen in their most advanced form at some land border crossing points along the US borders with Mexico and Canada where biometric- and RFID-enabled smart cards permit expedited crossing.[13] Though the UK does not currently have a consolidated expedited borders system in operation, the international schemes are drawing in UK customers and the commercial suppliers of the systems are set to expand. The link to commercial applications poses a particular set of questions for regulators. In many instances the schemes are linked to frequent flier programmes of other loyalty cards and, in the US, the trend is toward corporate sponsorship by companies such as Mastercard. The expansion of privatized 'ID guarantee' clubs is likely to shift the terrain for privacy impact assessment and renders some of the debates about national ID cards and biometric passports somewhat obsolete.

Directions: border surveillance trajectories

To identify trajectories for near-future surveillance scenarios is, of course, to engage in a degree of speculation about the future. In this section of the report, the identified trajectories are based on what we might call threshold border surveillance practices. These are either practices that are in use in another domain but are undergoing trials in border domains, or they are practices in use outside the UK that are likely to be imported or to impact on UK citizens.

1. *Algorithmic border surveillance*

An emerging trend in border surveillance practices concerns the data-led restructuring of the role of the border guard. The proliferation of 'smart borders' and 'electronic borders' have at the heart of their vision, the repositioning of border guards as "the last line of defence and not the first".[14] The everyday experience of surveillance at the border, then, is preceded by a dataveillant system that makes judgements about degrees of risk before the physical border checkpoint. This is not only the case in the mobility of people, but also in the mobilities of money and goods.[15] The UN's Financial Action Task Force (FATF) for intercepting terrorist finances, for example, envisages stopping the money before it reaches the border. As analyses have shown, however, the war on terrorist finance has resulted in greater surveillance of cross-border money transfer agencies such as Western Union and, by implication, the money transferred by migrants as remittances to their country of origin. An important issue here,

[13] Matthew Sparke, 'A neoliberal nexus: economy, security and the biopolitics of citizenship at the border', *Political Geography* 25: 2 (2006): 151-180.

[14] Accenture digital forum, 'US Homeland Security to Develop and Implement program at air, land and sea ports of entry' (www.digitalforum.accenture.com, 2004).

[15] Marieke deGoede, 'Hawala Discourses and the War on Terrorist Finance', *Environment and Planning D: Society and Space* 21: 5 (2003): 513-532. Brenda Chalfin, 'Border Scans: Sovereignty, Surveillance and the Customs Service in Ghana', *Identities: Global Studies in Culture and Power* 11 (2004): 397-416.

then, is how data is used to pre-judge the risk of a particular border crossing and whose lives are most significantly affected by such judgements.

The turn to information technology and science in border surveillance practices is following a logic of algorithmic calculations. As Gordon Woo of the London-based firm Risk Management Solutions puts it, "mathematics provides a whole new set of tools in the war on terror".[16] Specifically, algorithmic models can be embedded within surveillance systems so that a computer can 'see' a threat before the border security intervenes. Capable of profiling a 'normal' days financial transactions across a particular border, or an 'expected' flow of cargo through a major port, or a 'usual' rush our pattern at a land border checkpoint, algorithmic surveillance works by modelling a norm in order to identify a deviation from the norm. As such, algorithmic models pose particular problems for public regulators because everyday and apparently mundane information becomes strategically important. Rather like the way that insurance systems rely upon knowledges of daily journeys or domestic routines in order to designate risk, so algorithmic surveillance draws on an ever-wider array of prosaic information.

2. Tracking, screening and RFID

The radio frequency identification technologies that have become commonplace in smart cards, consumer products and personal electronics are on the near horizon for routine border surveillance practices. The RFID chips that enable goods to be tracked through a supply chain or office workers to scan a card to enter their office building are being fiercely contested in the domain of border surveillance. In the US, despite serious challenges to proposals for RFID in passports and visas, RFID-enabled border smart cards are being trialled at the US-Mexico border. On the supply side, the RFID industry is flagging the potential for the technology to allow the tracking or tracing of migrant workers who cross the border for a time-limited period. The important distinction here in terms of regulation is active versus passive RFID. Increasingly in the borders sphere the possibilities of the use of active RFID are on the agenda. Recent high profile bids for government border security contracts, for example, have included demonstrations of the potential of wireless tracking devices.

3. Ubiquitous border surveillance

The final significant trajectory to be identified here is the apparent move to incorporate citizen groups and watch groups into border surveillance practices. This is in its most advanced for in the US, where programmes such as Highway Watch, Citizen corps, Coast Watch and River Watch train citizens to "look out for unusual activities". However, there is one element of this form of everyday surveillance that has particular resonance in the border surveillance domain. For many of the private companies bidding for, or awarded, border surveillance contracts, consumer electronics such as mobile phones, PDAs and palm tops have played a central role. IBM, for example, contracted for the UK e-borders system and EU RFID programmes, also sponsored the US homeland security citizenship programme that allowed for personal computers, mobile telephones and consumer electronics to digitally connect neighbourhood security to homeland security. For privacy regulators there is an increased pressure on limiting the uses to which personal data can be put, the length of time it can be stored and so on. The use of everyday consumer telecommunications electronics to convey data, information or images from private domains to the sphere of public authorities blurs the boundaries between public and private spheres. As the ACLU have commented in their study of a new surveillance network, businesses and citizens are being "conscripted into the construction of a surveillance society".[17]

[16] S. Theil, 'Gordon Woo: Calculus for Catastrophe', *Newsweek* 12 July (2004).

[17] ACLU, 'The Surveillance-Industrial Complex' (Washington DC: ACLU, 2004).

Conclusions: summary of challenges for regulators

The processes and issues identified in this report pose a number of key challenges for privacy advocates, civil liberties groups and public regulators. Returning to the three key dynamics of change identified in the introduction, this report concludes with a summary of the central challenges.

- **Borders and pre-emptive surveillance**. The trend toward the surveillance and profiling of people, goods and services before a border is reached poses a number of key problems for regulators. Where data gathering and information integration takes place across a diffuse and dispersed array of domains and authorities, often involving multiple privacy regimes in different state contexts, how can surveillance be effectively governed and regulated? Where judgements are made that exclude or otherwise prejudice an individual or community on the basis of pre-emptive intelligence, how is transparency and access to information trails to be secured? Where pre-emptive border surveillance practices involve risk profiles, what are the checks and balances on racial or other forms of social discrimination?

- **Jurisdiction and juridical authority.** In a world where our daily practices cross juridical boundaries and enter ‘offshore’ spaces that are defined by their exemption from juridical authority, such as for example in our financial transactions, what are the particular dynamics of ‘function creep’? There can be little doubt that border surveillance is increasingly moving in the direction of general screening and risk profiling from data in other domains. Where that data is held offshore, what are the challenges for regulators? How can the unregulated extradition of data be prevented?

- **National security and civil liberties.** A unique challenge for the regulation of border surveillance is the renewed emphasis on national security post 9/11 and 7/7. How should privacy regulators respond to the juridical exemptions that are claimed for matters of national security? In effect, all border-related dataveillance could be considered a matter of national security. What are the practical steps that can be taken to prevent the creep from information on potential terrorism into immigration or asylum, for example? Is it possible to firewall data collected on security grounds (such as, for example automatic vehicle license recognition systems at land and sea ports of entry), from use in other domains such as social security, insurance or immigration?

Expert Report: Citizenship and Identity

David Lyon
The Surveillance Project, Queens University, Kingston, Ontario, Canada.
lyond@queensu.ca

Introduction

How can you tell who is a bona fide citizen of a given country? Much hangs on knowing this, from the right to vote or claiming health or welfare benefits to obtaining a passport for foreign travel. Citizenship and surveillance belong together in the modern world. Extensive records on each individual are needed to inform government departments about who has a right to what. But as those records grow, so they can be a source of power and of unease among citizens. Why do they need to know so much? Especially as biometric passports and new national ID card systems appear, some believe that the state is going too far.

This section looks at both the general issues of citizenship and surveillance and at specific contemporary examples, especially the rise of smart ID systems. While acknowledging the need for advanced records keeping systems in today's complex, mobile and fast-moving societies this section argues that the checks and balances have not kept pace with most recent developments. Under pressure from priorities such as national security this means that state surveillance today often has weak rationales, is insufficiently accountable and proceeds with inadequate oversight.

Historical background

Although taken-for-granted by many, citizenship is a contested issue, especially for refugees and asylum seekers or for nationals whose children are born out of the country. So how do we distinguish the real thing from the fake, the imposter? Modern states are in part constituted by their capacity to name, count and classify citizens, which they do by requiring documentary evidence such as the birth certificate or by mounting the census that enumerates populations according to citizenship, among other things. As well, in the twentieth century, increasing use was made of ID card systems and passports as means of checking on who really is a citizen. [1]

Two hundred years ago, when modern nation-states were being born, much attention was paid to the question of citizenship. Bit by bit, many rights, privileges and responsibilities came with citizenship, each of which was connected with an individual.[2] Being a member of a certain family, clan or class meant less for citizenship than proving that one was a resident, born of specifiable parents in a particular place. What once had mainly religious significance, the details of birth, marriage and death, now took on a new administrative significance in the burgeoning bureaucracies of government. The state sought to distinguish between one individual and another by clear and unambiguous criteria, so that the rights of citizens were extended only to those who were genuinely eligible.

[1] See John Torpey, *The Invention of the Passport*, Cambridge: Cambridge University Press, 2000; Mark Salter, *Rites of Passage: The Passport in International Relations*, Boulder: Rienner, 2003.

[2] Nicholas Abercrombie et al, *Sovereign Individuals of Capitalism*, London: Allen and Unwin 1983; Anthony Giddens, *The Nation-State and Violence*, Cambridge: Polity Press, 1987.

The means of keeping track of these personal details, which we call 'surveillance' (see the definition on page X) is thus very ambiguous. On the one hand, tremendous benefits accrue to citizens through being able to vote, be educated, or hold health coverage. But on the other, the state can also use those records to limit the activities or movements of citizens, or worse, to deem certain citizens second class and consign them to inferior or even brutal treatment. In the 1930s, Nazi Germany used early IBM machines on census materials, registrations and ancestral tracing records to sort undesirable Jewish citizens from desirable ('Aryan') ones and in Rwanda, the Belgian colonial ID card system was the means of singling out Tutsi targets for Hutu slaughter. In both cases, horrendous genocide was the outcome.[3]

Today, every nation state has complex and sophisticated ways of keeping tabs on individual citizens, recorded in large-scale departments such as employment, education, health, and taxation (see also Public Services section). Since the later part of the twentieth century, most of these records have been computerized. This adds efficiency (in most cases!) because of the hugely increased storage and transmission capacity available and, importantly, the ability to search those databases remotely. But the ambiguities of such state surveillance have never gone away. If anything, they have become more marked. Identification systems, for example, may simplify our interactions with government departments, granting ready access to information or benefits. But equally, they can be used to make dubious and sometimes dangerous distinctions between classes of citizens, advantaging some at the expense of others.

Key Developments

The early twenty-first century has seen the development of several new national identification systems. Indeed, some systems, such as those in Malaysia ('Mykad') and Japan ('Juki-Net'), have their roots in administrative and commercial ventures of the later twentieth century, but others, such as those in Italy and the UK (approved in Parliament in March 2006), are in part responses to 9/11 and the 'war on terror.' The USA has yet to develop a national ID system but the current attempt to rationalize and integrate federally the driver's licensing system (previously on a state-by-state basis) into the Real ID may turn out to be the *de facto* national ID system.

It is very important to note that the issue of citizen identification is not merely one of an ID card. ID cards of various kinds have been used for centuries, and in modern times especially in association with colonialism, crime-control and war.[4] The focus of these older types is the production of the card, on demand, to prove identity. New national ID card systems, however, are based on a national registry, a database (or databases in the UK case) containing personal information that can be searched and checked independently of any demand to see the card held by the citizen. The unique identifier contained in the card is also the key to unlock the database(s) and thus is itself a source of considerable power.[5] To understand the significance of this we have to step back and see the context in which new multi-purpose national ID systems are being developed.

The information revolution based on microelectronics that began in the 1970s was about the storage, retrieval, processing and transmission of data. It was as much about communication as about storage and processing. Personal data could be passed with ease from one department to another such that what once required official permission or even legal warrant became

[3] Edwin Black, *IBM and the Holocaust*, New York: Random House, 2001; Timothy Longman, 'Identity Cards, Ethnic Self-Perception and Genocide in Rwanda' in Jane Caplan and John Torpey (eds.) *Documenting Individual Identity*, Princeton: Princeton University Press, 2001.
[4] See Simon Cole, *Suspect Identities*, Cambridge MA: Harvard, 2002.
[5] See e.g. Roger Clarke, 'National Identity Schemes: The Elements' at www.anu.edu.au/people/Roger.Clarke/DV/NatIDSchemeElms.html

routine. From the point of view of bureaucratic efficiency communicating computers appeared to enhance organization by offering data matching between, say, customs and employment or education and police departments, citizens had less and less say in what happened to their personal records.

The searchable database was a tool that enabled discriminatory judgments to be built into systems, and such judgments may as easily work against individuals as for them.[6] Although data protection and privacy laws[7] were developed to limit such activities, these have found it very hard to keep pace with technical change or the ingenuity of those trying to sidestep regulation. In the case of ID card systems, the unique personal identifier makes it possible to obtain access to several kinds of database; the more multi-purpose the system the more databases are likely to be involved. If the UK ID card system is, as advertised, to guard against 'identity theft,' then this suggests that commercial data relating to banks and credit cards will be accessible as well as those relating to government departments such as immigration or health.

The combination of computing with communications capacities in surveillance – and this is clearly true for ID systems -- has a further implication which, though indirect, is singularly significant. It introduces a new reliance on those providing expertise, both technologically and commercially. The role of technologists and businesspersons within organizational bureaucracies has become increasingly significant, such that it is inappropriate to understand surveillance of personal data without considering the technological – usually software – and business practice – information management – priorities that now also inform the handling of personal data. This trend is also made possible, of course, by the economic restructuring that accompanied the technological revolution we have been discussing. It helped to produce what we now call globalization and also stimulated innovations such as outsourcing, now applied to aspects of ID systems.

The interplay of technological and business practices with organizational control occurs in the development of identification card systems. In any computerized system, the key to records retrieval is to have consistent and if possible unique identifiers and in this case for individual citizens. What spells efficiency from one point of view, however, spells potential social control from another.[8] But where does this control originate? In part, national ID systems may be seen as a means of increased state control, but they are also the products of technical and business expertise. So-called smart cards have been in use for some time in commercial settings but only more recently have they broken into the market of government administration.[9] Moreover, these systems, along with related biometric passports, rely on techniques developed in the on-line internet world, of identity management. That is, modes of regulating who may or may not have virtual access to web sites and other electronic domains are now applied to the offline world of borders and citizenship classification.

Note must also be taken of the growth of biometrics as a means of verification (checking that the individual is who they claim to be) and identification (checking that the individual's record matches that in the relevant database) (see also the Borders section). All new ID systems use some kind of biometric, based on a feature of the human body. Fingerprints, iris-scans, facial topography and hand-scans all count as biometrics and these enhance both passports and ID card systems today. The idea is that accuracy will be increased and the possibilities of fraud will be reduced by using biometrics. While PINs and passwords may be forgotten or lost, the body is always available and provides a direct link between the record

[6] Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.
[7] Such as the UK 'Data Protection Act' 1998.
[8] For a critical view from a computer scientist, see Roger Clarke's work on national ID systems: www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html
[9] Felix Stalder and David Lyon, 'ID cards and social classification' in David Lyon (ed.) *Surveillance as Social Sorting*, London and New York: Routledge, 2003.

and the person. As we note below, however, some surveillance problems persist with the use of biometrics.

The old bureaucratic logic of government administration now works its way through both biometrics and networked identification systems, into a world fraught with subtle nuance – identities and identifications. In this world those with access to resources are highly mobile – international businesspersons, tourists and the like -- and their identification systems (from credit cards to frequent flyer cards) tend to accelerate ease of movement. But for others, who are working (or worse, unemployed) migrants, refugees or asylum seekers, not to mention those with distinctive 'Muslim' or 'Arab' names, these systems tend to militate against movement both within and between countries. While older, twentieth century understandings of citizenship stressed the *inclusion* of all eligible persons in systems of health, welfare and legal protection, newer citizenship practices, including ID systems, seem to stress *exclusion* of undesirable elements.[10]

As the economic and political disparities between the global south and north have grown so resistance to the rich north has taken new and, for some, unexpected forms. In particular, the deep-seated humiliations of the Arab world at the hands of western colonial and economic powers has helped to spawn what is now regarded as a key international problem – a sort of permanent crisis – of global terrorism. Key events, starting symbolically (though not historically) with 9/11 have catalysed rapid growth of new surveillance and identification systems once again geared to establishing unambiguously who is a *bona fide* citizen of which country.[11] The difficulty is that many people are on the move, for many reasons and that ID systems are sought that classify them according not only to citizenship but also to status – temporary, permanent, national and so on. As we have seen, searchable databases already facilitate social classification and categorization. In this context, they appear as a godsend.

But not only are new ID systems raising questions about the reality of the very citizenship rights that identification was once supposed to guarantee – freedom of movement, freedom from want, equality before the law and so on – they are themselves subject to globalizing forces. Governments now seek ways of 'harmonizing' their identification procedures both for border crossing and for internal policing and controls and once again, this is facilitated by the new technologies. The International Civil Aviation Organization is a prominent player in this process, as they are setting standards for biometric passports and, by implication, for new national smart ID programs such as that in the UK. International conventions are held to develop 'globally interoperable systems' for identification in the field of 'MRTDs' (Machine-Readable Travel Documents).[12]

Critical Commentary and Future Directions

Identification and citizenship belong together in the modern world. Citizenship has increasingly come to be viewed as an individual matter for which a system of personal records is required. While this now appears in the broad swath of 'dataveillance' that exists across a range of government departments, the common denominator within them is the need for identifiers that will distinguish one individual from another. Increasingly, however, such identifiers are used across different domains.

[10] Didier Bigo, 'Globalized in-security: The field of the professionals of unease management and the ban-opticon,' *Traces*, 4, 2004.

[11] See, *inter alia*, David Lyon, *Surveillance After September 11*, Cambridge: Polity Press, 2003; Kirstie Ball and Frank Webster (eds.) *The Intensification of Surveillance*, London: Pluto Press.

[12] See www.icao.int/mrtd/Home/Index.cfm/

As James Rule pointed out more than thirty years ago, for example, the US driver's license is often used in practice as a universal ID in that country.[13] Today, pressure is on to find IDs that work for several purposes – border crossing, fraud control, access to government information and perhaps commercial (video rental) and semi-commercial ones (libraries) as well – which is shaping the field in fresh ways. As we have seen, the same criteria for identification are now sought across national boundaries as well.

The key developments in this story could be read as technological progress but whatever one's judgment on this, it's the (let's assume) unintended consequences that count. For however much one acknowledges, rightly, the ambiguity of surveillance as seen in areas such as ID card systems, the key problem is that once established, systems can easily acquire an apparent life of their own which is much easier to initiate than to halt or redirect. When agendas such as the 'war on terror,' curbing the migration of undesirable groups and even the quest for solutions for credit card fraud are shaping the development of ID systems, the 'impersonal' demands of a classic bureaucracy do seem somewhat undermined.

ID card systems offer unique identifiers and thus are critically significant for all government activity. This can range from anti-terrorism to access to government information. But the chief difficulty always lies in the powers granted to the state (now in alliance with corporate and technical bodies) that has control over the means of identification. In the UK case, the lack of clarity about the primary purpose of the ID system is a key issue for those attempting to evaluate the progress of development.[14]

As well there are other serious difficulties. One is the reliability of ID systems and the biometric tests on which they in turn rely.[15] The twin problems of 'failure to enroll (FTE)' (the biometric is unrecognizable) and 'false non-match' (subsequent reading does not match the properly enrolled individual biometric) remain, yet it appears that decisions have been made about biometrics before full trials have occurred. As many as one in six persons may not be able to use their cards readily to obtain health care or pensions, because of the FTE problems, even though they may in principle have 'entitlement.'[16] At their moment of vulnerability, they will actually be further handicapped.

Beyond this, ID systems may subtly classify populations according to opaque criteria. Major FTEs occur, for example, with non-white – black, asian, hispanic – persons, which may produce a bias towards whiteness in the very technique.[17] It is this ability to engage in social sorting that may in the long term be even more insidious than the fears about reduced mobility in countries where police may demand ID documents at any time.[18] It seems that the system will have the capacity to sort between those eligible for services or access, and others, but less-then-visible mechanisms will also operate, that skew the system against those already likely to be disadvantaged. Such social sorting tends to produce second class citizenship rather than supporting a more solidaristic and egalitarian practice.

Beyond this, increasing global integration and harmonization remove decisions more and more from local level and human scale as well as introducing other actors (technology experts, entrepreneurs) into the drama. When cultural and national identity has become such a contested dimension of life in the contemporary world, carrying a heavy freight of life-chances and choices, memories and hopes, it is ironic that parallel efforts are made to reduce

[13] James Rule, *Private Lives, Public Surveillance*, London: Allen Lane, 1973.
[14] See *Identity Card Technologies: Scientific Advice, Risk and Evidence*, Select Committee on Science and Technology, 2006; available at www.parliament.uk/parliamentary_committees/science_and_technology_committee/sag.cfm
[15] See, *inter alia*, Elia Zureik with Karen Hindle, 'Governance, Security and Technology: The Case of Biometrics' *Studies in Political Economy*, 73, 2004, 113-137.
[16] See A.C. Grayling *In Freedom's Name: The Case Against Identity Cards*, London: Liberty, 2005.
[17] Joseph Pugliese, '*In silico* race and the heteronomy of biometric proxies: Biometrics in the context of civilian life, border security and counter-terrorism laws' *The Australian Feminist Law Journal*, 23, 2005.
[18] David Lyon, *ID Cards: Social Sorting by Database*, OII Issue Brief 2004. Available at www.oii.ox.ac.uk/

it to machine-readable formulae and algorithms for ease of bureaucratic, policing and corporate administration. However human beings are identified by others, and especially by impersonal machine systems, it is not surprising that countervailing tendencies appear, challenging and offering alternatives to those identifications.

Challenges to regulators

How can new ID systems, whose use is so consequential for those citizens identified and classified by them, be made accountable to others beyond political constituents and corporate shareholders? Is there a larger frame than combating fraud or regulating immigration or even national security within which the administration of citizenship via ID systems may be understood? Put another way, can ID systems yet be made compatible with the desires of ordinary citizens not merely for national security but for human security, which is both more global and more personal?

At present, the British case of a multi-purpose national ID system does not offer much promise in this regard. It is far from clear that even national security will necessarily be enhanced by the emerging ID system. Many have suggested that national security would be better served by improving border security and conventional intelligence gathering, an idea that is underscored by the August 2006 alleged Atlantic flight terrorist plot involving more than 20 Britons.[19] Although the US Administration claimed that the operation showed the need for more advance passenger data,[20] it is clear that the alleged plot was foiled by the use of informers, undercover agents and tip-offs.

Plenty of ordinary citizens object to the various ID systems that have appeared over the past few years. Municipalities and states in Japan and the USA have objected to the new uses of personal data by refusing to cooperate, and in Britain numerous vocal protests accompanied the passage of the Identity Cards Bill through Parliament. The kinds of objections made should be considered by regulators, from the case against ID systems altogether – that they are superfluous and their objectives can be met by other means – to arguments about testing and improving the technologies *before* they are adopted and bringing the measures in line with at least EU Data Protection requirements.[21]

Assuming, pragmatically, that it is now too late to turn back the ID system tide in the UK, the challenge for regulators is to take every opportunity to install rigorous safeguards and transparency and accountability of use. The eventual system need not be as negative as its critics fear. Other countries, that have yet to adopt or even to debate ID systems, would do well to heed the whole debate as it has unfolded in the UK. Even though the Home Affairs Committee of the UK Parliament concluded that the ID proposals were ineffective, costly and a violation of civil liberties, the proposal has been pushed forward. Prime Minister Blair has assured the British public, against the evidence, that the civil liberties objections no longer carry weight and this seems to be linked to the often-heard argument of despair, that cards are already carried for every purpose anyway. Why not one more?

The reason why not is that other cards such as driver's licences, credit cards and passports are held voluntarily. The non-obligatory character of the initial ID system should fool no one. Once it is needed for a range of service-access it will become *de facto* compulsory. Moreover, the voluntary cards relate to single roles, as drivers, consumers or tourists whereas the ID card system gives the government powers – and this is the regulatory challenge – to monitor

[19] See www.guardian.co.uk/terrorism/0,,873826,00.html
[20] See *New York Times*, August 15 2006; www.nytimes.com/2006/08/15/world/europe/15visa.html?_r=1&oref=slogin
[21] There is disagreement, however, as to who is responsible for ID card developments within the EU. See www.statewatch.org/news/2006/jul/09eu-id-cards.htm/

activities across a range of roles that include the three mentioned as well as those more conventionally associated with government administration.

The challenges to would-be regulators of ID systems are thus manifold and urgent. If hard-won civil liberties are not to be stripped away in the name of a 'war on terror' or of dubious claims about greater administrative efficiency in service delivery, then ID systems need to be scrutinized very closely. The best possible ID system has civil liberties risks to be faced. The oversight of technical and legal provisions should be made more transparent and workable and public concerns should be heeded much more diligently. It is hard to escape the conclusion that at present the political need to be seen to be doing something and the persistent pressure from high technology companies seem to be dominant at present.

The best 'larger frame' for considering such matters is the notion of 'human security.' Although it is not in competition with 'national security' begins at a local community level and with the real everyday concerns of individuals and families. Combating terrorism is not usually high on such priority lists although freedom from fear and from want are more likely to be. According to Mary Kaldor, such 'human security' concerns may be locally rooted but they are simultaneously based in rights, multilateralism, legitimate government, and have a regional focus.[22]

New national ID systems play a crucial, pivotal role in the development of contemporary surveillance societies. Given the spiraling media-amplified public fears, the making of political mileage out of conspicuous and expensive 'anti-fraud' and 'anti-terror' schemes, and the corporate pressure from persuasive high-tech companies, the struggle for 'human security' and against civil liberties-compromising measures like ID systems is likely to be long and tough. But for the sake of common humanity it is a struggle eminently worth engaging.

[22] Mary Kaldor, 'What is human security?' in David Held, *et al*, eds. *Debating Globalization,* Cambridge: Polity, 2005, pp. 175-190.

Expert Report: Consumption and Profiling

Jason Pridmore
The Surveillance Project, Queens University, Kingston, Ontario, Canada.
9jhp1@qlink.queensu.ca

Introduction

The surveillance of consumption is the systematic gathering of personal data and transactional details regarding current and/or potential customers. It is a potentially broad area. Though many of the trends in the surveillance of consumption stem from "for profit" corporate sectors, surveillance of 'consumers' is also found in the public sector too: in relation to government services, health care, and airport security lines. [1]

Consumer surveillance has multiple purposes. Primarily it is used by companies to better understand the needs, desires, and trends within their customer base. It also generates data about the market performance of products and services, the success of particular marketing campaigns, or the demographic dispersion of customers. As it is part of institutional intentions to improve productivity and efficiency, it may also be used to evaluate the performance of employees in customer interactions, the timeliness of shipments, customer attrition and acquisition rates, consumer's "share of wallet" spending, and more. Data storage and retrieval costs have historically been limiting factors in the gathering of consumer data but consumer surveillance practices have increased in relation to advances in information communication technologies (ICTs). The decreasing costs for these technologies and the increasing ability to extract "actionable knowledge" and value from data has resulted in a "personal information economy" in which many corporations seek to gather as much consumer data as possible.[2]

Consumer data is now a viable commodity. It is sought in a variety of forms for the purposes of increasing productivity and, more importantly, *profitability*. The availability of data and advanced data processing techniques have led to a shift from mass markets towards markets of mass customization[3] based on what is digitally discernable or inferred about particular consumers' desires and needs.

[1] Education, disaster recovery, policing and other publicly oriented and oft funded practices are likewise gauged in consumptive terms. Numerous sources demonstrate this relationship. A very early discussion of government services as consumer items can be found in Rathmell, J. M. (1966) 'What is meant by services?' *Journal of Marketing* 30 (4):32-36. For a discussion of health care in terms of its consumption see Levins, R. (2003). 'Is Capitalism a Disease: The Crisis in U.S. Public Health.' in Hofrichter, R. (ed.) *Health and Social Justice: Politics, Ideology, and Inequality in the Distribution of Disease - A Public Health Reader.* San Francisco: Jossey-Bass. Last, despite recent concerns for airline security in the wake of September 11th, security itself has been relegated to the role of an efficient and expedient service. See the discussion of "through put" in Salter, M. (Forthcoming) 'Governmentalities of an airport: heterotopia and confession.' *International Political Sociology* 1 (1).

[2] See Dyson, E., Gilder, G., Keyworth, G., and Toffler, A. (1996) 'Cyberspace and the American Dream.' *The Information Society* 12 (3): 295-308. and 6, Perri. (2005) 'The personal information economy: Trends and prospects for consumers.' in Lace, S. *The Glass Consumer: Life in a Surveillance Society*. Bristol: The Policy Press.

[3] Mass customization is the process by which companies tailor their goods and services to large numbers of specific and specified consumers.

Key Developments

This section discusses the key dimensions of and recent developments in consumer surveillance. It reviews the types of data collected, techniques of analysis and its application within Customer Relationship Marketing strategies. It begins to speculate as to the associated privacy and regulatory concerns

The variety of consumer data gathered depends upon an organization's core business, and in the purposes for which data are to be used. Consumer data can be divided into four categories.[4] First, *geographic* data is used to describe a given region and includes population density, climate, and geographic features within a specific market area. These are demarcated by telephone area codes, postal codes, internet urls and domain names. This base information is always connected with specific and unique demographic information on consumers. *Demographic* data includes basic personal information such as name, age, sex, marital status, income, education, race/ethnicity, and occupation. A third set of data, *psychographic* data, connects the first two "geodemographic" forms of data to more social aspects of consumers in terms of class, values, lifestyle, life stages, and personality. Last, this data is connected to the consumer's previous interactions with the company. *Consumer behaviour data* includes frequency of patronage, brand loyalty, product preferences, product knowledge and marketing responsiveness. Data is categorised and coded by either an organization's in-house data analysis teams or through the assistance of one of the numerous data processing consulting agencies.

The types of data listed above are both created and collected in a number of ways. With increased attention given to consumer data, virtually every consumer transaction provides some form of "data trail," linkable either directly to a particular consumer or a particular type of consumer.[5] Personally identifiable data becomes generated through the use of credit cards, bank cards, mobile phones, the internet and more by means of connecting a particular consumer with a particular instance of use – that is, a purchase, search or phone call are all attached to a unique identifying number (such as a card/phone number or internet protocol address) that corresponds with the owner of that particular technology (the card, phone, or computer). This provides legitimate economic means for the exchange of money, information, services and products. Specific types of data are generated through specific channels, with a customer's enrolment in a program (loyalty, service agreement, membership, etc.) and subsequent transactions serving as the basis for a fair bit of the demographic and customer behaviour data. Additional data is generated through loyalty card programs, customer surveys, focus groups, promotional contests, product information requests, call centre contacts, web site cookies, consumer feedback forums and credit transactions. All of this data is *internal* to the corporation, though this proprietary data is often "overlaid" with more data to fill in or enhance what is unknown or unclear. This *external* data comes either from state agencies and non-profit organizations (National Statistics being a prime example) or from companies that specialize in consumer data collection. This business has seen dramatic growth, resulting in a burgeoning market for consumer databrokers who provide a wealth of knowledge to corporations eager to know more about their customers. Databrokers gather data by combining publicly available data (for example, the census and the phone book), with data produced by promotional contests, warranty information (complete with extensive surveys), door to door, telephone, and shopping centre surveys. They also examine media and informational subscriptions and track web page traffic. The data collected (which are geodemographic and psychographic data) are most readily connected to postal codes. These

[4] These categories are drawn from Michman, R. D. (1991) *Lifestyle Market Segmentation*. New York: Praeger. Also cited in Elmer, G. (2004) *Profiling Machines*. Cambridge, Mass: MIT Press.
[5] Cash transactions for example, though usually unable to be linked to a consumer directly are often analysed against similar past transactions and types of consumers who have made these purchases.

results serve to profile the inhabitants of a given street, from "prudent pensioners" to "fledgling nurseries" to "rustbelt resilience."[6]

The value in collecting consumer data is in layering of sets of data upon one another to create usable customer information. While customer names and addresses can be sold to provide basic templates for mass marketing campaigns and email addresses can be sold for internet "spam" solicitation,[7] the overlay of specific coded and categorized data creates value. Profiles provide the means for companies to target their marketing to a narrower band of consumers, thereby decreasing marketing costs and increasing response rates. This is frequently far cheaper than mass marketing channels of television, radio or print marketing. For example, a bank that has an agreement with a travel company may be able to market family holiday destinations to those it has categorized as families, with a different set of travel options to those who are retired.[8] Third party vendors may also provide lists of consumers who enjoy gardening (perhaps based on a magazine subscription) or of purported frequent travelers (perhaps drawn from survey research). The connections made between these sets of data are a result of 'data-mining' techniques designed to extract 'clusters' of data indicating patterns and relationships within a particular set of data.

More sophisticated data mining, often referred to as Knowledge Discovery in Databases (KDD), further assists in discovering previously unknown and *non-obvious* relationships within sets of information.[9] The "product" of these systems is perhaps most visible as the basis for web personalization systems, such as is employed by Amazon.com, which use multiple sources of data to predict the likely preferences of current shoppers.[10] These techniques enable both descriptions of patterns of behaviour and predictions for behaviour within a reasonable range of accuracy. They assume that a given customer will replicate the patterns of others before him whether or not these patterns are "obvious" or not. These models of consumer behaviour serve to demonstrate the propensity of consumers to buy certain products, respond to certain marketing campaigns, be at risk for attrition, become a credit risk, and more.

At its most basic, the modeling of consumer behaviour and the creation of profiles provide information for corporate marketing practices. They tell businesses where, when and why customers are shopping, and therefore where, when and how to market to them. Yet with more layers of data and more sophisticated analysis, these techniques can provide a "total" or "360 degree" view of the consumer. This view of the consumer, known as 'Customer Relationship Management' (CRM)[11] serves to simulate current and future engagements with individual customers.[12] Since the early 1990's, CRM has been a dominant marketing strategy,

[6] The former category is derived from the ACORN classification system by a company known as CACI and the latter two categories are MOSAIC classifications by Experian. More information about these products are available at http://www.caci.co.uk/acorn/ and http://www.business-strategies.co.uk/Content.asp?ArticleID=629. See also Burrows, R, and Gane, N. (Forthcoming) 'Geodemographics, Software and Class.' *Sociology*.

[7] The potential for use is limited by privacy legislation, as this example would legally require informed consent on the part of the consumer. The impacts of privacy legislation on data collection and its use are discussed in further detail below.

[8] Again, there are privacy limitations to the use of this information and the sharing between companies, yet certain clauses do allow for this scenario to occur, particularly if the marketing material comes directly from the primary data owner, in this case, the bank.

[9] For more on distinctions between KDD and data-mining, see Tavani, H. T. (1999) 'KDD, Data Mining, and the Challenge for Normative Privacy.' *Ethics and Information Technology* 1 (2): 265-273. Many sources discuss data mining as the overall process of working with data for the purposes described here. See Rygielski, C., Wang, J., and Yen, D. C. (2002) 'Data Mining Techniques for Customer Relationship Management.' *Technology in Society* 24 (4): 483-502 and Danna, A. and Gandy, O.H. (2002) 'All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining.' *Journal of Business Ethics* 40 (4): 373-386. For the purposes of clarity, the term KDD is used here to define the overall technical process that indicates particular affinities (obvious or not) within sets of data and data mining as the practice of accumulating critical data for further data analysis.

[10] See Fink, J. and Kosba, A. (2000) 'A Review and Analysis of Commercial User Modeling Servers for Personalization on the World Wide Web.' *User Modeling and User-Adapted Interaction* 10 (2-3): 209-249.

[11] Customer Relationship Management involves the electronic dispersion of personal data to analyze and create customised long term relationships with customers.

[12] CRM is now a fairly generalized marketing term that has been through a number of iterations. The term, derided for its poor performance in recent years, is also more commonly understood as data-mining itself, though this phrase tends to neglect the

with a shift in the focus of marketing toward customers and customer knowledge and, to some degree, away from products. CRM has been buoyed by CRM technology, and in the process, personal information has been actively sought and compiled about current and potential clientele in order to establish a continuing relationship that goes beyond a commercial transaction.[13] Historically, CRM was developed as an information integration system enabling a consistent flow of customer information throughout a corporation. For example, a company's call centre would hold the same customer information in real time as its retail outlets. The "relationship" part of CRM is specifically tailored to make these interactions consistent (at least in terms of information) throughout the enterprise. Yet it is this consistency in information that also makes it possible for corporations to *manage* their relationships with consumer, customising experiences by implementing consistent variations in service levels, product offerings and prices to each distinctive consumer.

Corporations use CRM techniques to create a consistent relationship between their customers and their corporate "brand," and, at the same time, "brand" their customers by sifting through customer data in order to predict their behaviours.[14] CRM serves as a means for sorting customers into categories of future risk and potential profitability. By knowing the social and economic background of current and potential customers, and by mining data, CRM allows business to discover, predict and attach a likely "customer lifetime value" (or CLTV) to each customer, to a degree of statistical accuracy.[15] Businesses are able to identify with whom they wish to continue doing business, both to what extent and at what costs, as well as sort out those that "do not fit their business model."[16] To some, particular product offerings are given, and particular levels of service deemed appropriate. For others, fees and rates are raised and assistance is minimised. The overall process essentially fragmented bits of data being gathered together, coded, and used to persuade customers into relationships which are more profitable for the corporation.

Critical commentary and future directions

Despite the economic value inherent in consumer surveillance – in 'knowing' your customers – it raises several critical issues. The surveillance of consumption must be understood as a dynamic process; data, profiles and models are continually being evaluated, augmented and tweaked for maximum performance. Yet it should not be understood as a simple process by which corporations gather and use data, but as the entire mechanism by which consumers are persuaded to continually divulge their personal information. This section begins to address some of the issues raised by consumer surveillance. In particular, technological developments, social sorting, discrimination, transparency and function creep are all important, as is the vulnerability of consumers and their data in a growing personal information economy. The information privacy issues raised by consumer surveillance are discussed in the final section which covers regulation.

As is the case with most forms of surveillance, data processing techniques form the backbone of consumer surveillance. Its current and future development lies in finding new means of creating, collecting, consolidating, categorizing and layering data. There are two key *technological developments* which are emerging as important: tracking consumers geographically in real time, and the formation of data co-operatives. Radio Frequency

effects of data-mining techniques. For further discussion see Kolsky, E. (2004) 'Want to Succeed in CRM? Don't Call it CRM.' Gartner research. 8 April. ID Number DF-21-1017.

[13] See Morgan, R. M., and Hunt, S. D. (1994) 'The Commitment-Trust Theory of Relationship Marketing.' *Journal of Marketing* 58 (1): 20-38.

[14] More on the "branding" of customers is discussed in Deighton, J. (2005) 'Consumer identity motives in the information age.' in Ratneshwar, S and Mick, D.G. (eds.) *Inside Consumption: Consumer Motives, Goals and Desires.* London: Routeledge.

[15] See Danna and Gandy, op cit 9

[16] See Ryals, L. (2002) 'Are Your Customers Worth More than Money?' *Journal of Retailing and Consumer Services* 9 (5): 241-251, Bergeron, B. (2002) 'CRM: The Customer Isn't Always Right.' *Journal of Corporate Accounting & Finance* 14 (1): 53-57.

Identification (RFID) tags and Global Positioning Systems (GPS), both of which are currently used for tracking products and corporate assets are a key component of the former. These technologies are seen as a means to produce customized marketing in real time to particular consumers, offering discounts on mobile devices to retail outlets in a given location, for instance. Despite the potential in this area, use has been fairly limited. Both RFID and GPS use have been hindered by the costs of the technology compared to the costs of the products to which they are attached. Applications for these have largely been a part of personnel and inventory management, both forms of workplace surveillance, yet as these technologies continue to become less expensive it remains likely that these location tracking devices, especially RFID chips, will be used to monitor both consumer products and consumers themselves.[17] Continued developments in the application of real time geographic data to consumer profiles will provide yet another layer of data to assist corporations in targeting marketing campaigns to particular consumers.

As layers of data comprise most of the value in consumer surveillance many corporations actively seek to enlarge their current databases. While a significant amount of information is provided by third parties, some corporations have developed mutual use policies with other companies. Partners within coalition programs such as those found in loyalty marketing often have agreements for some sharing of data, usually through the main coalition partner, but there is also a trend toward the creation of data cooperatives in which members share pooled sets of data. The Nectar card operated by Loyalty Management UK has over 50% of the UK population holding one of their loyalty cards. 216 catalogue companies in the UK are signed up to the Abacus data-sharing consortium, with information on 26 million individual consumers enhanced by Clarita's Lifestyle Universe. This overlays income, lifestyle, and life stage data at an individual level for each of these customers.[18] As future directions for consumer surveillance hinge on innovations in data use, the sharing of sets of data remains a concern for regulators because it challenges some key parameters of data protection legislation. This is discussed later in the report.

Social sorting processes and *discrimination and exclusion* are further areas of concern. As consumers continually supply business with their consumption data, they are part of an evolving feedback loop that binds acts of consumption with the gathering of transaction-generated data.[19] Consumers have come to expect that forms of personal data will be required of them in economic transactions. Moreover, they are often rewarded for providing personal information, (for example, when they benefit from loyalty programs), but otherwise do not believe that consumer surveillance has any effect on their day to day lives. Yet in this process, consumers are implicated into a system that perpetuates and reinforces systems of stratification, building up categories based upon their participation. For example, consumer profiles are attached to the particular geographic locale in which they reside. Overlays of consumer behaviour, psychographic and demographic data are anchored by the heavily weighted data of place, serving to determine, for example, the rate at which a customer service call will be answered, the costs of insurance, internet prioritisation, and the marketing exposure to which a consumer is subject.[20] Again, this is based on how much of a profitability "risk" a consumer in a given area may prove. While this may allow for potential flexibility in social mobility for some – by being in the right place at the right time and with the right data trail – place may also to perpetuate social divides in the imposition of negative consumer identities upon unsuspecting residents. Consumer surveillance serves to indicate who merits differing forms of corporate investment, and perpetuates stratification in specifying the

[17] More on current use and potential issues with location technologies is available in a report produced for the Privacy Commissioner of Canada, found at http://www.queensu.ca/sociology/Surveillance/files/loctech.pdf

[18] See Evans, M. (2005) 'The data-informed marketing model and its social responsibility.' in Lace, S *The Glass Consumer* Bristol: The Policy Press.

[19] This is detailed in Elmer, op cit 4

[20] See Graham, S. (2005) 'Software Sorted Geographies.' *Progress in Human Geography* 29 (5): 562-580 and Burrows and Gane, op cit 6

products and services for particular geographic locales. The risk of investment is therefore passed from the corporation to its potential consumers (and their geographic location), though there is little indication as to the means by which consumers and their neighbourhoods increase or decrease as a cost intensive risk.

What is significant in this is that consumers remain ignorant of the social and moral order created by the categorization practices they assist in producing. They are unaware of the way in which they are discriminated into previously categorised “lifestyle groups” on a per person basis and the way in which these categories come to define their expected and potential behaviour. Profiles serve to “describe” the consumer by setting the parameters in which consumers are expected to act;[21] deviations are limited and unexpected. Each engagement of the consumer with marketing is defined by prior data processing, and though these may be articulated as singularly customized representations, “a million segments of one”, businesses understand ‘consumers’ as the accumulation of statistically defined categories. More often than not consumers come to fit these prescribed expectations. What is unclear is how rigid and permanent these valuations remain.

One of the more alarming issues in this process is that the data gathered is rarely verifiable – the *accountability and transparency* of these processes is virtually non-existent. Incorrect or disputable data is integrated with little to no recompense for its contestation, despite clear requirements for this within privacy legislation. Data gathering practices are opaque, and the evaluation of personal information is invariably tedious and time consuming. Regardless of data quality, business interests are in the consumer profile as a whole. The effects of these profiles and their categories, whether visible or invisible, and whether contested or not, remains the same: consumers engage in a consumer society differently, because of the opportunities and limitations that are distributed among them.[22]

There is also an increased *function creep* between the information gathered through consumer surveillance and the concerns of security and intelligence agencies in the post 9/11 era. Not only are the same data-mining techniques developed for profiling consumers being used by security and intelligence services to profile potential terrorists, often the very data from which these profiles are created are the same. There remains a continual concern that privacy regulations were, are and will be overlooked and overridden due to concerns for national security. The increasing depth and breadth of consumer data remains an important element of information in scrutinising differing illegal activities, yet the potential for ensnaring innocent consumers in the process of using this information, thereby casting some into self-reinforcing categories of suspicion remains an important concern.

All of these issues are compounded by the fact that data created through consumer surveillance is never fully secure. Consumers *remain vulnerable* to accidental leaks, inappropriate disclosures, and theft of their data at any time. In the UK, companies are not required to disclose security breaches involving consumer data, though disclosures in the US (due to requirements of some state legislation) and other countries indicate that mishaps in the handling of data occur on a fairly frequent basis and to a large portion of the population.[23] Surveys indicating high levels of anxiety about the security of personal information and media reports regarding breaches of public and private security systems are pervasive in news

[21] See Zwick, D., and Dholakia,N. (2004) ‘Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing.’ *Journal of Macromarketing* 24 (1):31-43.

[22] This is discussed in more detail in Jenkins, R. (2000) ‘Categorization: Identity, Social Process and Epistemology.’ *Current Sociology* 48 (3):7-25.

[23] For a continuing chronology of data breaches made public in the United States, beginning with the infamous example of Choicepoint (where phoney companies were given personal data) to other relatively high profile incidents (including security compromises at Lexis Nexis and the US Department of Veterans Affairs) see http://www.privacyrights.org/ar/ChronDataBreaches.htm. For arguments as to why these breaches seem to be more prevalent in the United States that in Europe, see Cline, J. 2006 ‘Why isn't Europe suffering a wave of security breaches?’ http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001176.

reports. The fears that underlie these reports are not unfounded. A consumer's personal information can be used to secure loans, illegally purchase goods and services, or withdraw money from personal accounts. . This "identity theft" – the wholesale lifting of a persona – results in millions of pounds being lost each year and may occur as the result of internal theft of information (an employee uses access to sensitive data for personal profit), breaches in security (in which information systems are compromised by types of hacker activity) or purposeful disclosure of information to fraudulent corporations. Identity theft may also occur as the result of internet "phishing," where perpetrators create a fraudulent website that seems to be that of a legitimate (usually recognizable and trusted) business, through responses to unsolicited email known as "SPAM," or through computer viruses and "spyware." A majority of identity theft occurs at a personal level in which paper documents (stolen from one's post or out of their rubbish) are pilfered for personal information such as appears on discarded receipts, bank statements, credit card bills, cheque stubs, etc.[24]

Consumers have become increasingly vulnerable within the personal information economy. The tremendous reliance on particular technologies and unique numbers or codes to indicate identity creates opportunities for informational abuse and exploitation. Continuing innovations in data processing and increased collections of different types of data lead to social sorting practices rife with concerns for discrimination and exclusion. Further, the gathering of data for one purpose may always be used for another, particularly when certain concerns are deemed as more imperative than others. The vulnerability of consumers is also evident by the fact that corporations are neither fully held accountable for the data they collect or for the effects their mechanisms of categorization (whether based on valid or erroneous information) may have upon their customers. It is the concern over consumer's vulnerability that creates a pressing need for and challenges to the regulation of consumer surveillance.

The challenge of regulating consumer surveillance

Consumer surveillance makes good business sense. Increasingly it is action upon customer knowledge that demarcates the line between corporate solvency and bankruptcy. This is particularly true as businesses are able to effectively evaluate the layers of consumer data against forms of economic data, such as market indicators of interest rates, consumer confidence, inflation, etc. The concern here is not the elimination of these categories but rather how to balance the essential requirements of remaining fiscally prudent with the social, ethical and political issues that have and may arise. As data capture and the production of consumer profiles are integrated into the very fabric of everyday life, the continuing application of automated social classifications processes raises a number of regulatory concerns.

The challenge in regulating the use and flow of personal data within consumer surveillance is in ensuring that the boundaries of categories imposed upon consumers remain (somewhat) fluid and flexible. That is, the categories created by the analysis of data may be seen to perpetuate forms of social stratification antithetical to democratic sensibilities. In that the information processing by private corporations leaves unclear the potential for movement between the imposed categories, the concern is that these may more permanently set all interactions and expectations of particular consumers for life; these would be problematically self reinforcing for certain segments of the population. Therefore it is important that regulators provide the means for consumers to address the opaque nature of consumer

[24] There are a number of resources on identity theft. The Home Office has set up a website at http://www.identity-theft.org.uk/. The UK fraud protection agency CIFAS, which was created by consumer credit companies, has a dedicated section on identity fraud in their website found at http://www.cifas.org.uk/identity_fraud.asp. A report by the Congressional research Service was made to the US Congress focusing on issues of identity theft and the internet, found at http://www.opencrs.com/document/RS22082/. An extensive discussion of identity theft made by the Information and Privacy Commissioner of Ontario (Canada) is available at http://www.ipc.on.ca/docs/idtheft-e.pdf.

surveillance, strengthening existing privacy legislation and providing for more corporate transparency in information processing.

This also suggests that consumers need to be more actively engaged in recognising the importance of their own information processing. There are some attempts at resisting the routine collection of personal information, with varying degrees of organization and with varying degrees of effectiveness,[25] but largely consumers remain willing to forfeit their personal information to companies they deem as trustworthy. Consumers tend to be sceptical about revealing personal information to corporations they are less familiar with, but a number of factors influence what information they may or may not divulge.[26] It is the perceived benefits of participating, whether found in the incentives of loyalty programmes or in avoiding confrontational moments (by refusing to provide your phone number, for instance), that perpetuates participation in these systems. Consumer education about the use of personal data needs be a priority alongside its regulation.

An equally important democratic imperative is that the boundaries that ensure limited informational access to external agencies remains inflexible. That is, regulators must minimise information sharing and fiercely regulate the use of consumer data by government agencies, external corporations, healthcare providers, security agencies and insurance companies. There are instances in which consumer information may be of substantive use for criminal and security agencies, but these need to be narrow in focus as more widespread castings of informational nets may unnecessarily impose negatively associated identities upon particular citizens. The use of consumer databases is also a concern for how credit referencing, which merges financial and insurance information, may be connected to health and welfare databases. Fraud remains a crucial concern here, and more information is seen as a means for minimising the risk posed by false claims. Yet depending on how this information is used, this may affect the opportunities and life chances afforded to those who utilize and/or rely heavily on these social services by identifying them as high risk.

The breadth and depth to which consumer surveillance may go should therefore be limited. Privacy legislation within the European Union and countries that have enacted similar omnibus legislation[27] stipulate limitations on the collection and use of personal data, and require both that purposes be specified and security safeguards remain in place for personal data. Two of the "Fair Information Practices" (FIPs) included in the legislation are incompatible with the data mining techniques that underlie consumer surveillance. First, the use of data can not be clearly specified to the consumer. It is impossible to predict the results of data analysis conducted with technology designed to discover non-obvious relationships and patterns within sets of data. This means that corporations are unable to inform customers fully as to the use of their data, as the categories produced by data analysis are emergent. Second, because the principle of limiting the use of information defeats the very purpose for the collection and use of consumer data. The increase in data and potential variables increase the system's predictive accuracy.[28] Beyond the issues with these FIPs, even though privacy legislation limits the use of *personally identifiable* information, information stripped of these identifiers can continue to be used for consumer surveillance practices. This in turn can have the same effects for those categories of high risk consumers.

[25] Resistance to the collection of phone numbers at retailers and concerns about frequent flyer programs abound in internet web logs, though no empirical studies have been done to document this. One organization based in the US, Consumers Against Supermarket Privacy Invasion and Numbering, boasts an extensive and international listing of grocery store loyalty programmes. The organization aims to educate consumers, condemn marketing strategies that invade shoppers' privacy, and encouraging privacy-conscious shopping habits. More information is available at http://www.nocards.org/.

[26] See Phelps, J., Nowak, G. and Ferrell, E. (2000) 'Privacy Concerns and Consumer Willingness to Provide Personal Information.' *Journal of Public Policy & Marketing* 19(1): 27-41.

[27] For example, Canada and Australia have both enacted similar legislation. The United States and the EU have a "safe harbor" agreement that allows for some cross border transfers of personal data.

[28] For an extensive discussion of these issues with FIPs, see Tavani, op cit 9

The intention of current privacy legislation – that which is most often seen as the antidote to surveillance concerns – is to provide for increased informational control. While privacy legislation does mitigate some of the concerns inherent in consumer surveillance, its individualised focus and the hidden information processing techniques means that social categories and their effects are concealed from those directly affected by them. Genuine informational control requires an increase in corporate transparency regarding data gathering and information processing as well as clear indications of when the security of personal data has been breached. The difficulty is in balancing this transparency with the demands of a highly competitive economy in which transparency may in fact undermine the advantages gained through a corporation's data processing. Without finding this balance, whether through regulatory regimes or ethically transparent corporate practices, the concern remains that consumer surveillance will continue to perpetuate and amplify social divides and sorting that is antithetical to democratic principles. Consumer surveillance then stands to increase as a "cybernetic triage" separating consumers based on their presumed economic and political value rather than on their initiative and self-determination.[29]

[29] This is what is understood as "the panoptic sort" described in detail in Gandy, O. H. (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo.: Westview, 1.

Expert Report: Criminal Justice

Clive Norris
Centre for Criminological Research, University of Sheffield, UK
c.norris@shef.ac.uk

Introduction

The last decade has witnessed a massive programme of organisational and legislative reform aimed at transforming the criminal justice system. For New Labour the criminal justice system was in a state of crisis caused by the continuing trend for the number of reported crimes to rise year after year, while the number of crimes cleared up and offenders brought to justice had simultaneously fallen[1]. Strategies aimed at reducing this so called 'Justice Gap' have been at the heart of New Labour's criminal justice policies and justified the coordinated reform of all the agencies involved in the system so that they may contribute to 'Narrowing the Justice Gap'[2]. The prison and probation services have been unified into a National Offender Management Service, with probation being forced to shed its social work roots, which emphasised its role in advising, assisting and befriending the offender, to one primarily concerned with delivering 'punishment in the community'[3]. Similarly, the tension between welfare and punishment centred approaches that always surrounded the provision of youth justice services has been firmly resolved on the side of punishment. The Youth Justice System has been reorganised into multi-agency Youth Offending Teams, with a narrowly defined objective of reducing offending through intensive work with known offenders and preventative work with those at risk of offending[4]. The courts have been given a wide array of new powers to tackle both low-level crime and disorder, such as Antisocial Behaviour Orders and Curfew Orders. For more serious offenders, custodial tariffs have been increased and new sentences introduced such as Drug Testing and Treatment Orders, and Intensive Surveillance and Supervision Orders. The Crown Prosecution Service has undergone major structural reorganisation and has been explicitly charged with bringing more offenders to justice more quickly. Finally, the police have undergone a radical programme of restructuring which simultaneously decentralises the provision of front line policing to the 376 basic command units, while at the same time increasing centralised, Home Office control, by explicitly linking police performance at the local level to an agreed set of national standards and targets[5].

The heart of New Labour's modernisation agenda has been to transform a set of disparate agencies into a coordinated and joined-up system. In particular this has involved the complete modernisation of the way information is collected, stored and shared within the criminal justice system. The result has been a huge investment in IT provision, both to furnish the police with a host of new databases recording details of citizens and offenders, and to ensure that information is shared between all the agencies involved in delivering the Government's crime reduction programme. Underpinning this is a consistent commitment to

[1] Home Office (2001a) *Criminal Justice: The Way Ahead*, Cm 5074, London: Home Office
[2] Home Office (2002) *Narrowing the Justice Gap: Framework*, London: Home Office
[3] See chapter 5 Newburn, T (2004) *Crime and Criminal Justice* Policy, Harlow: Longman
[4] ***ibid.*** See chapter 8
[5] Home Office (2001) *Policing a New Century; A Blueprint for Reform*, London HMSO; Home Office (2004) '*Building Communities, Beating Crime: A better police service for the 21st* Century' London HMSO

utilise surveillance strategies and technologies in an effort not only to drive down crime generally but, specifically, to proactively focus on the 'hardcore' of persistent offenders that the Government believes is most responsible for the crime problem[6].

The extent of this commitment to surveillant solutions is documented below. First by examining how as citizens, suspects and convicted offenders we are increasingly subject to monitoring, testing, and recording at all stages of the criminal justice process. Secondly by examining the central role of IT systems and their attendant databases to the Government's strategy in reducing crime.

Surveillance of the general population

One of the most significant developments in criminal justice has been how surveillance, that was once reserved for the investigation of serious crime and targeted at the professional criminal or politically motivated suspect, has become extended to cover the majority of the population as it moves through public space.

It is now difficult for the average UK citizen to avoid being caught on cameras as they go about their daily business as it is estimated that there may be as many as 4.2 million CCTV cameras in Britain: one for every fourteen people.[7] Some estimates suggest that a person is captured on over three hundred cameras each day.[8] While this includes the privately owned cameras operating in the semi-public spaces of the shopping mall, restaurant or garage forecourt for example, it also attests to the huge investment of public funds in installing CCTV in city centres and high streets, schools, hospitals, and transport facilities. Indeed, during the 1990s the Home Office spent 78% of it crime prevention budget on installing CCTV[9] and an estimated 500 million pounds of public money has been invested in the CCTV infrastructure over the last decade.[10] The extent to which it has achieved its goal of reducing crime and enhancing the feeling of public security, is questionable. The major Home Office funded evaluation of the effectiveness of CCTV concluded:

> That the CCTV schemes that have been assessed had little overall effect on crime levels … (and) … CCTV was found to have played no part in reducing fear of crime; indeed those who were aware of the cameras admitted higher levels of fear of crime than those who were unaware of them.[11]

While citizens are largely anonymous as they walk under the gaze of a high street or shop CCTV system, this is not true as they drive along the nation's roads and, increasingly, the car licence plate registration number is being used to identify the registered owner of the vehicle. As a result, since 1996 there has been a dramatic increase in the camera based enforcement of speed restrictions; increasing from just over 300,000 in 1996 to over 2 million in 2004 and raising an estimated £113 million in fines per annum.[12] While the introduction of CCTV has

[6] Home Office (2001a) *Criminal Justice: The Way Ahead*, Cm 5074, London: Home Office, 20-23, but for a critique of the policy see Garside, R. (2004) *Crime, Persistent Offenders and the Justice* Gap, London: Crime and Society Foundation.

[7] McCahill, M. & Norris, C. (2003), 'Estimating the Extent, Sophistication and Legality of CCTV in London', in M. Gill (ed.) *CCTV*, Perpetuity Press

[8] Norris, C and Armstrong, G. (1999), *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford: Berg, 42

[9] *ibid.*, 54

[10] Norris, C. (2006) *Closed Circuit Television: a review of its development and its implications for privacy*, paper prepared for the Department of Home Land Security Data Privacy and Integrity Advisory Committee quarterly meeting on June 7th, in San Francisco, CA

[11] Gill, M. and A. Spriggs (2005). *Assessing the impact of CCTV*. London, Home Office Research, Development and Statistics Directorate.43, 60-61

[12] Wilkins, G. & Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office 1998; Ransford, F., Perry, D. and Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, London: Home Office

enjoyed high levels of public support[13] and favourable media coverage, speed cameras have been the one area where the increase in state surveillance has received a consistently negative press and provoked widespread public criticism.[14] This is despite the fact that speed cameras, unlike open street CCTV, have been shown to be effective and to have a significant impact in reducing death and injuries cause by traffic accidents.[15]

The intensification of surveillance of the motorist is set to expand rapidly over the next few years. By coupling the camera to a computer it is possible to read automatically the licence plates of passing cars and check them against the records held by the DVLC[16] and databases held on the Police National Computer (PNC). In 2003 the Home Office announced a national pilot of the Automatic Number Plate Recognition (ANPR) schemes as part of its general crime reduction initiatives. The pilot involved twenty-three police forces setting up fifty ANPR enabled intercept teams typically consisting of six officers operating from either cars or motorcycles who would stop vehicles that were flagged on various police databases as of police interest. In their first nine months of operation over twenty million vehicle registrations marks were read and 900,000 of these were flagged on police databases as being of interest to them. As a result over 130,000 vehicles were stopped and over 10,000 people arrested, three quarters for non-driving related offences.[17]

In the light of the pilot, in March 2005, the Association of Chief Police Officers published its strategic report on the development of ANPR, entitled 'Denying Criminals the Use of the Roads'[18]. Their vision: to create a national network of Licence Plate Readers 'utilising police, local authority, Highways Agency, other partner and commercial sector cameras'[19] and this includes integrating the existing town centres and high street cameras where they can be made ANPR compatible[20].

The strategy calls for each of England and Wales' forty-three police forces to establish at least one Intercept team by 2006, increasing to over 300 by 2008. They will be linked to the National ANPR Data Centre, which is planned to have an operational capacity to process 35 million ANPR reads every day increasing to 50 million by 2008. The centre will store details of each vehicle's movements for two years.

While camera-based surveillance has cast the surveillance gaze broadly over the entire population, two other forms of police surveillance routinely impact on citizens lives; the breathalyser testing of those suspected of drink driving and the stop and search of people whom the patrol officer believes to have been involved in crime. The roadside breath test was introduced in 1967 and requires suspected drink drivers to blow into a breathalyser to determine the level of alcohol present in the body. If the test is positive, the suspect is required to attend the police station to provide a further blood or urine sample in order to determine a more accurate measure of alcohol levels. By 1970 around 73,000 roadside tests were carried out which had increased to 577,000 in 2004, resulting in 105,000 prosecutions.[21]

[13] See for example Bennett, T. and Gelsthorpe, L. (1996) 'Public Attitudes Towards CCTV in Public Places', *Studies on Crime and Crime Prevention*, 5/1:72-90; Ditton, J. (2000) 'Public Attitudes towards Open Street CCTV in Glasgow', *British Journal of Criminology*, 40 692-709 and; Gill and Spriggs op cit.

[14] McCahill, M. & Norris, C. (2003), 'Estimating the Extent, Sophistication and Legality of CCTV in London', in M. Gill (ed.) *CCTV*, Perpetuity Press.

[15] PA Consulting (2004) *Denying Criminals the Use of the Road*, t:http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary Accessed 06/09/2006

[16] Drivers and Vehicle Licensing Centre

[17] PA Consulting , ibid

[18] Association of Chief Police Officers (2005) *ANPR Strategy for the Police Service 2005-8: Denying Criminals the Use of the Road*, London ACPO. Avialable at: http://www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc Accessed 06/09/2006

[19] ibid, 6

[20] ibid, 18

[21] Wilkins, G. & Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office; Ransford *etal* op cit.

In 2004/5 the police stopped and searched just over 850,000 people and around one in ten (11%) of the stops resulted in an arrest.[22] Stop and search powers do not impact on all sections of the community equally, with black people being six times more likely to be stopped and searched than white people.[23]

Police surveillance of those arrested

Although arrest might seem to be a rare event affecting only a small proportion of the population, in reality arrest is quite common-place, with some 5250 people arrested by the police in England and Wales each day; the equivalent of nearly two million people per year. Just under half are charged and one in seven are released with a formal caution. However, one in five of those arrested are released with no further action being taken against them.[24] Historically, when a person was arrested if they were released without charge, there would be no permanent, centrally held record of their encounter with the police, but in 2003 the Criminal Justice Act empowered the police to coerce all arrestees into providing fingerprint impressions and DNA samples. So even if a person is released without charge, or subsequently found not guilty by the courts, their records will remain on police databases and be accessible by the police national computer. The database of fingerprints now contains nearly 6 million sets of prints and the automation of the system has reduced the time taken to determine if someone has a criminal record from weeks or months to minutes.[25]

The National DNA Database was set up in 1995, and was originally confined to the investigation of the most serious of crimes such as rape and murder.[26] However, between 2000 and 2005 the Government invested an additional £240 million in the DNA expansion programme to ensure that ‘virtually the entire active criminal population would be recorded on the database’ by 2005.[27] In December 2005 the database held profiles on 3.45 million individuals, roughly 5.2% of the total population, although some sections of the population are more likely to be profiled on the database than others, as nearly 40% of black males are now profiled on the database compared with 9% of white and 13% of Asian males.[28]

The Drugs Act of 2005, which became operational in March 2006, gave the police the power to drug test all people arrested for certain trigger offences, including theft, robbery, burglary and begging. In total some 500,000 people, around a quarter of all those arrested each year, will be eligible for testing.[29] The tests are for Class A drugs such as heroin, crack, and cocaine. If the presence of drugs is found, regardless of whether they have been charged with any offence, a person can be required to attend a compulsory drug assessment to assess their suitability for enrolment on a drug treatment programme. Failure to supply a sample at the police station and failure to attend the compulsory assessment can result in a fine or imprisonment.

[22] Ayres, M and Murray, L. (2005) *Arrest for Recorded Crime (notifiable Offences) and the operation of Certain Police Powers under PACE England and Wales 2004/5* Home Office Statistical Bulletin, London Home Office.
[23] Home Office (2006b) ‘Operational Policing – Impact: about the Programme’ available at http://police.homeoffice.gov.uk/operational-policing/impact/impact-about-the-programme/; viiii Accessed 06/09/2006.
[24] Home Office (2001a) *Criminal Justice: The Way Ahead*, Cm 5074, London: Home Office, 122
[25] PITO (2005) Police Information Technology Organisation, *Annual Report 2004 – 2005*, HC 261, London Stationery Office.
[26] Williams, R (2004) ‘Circuits of Surveillance’ in *Surveillance and Society* 2 (1) 1-14
[27] Forensic Science and Pathology Unit - (2005) *DNA expansion programme 2000-2005: reporting achievement.* London, Home Office:3; Postnote (2006) *The National DNA Database*, Parliamentary Office of Science and Technology, February 2006 No. 258, 200
[28] *Guardian On-line* ‘DNA of 37% of black men held by police’ http://www.guardian.co.uk/frontpage/story/0,,1678168,00.html Accessed 07/09/2006.
[29] Derived from Ayres and Murray op cit.

Surveillance by the courts, prison and probation

Once a person has been arrested and charged they will be brought before a court to determine whether they should be released on bail pending trial or remanded into custody. The 2003 Criminal Justice Act gave the court the power to impose a drug assessment and treatment regime as a condition of being released on bail. Electronic monitoring has also been introduced as a condition of being granted bail and in 2004/5 some 631 adults and 5751 juveniles, some as young as twelve years old, were 'tagged' allowing them to await trial at home rather than be remanded into custody.[30] At the sentencing stage the courts can impose a Drug Treatment and Testing Order which makes a non-custodial sentence conditional on a person agreeing to undertake drug testing and enrolling on a treatment programme. In 2004/5 some 7,500 offenders were subject to the order[31].

The courts can also impose curfew orders enforced through electronic monitoring, requiring that an adult or juvenile offender is confined to their home during specified times. Typically, curfew orders are imposed for 12 hours per day and can be imposed on offenders as young as ten years old. Since 1999 the number of curfew orders has risen from 423 to over 25000 in 2004/5.[32]

Since 2001 eligible young offenders at risk of a custodial sentence from the courts have been able to avoid custody by enrolling on the probation led Intensive Supervision and Surveillance Programme (ISSP). The programme aims to address all aspects of a young offender's behaviour, lifestyle and cognitive skills with an aim of preventing them re-offending.[33] The ISSP can insist on routine drug testing to ensure offenders are not engaging in substance misuse and can subject offenders to a variety of additional surveillance measures. Minimally, at least two checks have to be made each day, with the potential of increasing the surveillance to continuous 24-hour monitoring. The checks include: face-to-face monitoring by a probation officer at specified times during the week who accompanies them to scheduled activities and appointments; electronic monitoring to ensure that curfew conditions are met; voice-print verification over the telephone to ensure that the person is where they say they are; and overt police surveillance 'of the movements of these young offenders at key times to reinforce the programme, as well as share information with the ISSP staff in the youth offending team'.[34]

Of the one and a half million people sentenced by the courts in 2003 some 107,000 were sentenced to immediate custody.[35] A sentence of imprisonment not only involves a loss of liberty but a loss of privacy as the offender is subject to almost constant surveillance. Since 1996, this surveillance regime has included mandatory drug testing with an expectation that between five and ten per cent of the prison population would be subject to a random test each month.[36] In 2004/5 a total of 51,484 tests were carried out, of which 11.6 percent were positive.[37]

[30] National Probation Service (2006) 'Satellite Tracking' http://www.probation.homeoffice.gov.uk/output/Page251.asp accessed 20th May 2006, 6.

[31] Home Office (2005) *Sentencing Statistics 2003* England and Wales. London Home Office

[32] National Probation Service 2006 op cit.: 6.

[33] Youth Justice Board (2006) 'Who is ISSP for?' available at http://www.youthjusticeboard.gov.uk/YouthJusticeBoard/Sentencing/IntensiveSupervisionAndSurveillanceProgramme/WhoIsISSPFor.htm Accessed 06/09/2006

[34] ibid.

[35] Home Office 2005 op cit.:3

[36] Singleton, N. *etal The Impact and Effectiveness of Mandatory Drug Testing in Prisons*, Home Office Research Findings 223, London Home Office

[37] Her Majesty's Prison Service (2005) *Her Majesty's Prison Service Annual Report and Accounts, Annex 1: Statistical Information*, London: Stationery Office:110

Once released from prison, offenders are also increasingly subjected to electronic monitoring either as a condition of early release from prison under the Home Detention Curfew Scheme[38] or as a condition of being released on Parole.[39]

From Criminal Records to Deviant Databases

At the heart of the police IT infrastructure is the Police National Computer (PNC). The PNC holds a range of databases and provides the ability to read external databases such as the register of drivers held by the DVLC and is now linked to more than 30,000 terminals across the country. The PNC started modestly enough in 1974 with an index of stolen vehicles, quickly expanding to include indices of: fingerprints criminal names, wanted and missing persons, disqualified drivers and sex offenders. It was, however, primarily a record keeping system, with very limited capacity for searching and cross-referencing[40] However, the last decade has seen the PNC moving from being an electronic filing cabinet to a fully-fledged intelligence tool in its own right with the ability to search across any of the fields. It is therefore now possible to locate, for instance, 'all red Jaguars registered in Hull' in a matter of minutes.[41]

Over the last few years the databases have been augmented in various ways. In 2001 in the UK the National Automated Fingerprint Identification System (NAFIS) was introduced, and contains nearly 6 million sets of prints. The automation of the system has been achieved through two PITO[42] led projects, Livescan and LANTERN. Livescan developed the hardware and software for the electronic recording, rather than paper based ink-based impressions, of a person's fingerprints, and LANTERN has created a mobile reader so that fingerprints may be taken at the scene rather than back at the police station.[43]

In 2004 the new Violent Offender and Sex Offender Register (ViSOR) was rolled out. It now contains details on over 50,000 offenders. ViSOR provides police and probation with a shared national database that contains an expanded set of information on offenders, including personal details, descriptive details, behavioural traits, details of risk assessment, intelligence reports, an activity log and a photographic[44] library

As already mentioned, a national strategy for automatic licence plate recognition (ANPR) was endorsed, creating a network of surveillance cameras which will automatically log the movements of millions of vehicles every day with a capacity, by 2008, to store up 50 million licence plate 'reads' per day. The data will be stored for two years to enable retrospective searching and the system will provide links to a variety of externally held databases. According to ACPO:[45]

> It will also drive criminal underclass vehicles off the road, virtually eradicating the opportunity to drive without a Vehicle Excise License, insurance, MOT, driving licence, proper registration of the vehicle or whilst disqualified. [46]

[38] The HDC scheme allows for those sentenced to between 3 months but under four years imprisonment to be released between 2 weeks and four and a half months early on a curfew enforced by electronic monitoring. In 2004/5 19096 people were release early under the scheme (NPS 2006 6).

[39] National Probation Service (2006) *Electronic Monitoring,* available at http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes Accessed 20/05/2006: 6

[40] Povey, K. (2000) *On the Record, Thematic Inspection Report on the Police Crime Recording, the Police National Computer and Phoenix Intelligence System Data Quality*, London: Her Majesty's Inspectorate of Constabulary: 74

[41] ibid

[42] PITO is the Police Information Technology Organisation and has an annual operation budget of £226 million to modernise the IT systems of the police and Criminal Justice System.

[43] Police Information Technology Organisation (2005), *Annual Report 2004* – 2005, HC 261, London Stationery Office

[44] Police Information Technology Organisation (2004) *Memorandum by the Police Information Technology Organisation to the Bichard Inquiry*, available at: http://www.bichardinquiry.org.uk.edgesuite.net/10663/full_evidence/0018/00180001.pdf Accessed 06/09/2006

[45] The Association of Chief Police Officers

[46] Association of Chief Police Officers (2005) op cit.: 14

One of the most recent initiatives has been a project to develop a Facial Images National Database (FIND), to be fully operational by 2009, which will allow the police to contribute to, and access, a library of photographic and video images. The database will have the ability to store more than one image for each person, and record the names and aliases associated with an individual and allow it to be crossed to all the associated data held on the PNC.[47]

The centrality of the database record is also evidenced by the introduction of Criminal Records Checks, which are now mandatory for persons seeking employment in jobs involved with the care of the young or vulnerable. Since 2002 it has produced 8.2 million disclosures of which around 400,000 contained convictions or police intelligence information.[48]

The development of the databases has been accompanied by a massive investment in the system architecture to allow information to be shared, both between individual police forces, and across all the agencies in the criminal justice system. Historically, police forces and the different agencies involved in criminal justice developed their own IT strategies, with little central co-ordination by government. As a result there were a plethora of local initiatives. This made data sharing between agencies difficult, if not impossible, and with the development of a host of multi-agency programmes, proved a major operational limitation to the partnership approach. This problem has been addressed by developing a criminal justice extranet to host a web-based communications system called the Criminal Justice Exchange (CJX), which will enable information to be shared across all the agencies of the criminal justice system.[49] Not only will this information be available at force headquarters and local police stations but, with the development of Airwave, the new police radio and digital communication system, the patrol officer on the street will be able to access all the databases of the PNC directly via a hand held computer at the scene rather than having to return to the police station.[50]

The most ambitious project to date was announced in 2005 when, in response to the Bichard Enquiry[51], the Government announced plans to create a single national police database that would integrate all the databases held centrally on the PNC with a all those held locally at force level.[52] The new natonal database is expected to become fully operational in 2010 In the meantime a number of interim solutions are being developed[53] until the Cross Regional Information Sharing Project (CRISP) becomes operational. CRISP will 'take the Police Service through a process of aggregating its data into local data warehouses which is the starting point for national information sharing'. Eventually this will bring 65 million computer records and 11 million paper records, related to around 10 million individuals on to a single centrally controlled database.

[47] Police Information Technology Organisation (2006) *Facial Images National Database (FIND),* available at http://www.pito.org.uk/products/FIND.php Accessed 06/09/2006.

[48] BBC (2006) 'Criminal Records Mix-up Uncovered', *BBC Online news*, available at: http://news.bbc.co.uk/1/hi/uk/5001624.stm

[49] Criminal Justice Information Technology (2005) *CJS Exchange,* available at: http://www.cjit.gov.uk/glossary/#c

[50] ACPO (2002) - Association of Chief Police Officers – *Infinet: A National Strategy for Mobile Information*, Association of Chief Police Officers

[51] The Bichard enquiry into the murders of two teenage girls Jessica Chapman and Holly Wells squarely implicated the non-standardised and localised procedures of intelligence and information handling in hampering inter-force co-operation. The enquiry recommended that setting up an IT System capable of allowing police intelligence to be shared nationally should be a priority.

[52] Home Office (2006) 'Operational Policing – Impact: about the Programme' available at http://police.homeoffice.gov.uk/operational-policing/impact/impact-about-the-programme/

[53] Home Office (2006) 'Operational Policing – Impact: What we are delivering http://police.homeoffice.gov.uk/operational-policing/impact/what-we-are-delivering/ini/?view=Standard

Trends and trajectories

It is clear that the last decade has elevated the database to a pivotal role in criminal justice policy. Inscription in the databases means that electronic data-doubles are processed and evaluated to determine 'real world' interventions and consequences. For instance, the classification of a 'persistent' or 'prolific' offender is a statistical category determined by the number of convictions, over a particular period of time, an individual has accrued on the Nominal Index contained on the Police National Computer. This classification makes an individual a candidate for intensive targeting and intervention by a range of criminal justice agencies as part of the persistent offender strategy.[54] Once selected a candidate will be entered on the J-track system for tracking and managing persistent offenders at all stages of the criminal justice system.

With the development of the National ANPR Strategy the database is set to become an even more central feature of routine policing. For instance, under the ANPR strategy there is a plan to link garage forecourt cameras to the system, which will greatly increase the coverage of the system since, at some point, all vehicles must fill up with petrol. In exchange, the petrol stations will 'benefit from our intelligence telling them which vehicles to take payment from before they serve them'[55]

Similarly, the database of citizens' vehicle movements will be interrogated retrospectively to identify pattern associations between vehicles and their movements. Given that ANPR systems are not 100% accurate in reading license plate details[56], this means, inevitably, that information in the database will be compromised, and that the system may well lead to a person's vehicle being wrongly identified as associated with known criminals. This issue of misidentification on police databases was most recently illustrated when the Criminal Records Bureau revealed that around 2,700 people have been wrongly identified as having criminal convictions. As a consequence of the incorrect information contained in their data-doubles, a number were refused jobs (BBC 2006). The problem of the quality of the data held on the PNC has been highlighted by a number of reports from the Police inspectorate.[57] The prospect of the National Police Database also brings dangers as low-grade intelligence of uncertain providence is made available more widely and used as the basis for risk based decision-making by various agencies.

Information sharing

The effect of the massive investment in IT systems and software across the criminal justice system has been to allow for the integration and cross referencing of disparate databases held across police and criminal justice agencies. In effect this means there is now one 'master' file. For instance a vehicle passes under an ANPR system, its license plate is extracted, this is then checked against the DVLC register of licensed vehicles and their registered keepers. With this information, it is then possible to access all the other databases available on the PNC, for instance the database of fingerprints, criminal history, or violent and sex offenders register, and insurance and MOT databases. The extent of this integration is illustrated by Hertfordshire Constabulary's ANPR system which accesses 40 nationally or locally held databases when tracking a vehicle[58].

[54] Home Office (2004), *Prolific and Other Priority Offender Strategy Initial Guidance*, available at http://www.crimereduction.gov.uk/ppo_e.doc

[55] Association of Chief Police Officers (2005) op cit.

[56] PA Consulting (2004) suggest that the accuracy read is around 96%, which may sound high, however, even if only one percent of licence plates are incorrectly read and recorded on the data base, this would mean potentially up to half a million erroneous number plates logged each day.

[57] See for example Her Majesty's Inspectorate of Constabulary (2002) *Police National Computer: Data Quality and Timeliness, Second Report*

[58] Hertfordshire Constabulary (2005) *ANPR 'The Human Chassis Number'* Application for Tilley Award available at http://www.popcenter.org/Library/Tilley/2005/05-02.pdf

However, information sharing goes further. With the advent of multi-agency approaches to reducing the risk of crime and re-offending, the boundaries between criminal justice information and the information held by others are considerably blurred. For instance youth offending teams consist of representatives from police, Probation Service, social services, health, education, drugs and alcohol misuse services and housing officers and they have all signed an information sharing protocol so they may exchange information on individuals and families under their jurisdiction.[59] Similarly, the Identification Tracking and Referral System, developed in response to the recommendation of the Climbie Inquiry, creates an information hub which alerts practitioners to all the information held by the entire range of children's services including police and youth offending teams.[60] Under these circumstances, the compartmentalisation envisaged by data protection regimes, where information about an individual provided for one purpose should not be used for another without the express consent of the individual concerned, appears outmoded.

The issue of consent is compounded throughout the criminal justice system. We do not consent to CCTV system monitoring us we walk though public space, and no one has consented to having their vehicle movements logged at the ACPO's ANPR Centre. Arrestees do not consent, and are coerced, into providing fingerprint and DNA samples, which will be permanently logged on the police national database, even if they are released without charge. And, while a person cannot be forced to give a urine sample to test for the presence of drugs, it is hardly a matter of choice, as refusal can result in a fine, imprisonment or both.

The regulatory challenge

Given that much of the information now collected on citizens by the criminal justice system is collected without their knowledge or consent, it is almost impossible for a person to know how information is being used, and how it may, in subtle ways, affect their lives; for instance, by increasing the chances that their vehicle is stopped by the police, or the demand that they pay in advance for goods and services. The task of regulating this new environment is indeed challenging, and will need much thought and analysis to determine the appropriate response. It will also require an assessment as to how far existing Data Protection legislation is able to meet such a challenge.

So I will end with just one, tentative, and hopefully thought provoking proposal:

Citizens should have a right to know what information is held about them, and how it is being used. This right would require a positive reporting requirement on the part of the authorities to provide to each individual an annual information transaction report. The report would include a copy of all the data they hold and details of any processing it has been subject to. This would at least go some way to rectifying the asymmetry of power of the surveillance gaze, particularly where consent to use our personal data has been implied, rather than positively granted.

Of course there will be an immediate reaction that you can't give criminals and suspected terrorists access to the data held on them. Well maybe not, but then we would have to decide, as we should in a democratic community, what personal data, under what circumstances, should not be disclosed to its rightful owners.

[59] See Newburn op cit. 211ff for a discussion of Youth Justice Teams

[60] See for a discussion of the Climbie case see chapter 3 of Parton, N. (2006) *Safeguarding Childhood: early intervention and surveillance in late modern society*, Basingstoke Palgrave Macmillan.

Expert Report: Infrastructure and Built Environment

Stephen Graham
Department of Geography, Durham University, UK.
s.d.n.graham@durham.ac.uk

with

David Murakami Wood
Global Urban Research Unit, Newcastle University, UK.

Introduction: The Software-Sorted Society

Cities are rapidly becoming 'intelligent'. Infused with a myriad of digital sensors and surveillance systems, the built environments and infrastructures of cities are being managed, produced and used in ways which were unthinkable only a few years ago. Organised through millions of electronic tags, radio transponders, CCTV cameras, mobile phones and computers, and other digital devices, the movements, flows and interactions that constitute urban life are now tracked like never before. Indeed, in many ways, city spaces and infrastructure systems can now be thought of as structures of pervasive and continuous surveillance. These automatically sort and prioritise the life chances of people and places based on the judgements of computer code embedded in digital networks.[1]

The remaking of built environments and infrastructures through intensifying surveillance radically challenges the idea of anonymity that was long seen as one of the key aspects of city life. This is an ambivalent shift, full of possibilities and risks. The new ways of managing cities that have come with ubiquitous digital surveillance certainly help to create many new services, and a speeded-up urban lifestyle characterised by individually tailored services, continuous electronic and physical interaction, an always-on digital economy, and the transcendence of many of the time and space barriers that traditionally acted to inhibit urban life.

However, much less reported, the intensified surveillance of urban life also involves powerful processes of social exclusion. This is characterised by the creation of disconnections for those people and places deemed in some way unprofitable or risky. Crucially, then, the new surveillance technologies can thus forcibly *slow down* certain people's lives, making them logistically more, not less, difficult.

Importantly, then, new surveillance systems are being used to automatically sift and prioritise people's life chances and rights, adding radical new functionality and power to some people and places, whilst actually undermining and worsening those of others, both relatively and absolutely. The result is what Graham has termed a "software-sorted" society where software-based techniques, linked intimately to computer databases, increasingly sort users

[1] See Graham, S. and Wood, D. (2003) "Digitising surveillance: Categorisation, space and inequality," *Critical Social Policy*, 23, 227-248.

based on automated judgements of their importance, profitability, risk or value.[2] Such software-sorting surveillance systems increasingly work automatically (i.e. without human discretion), continually (i.e. 24 hours a day), and in real time (i.e. without delay). Very often, the motivation here is not surveillance or social control in itself. Rather, surveillance is used as a means to overcoming the barriers of electronic and physical congestion facing affluent, privileged or powerful people and places, as they confront the challenges of living and operating in dense, urban, and increasingly mobile societies which place a premium on networked connections and flows connecting to other places.[3] However, for neither the wealthy nor the underprivileged is this particularly negotiable, whether or not such controls were originally accepted voluntarily or even requested (as most are in the case of higher income groups) or were enforced. Once introduced, both access and blockage are increasingly policed automatically.[4] The main danger here is a tendency towards technological lock-in which threatens to divide contemporary societies more decisively into high-speed, high-mobility and connected and low-speed, low-mobility and disconnected classes and geographical areas.

Cities of Passage-Points

Such continuous software-sorting of people and their life chances in cities is organised through a myriad of electronic and physical ‘passage points’ or ‘choke points’. These, increasingly, help to make up the fabric of cities. They must be continually negotiated through a widening number of code words, pass words, PIN numbers, user names, access controls, electronic cards or biometric scans, as part of urban everyday life.

Such passage points vary considerably. They do so in three key ways. First, some are highly visible and obvious and are negotiated willingly and knowingly by users (as in a PIN credit card purchase or an airport passport control). Others are more stealthy and covert (as with the sorting of internet or call centre traffic allowing certain people’s traffic to be speeded-up whilst other’s is slowed-down or even blocked). Such stealthy passage points force users to unknowingly negotiate surveillance as a hidden background to their everyday life and movement. On still other occasions, the presence of the passage point is clear -- as with a CCTV camera on a city street or a speed camera on a motorway. But in these cases it is still impossible to know in practice if one’s face or car number plate has actually been scanned, or if the legality or legitimacy of one’s movement or presence has been assessed.

Second, whilst most passage points are now fully automated, and involve little immediate human supervision, some have resisted full automation and still involve human discretion. In such cases there are still ‘humans in the loop’ supervising and directing the surveillance process. Traditional CCTV control rooms, with operators directing cameras with joysticks, are a good example here.

Finally, passage points vary in their level of effectiveness. This depends largely on how difficult it is to comprehensively control access to the service or city space in question, without the produced borders or access controls being challenged, resisted or transgressed. Generally, here, electronic services and realms are relatively easy to control compared to physical urban streets which, by their nature, are more porous. Similarly, closed urban spaces which have tightly controlled passage points (like those between the ‘land side’ and ‘air side’ of airports, or at the entry points to malls or gated communities, are more easy to control and surveil than the open streets of a typical city centre. (We should remember, of course, that, in

[2] Graham, S. (2004) “The software-sorted city: Rethinking the ‘digital divide’.” In S. Graham (ed.), *The Cybercities Reader*, London: Routledge. 324-332. Graham, S. (2005), “Software-sorted geographies”, *Progress in Human Geography*, 29(5), 562-580. See also Lyon, D. 2003: *Surveillance as social sorting: Privacy, risk and digital discrimination*, New York: Routledge

[3] Andrejevic, M. (2003) “Monitored mobility in the era of mass customization,” *Space and Culture,* 6, 132-150.

[4] Lianos, M. (2001) *Le Nouveau Contrôle Social*, Paris : L’Harmattan; Lianos, M. (2003) ‘Social control after Foucault’ *Surveillance & Society* 1 (3): 412-430. Online. http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf (accessed 31 July 2006)

software-sorted cities, most passage points now involve *both* electronic and physical parts working closely together).

The Scope of this Report
This report develops an explicitly geographical approach to the current reorganisation of built environments and infrastructures through the widespread application of electronically surveilled passage points and software-sorting technologies. By exploring the background, context and main characteristics of such trends, its aim is to identify the key challenges facing Information Commissioners and Privacy Regulators, as the digital surveillance which now orchestrates so much of urban life continues to intensify and become more interconnected in the short and medium term. The discussion that follows falls into three parts:

- A general overview of key developments in geographical surveillance of cities and infrastructures;
- A more detailed discussion of specific examples and directions of change in the area; and
- An analysis of the challenges facing information commissioners and privacy regulators in this area.

'The Most Profound Technologies Are Those That Disappear': Three Key Developments

The starting point for our discussion is the assertion that organisation of the rights to services needed to sustain urban life by digital tracking and surveillance systems means that an explicitly *geographical* perspective is now necessary for Information Commissioners and Privacy Regulators. As surveillance practices become both more automated and more invisibly embedded in the wider urban environment, so an understanding of how they impact on privacy, social exclusion, empowerment and accountability becomes both more pressing and, paradoxically, much more difficult. After all, technologies are at their most important when they become ubiquitous, taken for granted, and largely invisible -- the background to everyday life which few seek to expose of question. As PARC Xerox's Mark Weiner argued in 1991, "the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it".[5]

The surveillance systems now being sunk into the fabric of cities and infrastructures, as the basis for radically reorganising urban life, are now at such a critical point. Because they literally orchestrate the flows, services and rights that sustain contemporary urban life, they require urgent analysis and regulatory attention. Without this, they and their effects will quickly be rendered largely invisible. This is because the technologies they rely on will increasingly be miniaturised and so blend into the background. But it is also because their effects will become so normal and taken for granted as to be virtually invisible from a cultural and regulatory perspective.

The time is therefore ripe to consider how the radical intensification of digital surveillance is helping to reorganise the ways in which cities and infrastructures work. To understand the challenges here, it is worth exploring briefly how surveillance relates to the geographies of cites.

It is not new for surveillance practices to become part of the geographies of cities, or for these practices to shape everyday urban life. But the remarkably rapid intensification of electronic surveillance which is currently underway presents an unprecedented set of transformations in

[5] Weiner, M. (1991), "The computer for the 21st century", *Scientific American*, 265, September, 94-104.

the connections between surveillance, built environments and infrastructures. Three main trends can be identified.

Towards Computerised Visual Surveillance

First, whole city districts and infrastructure systems are being subject to remote, visual electronic scrutiny for the first time. The several million CCTV cameras currently installed in the UK rely overwhelmingly on the discretion of human operators to function. Following early experiments of face recognition software in Newham, Birmingham, Tameside, Manchester, and other locations, however, a shift towards digital CCTV, which uses computer algorithms to automatically search for stipulated people or behaviours, is gaining momentum. Face recognition, and other biometric CCTV systems, still face major technical obstacles in operating outdoors on city streets. However, considerable research and development investment is rapidly addressing these.[6] This is part of a much broader exploration, often funded with support from the US/UK 'war on terror', of the use of interconnected 'smart' CCTV systems to track movements and behaviours of millions of people in both time and space. In industry parlance, this is called "multiscale spatiotemporal tracking".[7]

Although only in its infancy, the combination of biometric tracking -- based on scans of faces, retinas, irises or even facial expressions ('micro expressions') and walking styles (gait recognition) -- may allow the many 'islands' of CCTV systems in cities currently to be quickly joined up. This may prefigure a comprehensive collapse in the age-old notion of urban anonymity: security and law enforcement personnel may soon be able to identify people using computer databases or biometric signatures remotely and continuously track these people on an individual basis, as they move about within a city, or even within whole national or international systems of cites.

Software-Sorted Infrastructures

Second, the public spaces and physical and electronic infrastructures of cities are rapidly being restructured in ways that directly exploit the capabilities of new surveillance technologies. On the way out are universal and standardised provisions of access to services, spaces and infrastructures, based on notions of democratic citizenship, open access or traditional ideas of public services and spaces either freely accessible to all at the point of consumption or charged through universal tariffs. On the way in are notions of targeted services, infrastructures and spaces, accessible only to these who are allowed access, and priced very differently to different people and places.

Often, such shifts are based on commercial judgements and profiles of the ability of people and places for increasingly commercialised services. Here this is a widespread tendency to apply market principles, and differential pricing, to people and places at different ends of the social spectrum. On other occasions, such software-sorting reflects a desire to allow certain, privileged social elites to bypass the congestion presented by the mass of the population in increasingly crowded cities, urban corridors, or infrastructure systems. Such an approach is encouraged because a globalised, network-based society means that the ability to connect and move reliably is of paramount economic and social importance, especially for social and economic elites.

Many examples of commercialisation and bypass are relevant here. On our increasingly 'sanitised' shopping streets, for example, those deemed not to belong are increasingly tracked and removed by private and public security personnel. Car drivers who choose to pay electronic congestion charges in city centres or on premium highways benefit from reduced

[6] See Norris, C. 2003: "From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control." . In D. Lyon, (ed.) *Surveillance as social sorting: Privacy, risk and digital discrimination*, New York: Routledge. 249-281; Norris, C. and Armstrong, G. 1999: *The maximum surveillance society : The rise of CCTV*, Oxford: Berg.

[7] Hampapur, A. et al (2005), "Smart video surveillance", *IEEE Signal Processing Magazine*, March, 38-51.

congestion to the exclusion of the majority. Train travellers now access a labyrinth of different tariffs and prices based, using software-sorted web sites and call centres, on when they book their tickets, who they are, and even where they live. Business travellers opt in to biometric identity schemes allowing them to bypass immigration controls whilst those very same biometrics are being introduced to make those very same controls *less* penetrable to those whose mobility is not sanctioned. Even the electronic traffic on the Internet or the telephone queues in call centres are now routinely queued using new surveillance systems. This allows privileged or more affluent users to bypass congestion whilst those deemed a low priority are forced to wait, or are even dropped from the network on purpose. In a very real sense, then, the geographies of access and exclusion in our society are now being sorted automatically and continuously by hidden worlds of computer software.

The Geolocation and Pervasive Computing Booms

Third, befitting their role as a means to organize and coordinate the geographies of cities, surveillance practices are increasingly referenced, organised and located geographically.[8] Most systems of electronic surveillance are now actually organised geographically and are integrated with computerised maps known as Geographical Information Systems (GISs). Many actually track the geographical movements of people, vehicles or commodities using Radio Frequency Identification (RFID) chips, Global Positioning Systems (GPS), smart ID cards, transponders or the radio signals given off by mobile phones or portable computers. Whilst opening up the potential to improve logistics management, learn more about the make up of neighbourhoods, offer specialised or customised services, or track one's friends as they move around cities, this geo-referencing of surveillance brings with it major risks. Services and advertising can be targeted only at those deemed more profitable as they move about the city, as sensors automatically detect their presence. Computerised mapping systems can exacerbate the gaps between rich and poor neighbourhoods and ossify prejudice into urban geographies through the electronic 'red lining' of areas and people deemed unprofitable, risky, or problematic in some way.[9] And people's movements can be continually tracked for commercial or social control purposes, with such highly valuable information also traded at great profit on the burgeoning marketplace for geographically referenced data.

In most cases, any surveillance function of geolocational devices is secondary to their main purpose, or is used to enhance the primary purpose. A shop loyalty card provider, for example, may use the data on where someone shops (as well as what they buy) to target certain services at the holder. In some cases, surveillance is essential to the functioning of the technology involved. In the case of mobile phones, for example, if the system is unable to tell which geographical 'cell' a phone is currently located, no calls will be able to be transmitted or received. For GPS receivers, of course, the primary purpose is to establish exact location for the user, so surveillance of that user's position is vital.

Directions and Examples

To understand the challenges of regulating the electronic passage points and surveillance systems which now organise urban life, it is necessary to look briefly at some more specific examples of how the intensification of digital surveillance raises key questions about privacy, social exclusion, discrimination, transparency, accountability and surveillance creep in highly urbanised societies.

[8] See Institute for the Future, (2004), *Infrastructure for the New Geography,* IFTF, Menlo Park, California.

[9] Burrows, R. and Ellison, N. 2004: Sorting places out? Towards a social politics of neighbourhood informatization, *Information, Communication and Society*, 7, 321-326.

Towards Automated Visual Tracking infrastructures?

It is imperative that Privacy Regulators and Information Commissioners consider the challenges raised by a shift from multiple 'islands' of analogue CCTV (based on traditional video recorders and the 'Mk1 eyeball' of the control room operators) to biometric CCTV systems. This is a vital issue because biometric CCTV systems remove many of the constraints that have inhibited the size of analogue CCTV systems (primarily, the limits on the ability of an operator to monitor footage from a large network of cameras). Because biometric CCTV systems delegate the search for 'targets' of surveillance to computer software – usually in the form of facial recognition software -- biometric CCTV networks are likely to grow much larger, to reap the benefits of economies of scale and to cover larger geographical areas more economically. Biometric CCTV systems thus have at least the potential for interoperability and integration across larger and larger geographical scales.

The establishment of Automated Number Plate Recognition (or ANPR) CCTV camera systems across the UK road and highway systems provides a precedent here. Such systems offer an example of how extended tracking and surveillance systems can be 'knitted together' based on automated use of software, liked to centralised databases, which tracks subjects based on scanning them in some way. They also show how digital telecommunications, linked with centralised databases, allow shifts towards automated law enforcement across large geographical areas or infrastructure networks (in this case, for the policing of speeding cars on the main road network).

To computer ethics specialist, Phil Agre, a parallel shift to wide scale social tracking using face recognition CCTV on city streets would usher in a "tremendous change in our society's conception of the human person." It would mean that "people would find strangers addressing them by name" in previously anonymous encounters in city streets and commercial spaces.[10] More worrying still, commercial judgements, based on continuous connections to credit registers and the like, could lead to the regular exclusion and targeting of people deemed to be commercially marginal within increasingly commercialised and gentrified town and city centres.

Two particular challenges present themselves here. First, there is a danger that algorithmic CCTV systems will embed social prejudice deep into the very software that makes them work. With the discretion of camera operators increasingly removed, the code within the software that 'decides' which behaviours, appearances, faces and identifiers warrant further action, scrutiny, or exclusion, out of the mass of a city's or nation's population, becomes the key site for regulation. The difficult challenge here is for regulators to make transparent the types of faces, behaviours and movements that systems are designed to track as supposedly 'risky', 'threatening', 'abnormal' or 'of interest' within cities.

A range of pressing questions arises here. Are such systems likely to rely on crude racial profiling as bases for their operation? Will facial recognition databases be interoperable, allowing the possibility of individual tracking across larger and larger scales? Will such systems be used to police the boundaries of commercialised, gentrified or strategic city spaces, allowing those deemed to be 'failed consumers' within regenerated cities to be tracked and even excluded? Finally, how can ethical codes of practice and accountability be established to prevent abuse when the key algorithms that make face recognition work are themselves so difficult to scrutinise and make transparent, trapped as they are within what social scientists often call the metaphorical 'black box' which tends to surround automated technologies?

[10] Agre, P. 2001: Your face is not a bar code: Arguments against automatic face recognition in public places, *Whole Earth*, 106, 74-77.

Second, there is evidence that facial recognition systems are likely to have inbuilt social and ethnic biases. Evidence for this comes from a major test of emerging systems, the Facial Recognition Vendor Tests of 2000 and 2002.[11] This showed that the very physics that allows the systems to work are strongly influenced by the social, demographic or ethic characteristics of the human face under scrutiny. For example, recognition rates were higher for males than for females and for older people than for younger people. More troubling still, groups classified as 'Asians' and 'African Americans' were easier to recognise than Caucasians because the facial recognition software was programmed to search for the supposedly distinct physical characteristics of such populations.

Clearly, installing widespread face recognition systems whose inbuilt performance biases them to recognise and track particular age and ethnic groups more effectively than others raises major questions about how to regulate these emerging technologies. This is a particular risk with Western security rhetoric focusing overwhelmingly on monitoring and scrutinising people of 'Arab appearance' in the post 9/11 context.[12]

To pre-emptively inhibit or monitor the movements of a group of people simply because they fall into a category of people seen as 'risky' is clearly problematic. However, it should not be forgotten that, in many cases, categorical suspicion has an entirely justifiable and caring aim. For example, one pioneering set of algorithms, developed through the Chromatica and Prismatica programs,[13] has been tested with London Underground as the Intelligent Pedestrian Surveillance (IPS) system[14]. Although originally aimed at identifying places where crowd flow was blacked, it has become an effective tool for preventing suicides. It does this by combining the recognition of stationary blocks of colour on platforms (a person), with prior knowledge of the behaviour of suicides (who usually wait while several trains pass before jumping). The makers, Ipsotek, now market the software as part of a system of 'visual intelligence' that provides 'real-time incident detection' in CCTV systems[15], one of many such systems now available.

Software-Sorted Infrastructure

A wide range of pertinent examples are emerging in software-sorted infrastructure:

- *Road and Highway Congestion Charging and 'Intelligent' Public Transportation:* Growing parts of the UK road network are now being 'splintered' off from the main, public, and freely-accessible network, to be allocated on a pay-per use basis for drivers who choose to pay money for the improved journey times that come with charged access.[16] There are also many systems overtly designed for surveillance of movement and activity through technological substitutes for the person. Drivers of Heavy Goods Vehicles (HGVs), for example, have for several years had tachographs installed in their cabs, which monitor the number of miles driven, as well as speed, hours at the wheel, and increasingly geographical position, through GPS. These are primarily designed for safety reasons (to prevent accidents caused by drivers falling asleep at the wheel). Automatic Number-Plate Recognition (ANPR), in operation since the early 1990s around the City of London following IRA attacks, and earlier

[11] Phillips, P. et al (2002), *Face Recognition Vendor Test, 2002: Overview and Summary*, Biometric Institute. See: Introna, L. and Wood, D. (2004), "Picturing algorithmic surveillance: The politics of facial recognition systems," *Surveillance and Society*, 2, 177-198; Gray, M. (2003), "Urban surveillance and panopticism: Will we recognize the facial recognition society?" *Surveillance and Society,* 1, 314-33.

[12] Gates, K. (2004), *The Past Perfect Promise of Facial Recognition Technology*, ACDIS Occasional Paper, University of Illinois at Urbana-Champaign.

[13] Velastin, S. et al. (2005) PRISMATICA: Towards Ambient Intelligence in Public Transport Environments, IEEE Transactions on Man, Systems and Cybernetics – Part A: Systems and Humans 35(1): 164-182. Online: http://ieeexplore.ieee.org/iel5/3468/29969/01369353.pdf?isnumber=&arnumber=1369353

[14] Hogan, J. (2003) Smart software linked to CCTV can spot dubious behaviour, *New Scientist*, 11 July. http://www.newscientist.com/article.ns?id=dn3918 (accessed 31 July 2006)

[15] SNX1302 brochure, Ipsotek website http://www.ipsotek.com/download/SNX1302-200brochure.pdf (accessed 31 July 2006)

[16] See Graham, S. and Marvin, S. (2001), *Splintering Urbanism,* Routledge: London

in Japan and Singapore, relies on CCTV cameras to take pictures of vehicles license plates, optically read the registration and compare it a database, to detect uninsured vehicles, people wanted in connection with particular crimes and so on. However, the London congestion charge, which commenced in 2003, and the Birmingham Northern relied road, both now use ANPR as a method of charging for road use. In the UK, ANPR will be national by 2008, which coincides with plans for national congestion charging, and the UK and EU Governments are exploring the possibility of using GPS navigation systems to charge for all road use everywhere within UK and EU space.[17]

There are major concerns here that the comprehensive electronic movement records inevitably generated by such systems will be used as a social tracking system and that function creep will occur through which law enforcement and security agencies will gain access to tracking records. Already, the London congestion toll system has been enrolled as part of an anti-terrorist initiative proactively searching for suspect and stolen cars. In a similar development, the tracking databases generated by the new 'Oyster' smart card, used by 5 million Londoners to access London's public transport system, are now regularly accessed by the Metropolitan Police for criminal investigations. However, the story of ANPR also shows that function creep works both ways: a technology developed for security reasons develops a role in both traffic management and commercial revenue raising.

- *Automated Telecommunications Interception:* In theory, police 'telephone tapping' – the monitoring of individual phone lines – requires a court order, and many such operations are authorised against targets suspected of particular crimes. However, states also routinely filter vast amounts of telephone, telex, e-mail and fax traffic for reasons of 'national interests' (both security and economic interests) without the knowledge of those whose communications are being intercepted. In this context the so-called 'ECHELON' system, a global surveillance network based in the UK, at the American National Security Agency base at Menwith Hill in North Yorkshire, routinely automatically filters all communications passing thorough the UK for key words and phrases and increasingly employs more sophisticated algorithms for advanced speech and even meaning recognition[18]. Whilst some protections exist in the USA, to protect US citizens from unwarranted intrusion (even for national security reasons), no such rights exist in Britain.

- *Differential Call Centre Queuing* : Following widespread practice in the USA, UK based call centres now routinely use software programmes known as Customer Relations Management (CRM) systems to queue incoming calls differently based on sensing the numbers of incoming calls. This is done by linking to customer databases. Automatic judgements are then made about the quality, worth, or profitability of calling customers. This allows service providers to concentrate on the most profitable 'premium' customers, who are given tailored services, individual attention, and the best promotions and deals. Meanwhile, people from more marginalised backgrounds, called "pond life" recently by one call centre IT executive,[19] are forced to wait longer periods for inferior or automated service. "It's all about finding out who the customer

[17] Grayling, T., Samson, N., and Foley, J. (2004), *In the Fast Lane; Fair and Effective Road User Charging in Britain*, Institute for Public Policy Research: London.

[18] Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: the state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition (AKA Interception Capabilities 2000)*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme; Wood, D (2001) The Hidden Geography of Transnational Surveillance, Unpublished PhD Thesis, University of Newcastle, UK.

[19] Booth, N. (2006), "Press 1 if you're poor, 2 if you're loaded...", *Technology Guardian*, March 2nd, pp.3.; Bibby, A. (2006), "Left hanging on the line as call centres target wealthy", *Daily Mail Online,* www.dailymail.co.uk , 23rd April.

is, and putting then in the correct bucket", explains Ian Davis, a customer relations manager at the IT company ATG. This way, "the unprofitable customers never hear about the discounts and promotions".[20] Thus, different service packages, prices and promotions -- even for previously nationally standard services or products like rail fares -- can be offered to different individuals, organisations and even localities with different prices or conditions.

This process is known as the 'unbundling' of aggregated prices. Normally, this practice is based on real-time surveillance of demand, income, the time of purchase, and the characteristics of customers. It is familiar to anyone using a web site to book an air ticket with a cheap airline. Such unbundling allows users to be given very different experiences of a single call centre. The US phone company Orange, for example, allows immediate access to a human being only to those users who sign up for a premium 'panther' service. The Virgin call centre, *thetrainline.com*, meanwhile, deters first time callers with lengthy interactive voice response menus whilst prioritising regular, business, train users for tailored, human, support.[21]

- *A Two-Tier , Software-Sorted Internet:* Similar 'unbundling' techniques are also now being used to sort the flows of electronic traffic on the Internet. Originally developed to accord all the 'packets' of information that flowed within it equal status, the Internet was originally configured by the so-called 'best effort' model of switching packets of information. Here, equal effort was made to allow all packets to flow to desired destinations at all times. Now, however, complex surveillance techniques are being used to sift and prioritise each of the billions of data packets that flow over the 'Net at any one time. The world's biggest manufacturer of Internet routers, Cisco,[22] for example, now sift packet flows on the Internet to allow them to offer premium internet services to what they call the "transactional/interactive data class" of users. At the same time, the electronic mobilities of what they term the "scavenger class" are actively *impeded* based on the software-sorting of every single Internet packet. "The Scavenger class [categorisation] is intended to provide differential services, or 'less-than-Best-Effort"' services, to certain applications", Cisco suggests.

  Plans to charge a 'congestion charge' to low grade Internet users, announced by the US telecommunications group AT&T in July 2006,[23] look set to exacerbate the reconfiguration and 'unbundling' of the Internet into two-tier systems which works to reinforce social and economic gaps between privileged and marginal users and places though the sorting of packets flows. There is also heavy pressure now from corporations and the US state to change the nature of the Internet entirely to remove what is known as 'Net Neutrality' to further facilitate differential flow of information based on perceived importance and value of consumers.

From Uniforms to RFID: the Pervasive Surveillance Revolution

The rapid diffusion of tiny Radio Frequency Identification (RFID) chips raises a third series of key challenges to the regulation of geographical surveillance.[24] Here, computers literally blur invisibly into the background of the material city, underpinning new 'smart' means of continually tracking goods and people wirelessly as they move across geographic environments. They facilitate a continual assembly of tracking data and the emergence of city environments which are continually 'aware' of who and what is moving around within them, along with their previous associations, consumption habits and movements.

[20] Cited in Bibby (2006) op cit. n.19

[21] Ibid.

[22] Cisco (2002): *Service provider quality of service -- Design guid*e, Washington DC: Cisco Inc.

[23] Smith, D. (2006), "Internet users face congestion charge", *The Observer,* 2nd July, pp. 14.

[24] Kang, J. and Cuff, D. (2005), *Pervasive Computing: Embedded in the Public Sphere,* available from dcuff@ucla.edu. Cuff, D. 2002: Immanent domain: Pervasive computing and the public realm, *Journal of Architectural Education*, 57, 43-49.

Such direct intervention to make a person, animal or thing more surveillable has a long history. Farmers have long used branding or marking to identify their animals. Ecologists have tagged animals to monitor populations. And states and institutions have been using such systems for many years, most notably in having prisoners, soldiers and others wear particular recognisable clothes (uniforms), and, in extreme cases such as Nazi Germany, in wearing signs of categories like the yellow star for Jews worn on clothes, and the tattooing of concentration camp inmate numbers on the skin.

All of these examples of surveillance through tagging and tracking require some form of direct visual monitoring to confirm identity or track movement. However, developments in electronics and computing have allowed more sophisticated tags and markers to be produced which do not need such constant and direct confirmation. These developments were based around the increasing portability and small size of devices that can emit radio waves or communicate with satellites. Electronic tags, usually worn around the ankle and designed not to be able to be removed without authorization, have been worn by offenders and those on bail in the USA since the 1980s, after they were suggested by a Texas judge. They have also become increasingly common in the UK for those on supervision orders or with Anti-Social Behaviour Orders or other restrictions that tie them to a particular area (sometimes as limited as an individual house) for all or some hours of the day. The tags used within the British probation system communicate either constantly or at regular intervals with a receiver which can transmit the information to a monitoring station, either centrally or on a portable device carried by a monitoring officer. It is increasingly the case that such tags are linked to GPS rather than simple radio monitoring systems, increasing accuracy and allowing much more flexible supervisory conditions to be imposed.[25]

RFID chips emit a limited range radio signal that can be picked up by receivers usually within a few centimetres. Until recently their use has been restricted to large shipping containers (ports being a major area of vulnerability to smuggling, illegal immigration and terrorist attack, but very difficult to police effectively by traditional methods), as well as consumer goods. However, recently, a notable change has occurred: the implantation of RFID chips into living beings. Race horses and pets were the first groups to be targeted in this way. For pets, RFID chips containing information about immunisation records and ownership have gradually replaced quarantine requirements in the EU since February 2000 through the PETS scheme, which has since been extended beyond Europe[26].

For humans, the first use of RFID chips has been in elderly people suffering from degenerative diseases in the United States, and around 70 people have now been implanted to enable carers to locate them easily and prevent them from wandering and possibly endangering themselves[27]. Researchers and technological enthusiasts have also been implanting themselves with chips for several years now in order to be able to automatically performs small household tasks (turning lights on and off etc.)[28] At least one chain of Spanish nightclub has offered patrons the chance to have cash and access privileges held on implanted chips[29].

[25] For more on tagging see the work of Mike Nellis, e.g.: Nellis, M. (2005) 'The electronic monitoring of offenders in England and Wales: a critical overview,' in Hucklesby, A. and Mair, G. *Issues in Community and Criminal Justice – Monograph 5*, London: National Association of Probation Officers.

[26] For details, see the Department of Environment, Food and Rural Affairs (DEFRA) PETS website: http://www.defra.gov.uk/animalh/quarantine/pets/index.htm (accessed 31 July 2006)

[27] The company involved is Verichip Corporation. http://www.verichipcorp.com/ (accessed 31 July 2006)

[28] Amal Graafstra is one such high profile enthusiast and advocate of self-chipping. Explanations, pictures and videos can be downloaded from his website http://amal.net/rfid.html (accessed 31 July 2006)

[29] Graham-Rowe, D. (2004) 'Clubbers chose chip implants to jump queues', *New Scientist*, 21 May,. Online. http://www.newscientist.com/article.ns?id=dn5022 (accessed 31 July 2006)

A further step-change in RFID application occurred in February 2006 when a security company on Ohio, USA, implanted two of its workers with RFID chips to allow them to access company property[30]. Although such an invasive procedure was carried out voluntarily, it raises enormous questions about the integrity of the body and privacy in relation to employers. It is also not entirely surprising that the call for everyone to be implanted is now being seriously debated on some technology websites.

RFID and pervasive computing technologies raise a host of crucial questions for Privacy and Information Regulators.[31] For example:

- How can principles of transparency and accountability be implemented when cities, streets, rooms and infrastructures literally become sentient and continually and covertly track who and what goes on within them, or when human bodies, or their RFID identifiers, are subject to continual, covert, tracking and scrutiny?
- How can the principle of the free mixing of people within the public realm in cities be maintained when those managing malls and increasingly privatised public spaces, for example, might soon have the possibility of identifying each individual who enters their realm covertly and automatically, as well as their tastes, wealth, habits, associations and potential profitability?
- How can regulators respond to the dangers that such operators will use RFID to continually link with profiling databases to sort users, offering incentives, extra services and benefits to these deemed most desirable whilst attempting to remove or discourage those deemed to be problematic, unprofitable, or “irregular” in some way?
- What issues for privacy, accountability and social exclusion are raised by the use of tagging to further unbundle previously standardised price or service structures? With Amazon.com already shown to be selling DVDs to different customers at different prices, is regulatory intervention necessary to ensure that mass commercial price-fixing does not emerge based on the operation of automated RFID surveillance?
- How can the covert scanning of people’s houses, consumption habits, associations and private realms for consumption data be best regulated and how can the use of such data to identify ‘risky’ individuals be controlled ?
- How, in short, can freedom of movement and assembly in cities be protected in a world of ubiquitous and continuous tracking where such technologies are being widely invested with the power to improve security and fight terrorism?[32] The clear danger here, given such a context, is that pervasive computing and RFID revolutions will work, as Kang and Cuff put it, to “chill [the] irregular, deviant or unpopular speech and actions”[33] that, in the long term, are essential to the maintenance of a democratic urban society.

Challenges to Regulation

The regulatory environment within software-sorted societies is becoming ever more complex and challenging. The shift towards automated and digital surveillance systems, embedded into the urban background, which reduce or remove the discretion of supervising human beings, is the main regulatory challenge here. The fortunes, opportunities and constraints facing individuals and places are increasingly being shaped by tracking, profiling and surveillance technologies which are literally being ‘designed in’ to the fabric of cities and infrastructures.

[30] Waters, R. (2006) ‘US group implants electronic tags in workers’, *Financial Times*, 12 February. Online: http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html (accessed 31 July 2006)

[31] See Kang, J. and Cuff, D. (2005), *Pervasive Computing: Embedded in the Public Sphere*, available from dcuff@ucla.edu.

[32] See International Telecommunications Union (ITU) (2005), *Ubiquitous Network Societies: The Case of Radio Frequency Identification,* ITU; ,Document UNS/04/

[33] Kang and Cuff (2005) op cit. n.31: 33.

These use automated judgements, based on surveillance linked to databases, to automatically prioritise certain people's' interests at the direct expense of others.

The challenge that software-sorted cities and infrastructures present to Information Commissioners and Privacy Regulators is made especially complex because of two factors.

First, it is extremely difficult to penetrate the computer code that acts as the agent and power-broker in software-sorting systems. Where, after all, is such code located in the strung-out international data flows which characterise globalising societies? Who stipulates the parts of the software code which decides whose traffic or access in Internet, call centre, migration, road pricing, face-recognition CCTV, or RFID systems is warranted, legitimate or speeded up, and whose is blocked, slowed down, excluded, or subject to the extra scrutiny or sanction? Can such powerful decisions ever be made transparent or open to the challenge of regulators when often even the effects of such decisions are invisible from the point of view of those who's rights are strengthened or weakened in the process? Who shapes the code that stipulates the behaviours, facial appearances or even walking styles that are deemed deviant, abnormal, irregular, or characteristic of a 'target' for video surveillance on a city street? How can the simple use of prejudice and social profiling to shape such decisions be prevented? And how can regulators bring the operators of such systems to account when, by definition, they tend to straddle the national jurisdictions that information commissioners and privacy regulators are forced to work within?

Second, there is a major current tendency towards the increasing interoperability of software-sorting systems. Thus, the kinds of 'smart' ID cards being discussed by many Western nations, which store biometric signatures and can even be equipped with RFID tags, might potentially act as a portal connecting a widely distributed set of databases encompassing such issues as social security, immigration, health, security, work, taxation, consumption, neighbourhood, and so on. Such interoperability and integration brings the spectre of function creep in geographically-based surveillance systems, and such creep works in many different directions. Thus, for example, London's ANPR cameras moved from being part of an anti-terrorist system (initially around the City of London), to being incorporated into an expanded network of congestion charge cameras (around the whole centre of London), to moving the whole expanded network back to civil disorder and anti-terrorist functions. With many surveillance systems increasingly becoming automated and driven by software-sorted databases, it becomes much easier to organise such interoperability and function creep. And with increasingly blurred boundaries between state and private sector interests, as more and more tasks of government are carried out by Public-Private Partnerships or private sector consortia, and where state information is available for sale (as has been suggested with the National Identity Database), concerns have to be raised about the limits to the consent of people as citizens and as consumers, and where those boundaries lie.

Despite these difficult challenges, this report, drawing on recent examples of progress in this area,[34] recommends that Information Commissioners and Privacy Regulators undertake a series of major regulatory reviews into the emergence, functioning and regulation of software-sorted surveillance systems. Such reviews should particularly emphasise the ways in which such systems are being used to radically reorganise cities and infrastructures.

These reviews need to focus on three particular challenges:

1. *Privacy Audits:* Introducing a system of *Privacy Audits* on all software-sorted and geographical surveillance systems to ensure that such systems:

[34] Cavoukian, A. (2004), *Tag, You're It; Privacy Implications of Radio Frequency Identification (RFID) Technology*, Ontario Information and Privacy Commissioner., Toronto; Friedewald, M. et al (2005), *Safeguards in a world of ambient intelligence (SWAMI): Scenario and Legal Framework*, SWAMI Project, available a http://swami.jrc.es; International telecommunications union (ITU) (2005), Privacy and Ubiquitous Network societies, Document UNS/05/

- Are designed and operated to respect informational privacy,
- Offer subjects some transparency in understanding how and why they are surveilled,
- Offer an acceptable level of transparency, accountability, and Freedom of Information; and
- Are based on the principle that open access to cities and their infrastructures should be maintained wherever possible, within the constraints imposed by the operation of markets for goods and services.[35]

2. *Social Exclusion Audits*: Working with relevant social policy makers, Information Commissioners and Privacy Regulators should audit software-sorted surveillance systems in digital CCTV, 'smart' urban infrastructure and pervasive computing identify in detail whether such systems:

   - Are being used to automate processes of social and geographical exclusion; or
   - Are introducing interoperable software to underpin systematic social and geographical tracking for the purposes of social control, data generation or the development of commercial information products.

   Here, computer code itself needs to be utilised as a regulatory and auditing mechanism, to surveil the processes of social-sorting through which contemporary processes of surveillance work.[36]

3. *A Robust Regulatory System*: Explore the introduction of a robust programme of penalties, fines and legal sanctions to be applied when software-sorted surveillance systems are demonstrated to have undermined or transgressed the above sets of principles.

[35] Kang and Cuff (2005) op cit. n.31

[36] Shaha, R. and Kesan, J. (2005), "Manipulating code; how society can utilize code as a regulatory mechanism". Available from rshaha4@uiuc.edu.

Expert Report: Medicine

Ann Rudinow Saetnan
Norwegian University of Science and Technology, Trondheim
ann.r.saetnan@svt.ntnu.no

Introduction

This report begins by looking at medical surveillance issues –diagnosis and monitoring of disease in individual patients, population-wide screening programs, and the registration of diagnoses in population-wide databases. The report discusses how diagnostic technologies are, traditionally and normatively, tested within medical science. It then goes on to discuss some ethical and social issues that medical technology assessment (MTA) does not adequately address. Finally, the report discusses situations where medical technologies are used in forensic surveillance.

Why this final move from medical to forensic surveillance? Disease and crime have quite a bit in common. Both are, in sociological terms, forms of deviance[165]. Both can be caused by and causes of poverty. Each has, at times, been seen as a possible cause of the other, as when disease is seen as divine punishment for sin or when certain criminalized behaviours are seen as manifestations of disease. And both are seen as potential threats to public as well as individual interests, therefore both are subjects of surveillance – sometimes (and most important for this report) using the same techniques and technologies. This report discusses medical surveillance technologies, first in a public health context, then in contexts where the same or similar technologies are applied to security and/or criminal justice surveillance.

Medical surveillance of public health

Medical surveillance for public health purposes takes three main forms:

- **Monitoring and tracking** individual disease cases. For the individual patient this may serve to insure patient compliance with a treatment regime as well as to repeatedly evaluate and adjust that regime. In a perspective broader than the individual patient's interests, tracking and monitoring is used to identify sources of infection and/or genetic risk, and to identify and alert potentially infected individuals who have been in contact with a person carrying a disease (e.g. tracking all the contacts of someone diagnosed with tuberculosis) or affected relatives bearing the same genetic risk (e.g. offering genetic testing and counselling to relatives of persons diagnosed with Huntington's Disease).
- **Recording** occurrences of disease for statistical analysis (e.g. identifying cancer clusters by analysing data in a cancer register).
- **Screening** whole (sub-)populations to identify unaffected carriers of a disease, affected individuals who have not yet recognized symptoms of a disease, and individuals or groups at higher than average risk of a disease (e.g. mass screenings for high blood pressure, or routine mammography for early identification of breast cancer).

[165] In the interests of brevity, the report does not go in any depth into discussion or literature review on the sociological concept of deviance: how deviance is constructed through social interactions, its potential functions in defining and maintaining "normal" social structures, its potential as a source of social change, and so on. Suffice it to say that deviance is thought to serve a number of functions towards the preservation of "normal" society. If so, then the complete elimination of deviance is not an achievable or even desirable goal.

Each of these strategies can be pursued using any of a vast repertoire of diagnostic technologies, and new diagnostic technologies are continually being developed. However, though the details of the answers will vary from technology to technology and from one social historical context to another, the social, legal, and ethical questions faced when applying any technology via these strategies remain the same:

- How accurate is the diagnosis?
- What benefit (physical, psychological, social) is the patient likely to have from knowing the diagnosis?
- What benefit accrues to others? To society as a whole?
- What harm might the patient receive from the technologies used to arrive at the diagnosis?
- What harm (including not only physical or psychological harm, but also social harms such as stigmatisation, loss of dignity, loss of autonomy, economic losses) might the patient receive from knowing the diagnosis, or from others knowing the diagnosis?
- Has the patient consented to the diagnostic procedures, and what information does the patient have as a basis for that consent?
-

What might strike some as counterintuitive is that **as we move from individual diagnosis towards increasingly broad surveillance**, not only does the balance of benefits shift from the individual to society and possibilities for (especially social) harms to the individual increase, but **the accuracy of diagnosis decreases dramatically**. Since the overall possibility of benefit -- to the individual patient and to society at large -- hinges on the accuracy of diagnosis, we will focus first on this aspect.

Diagnosing disease – some social, legal, and ethical questions

Typically, the diagnosis process begins when a patient, suffering from some symptom or symptoms of disease, approaches a doctor[166] with a request for diagnosis and treatment. As is the case for all data, symptoms are interpretatively flexible. In this context, a symptom or symptoms may indicate any number of diseases (including those as yet undefined by medical science). A patient may also have multiple diseases and any given symptom may be attributable to one or several of these or to some interaction amongst them. Thus diagnosing is a complex process and any given diagnosis is always tentative, subject to revision – even after a patient's death. As long as the patient remains alive and in need of treatment, the diagnosis serves as a working hypothesis. In parallel with treating the disease according to that hypothesis, a good doctor is also continually considering alternative hypotheses. This entails multiple and repeated tests (symptom queries, bodily performances and examinations, physiochemical analyses of tissue samples, images based on translations of physical or physiochemical properties of tissues) that might help the doctor discriminate amongst potential diagnoses. However, each additional test adds complexity to the diagnostic process, for although tests may render one or more hypotheses improbable, few potential diagnoses can be entirely excluded no matter how many tests are performed.

When asked how they arrive at a diagnosis through all this complexity, doctors will often cite Occam's razor[167] as a guideline. In this context, Occam's razor is interpreted to mean that the

[166] Prior to approaching a doctor for diagnosis and/or treatment, many – perhaps most – patients will have spent some effort at self-diagnosis and will have consulted relatives and/or friends. In particular, wives and mothers tend to be used as "first diagnosticians". See for example the findings of Boneham & Sixsmith (1982). However, as data collected for surveillance purposes originates with a doctor's diagnosis, we will skip over these initial lay consultations.

[167] Occam's razor (also spelled Ockham's razor) is a principle attributed to the 14th-century English logician William of Ockham. In general terms the principle states that the explanation of any phenomenon should make as few assumptions as possible, eliminating, or "shaving off", those that make no difference in the observable predictions of the explanatory hypothesis. In medicine, the principle is understood to recommend that when diagnosing a given injury, ailment, illness, or disease a doctor should strive to look for the fewest possible causes that will account for all the symptoms. If followed strictly, Occam's razor is likely to lead to error. For instance, it is more likely for a patient to have several common diseases, rather than having a single rarer disease which explains all their myriad of symptoms. Therefore, a variant of Occam's Razor typically taught to medical students learning how to make diagnoses, is the expression, "When you hear hoofbeats, think horses not zebras." This is to impress upon the future doctors that the more common ailment is the most likely. The actual process that occurs when diagnosing a patient is a continuous flow of hypothesis and testing of that hypothesis, then modifying the hypothesis and so on. At no stage can a diagnosis properly be made or excluded because it does or doesn't immediately appear to fit the principles of Occam's razor. The

diagnosis that offers the simplest explanation of the most symptoms and test results is probably the right one. However, other guidelines are also applied to the task and may point to different conclusions. For instance, doctors will often begin with the most likely diagnosis -- e.g. the diagnosis most frequently associated with a given set of symptoms and test results, a diagnosis previous doctors have recorded in the patient's journal, or a diagnosis currently common in the local population (such as influenza during an epidemic). Similarly, they may tend to postpone considering diagnoses that are rare in the local population or diagnoses previous doctors have rejected for the patient. At other times they may begin by attempting to eliminate or treat the most serious diagnosis, i.e. the diagnosis it would be most damaging to the patient if they miss or arrive at too late. Or they may postpone confronting a diagnosis that offers dim prospects for treatment. These approaches may not point in the same direction, and – like the individual tests used in the process – none of them are "foolproof".

In addition to considering the possibility of error, the doctor must also bear in mind other social, legal, and ethical issues. Among these are:

- The probability and seriousness of harm vs. the possibility and degree of benefit from any given test, diagnosis, or treatment.
- The probability and degree of relief from disease the patient can expect.
- The patient's autonomy, dignity, and right to privacy.
- The patient's right to know
- The patient's right NOT to know
- The public interest

The order of issues in this list is not arbitrary. Doctors are, as a general rule, sworn to ethical principles demanding that they protect their patient's individual interests, and especially their safety, before the interests of other individuals, groups, or even society at large.

Because the overall process is so complex, because none of the tests involved are absolutely certain, because none of the tests involved can be said with certainty to be absolutely safe, because of historical abuses of diagnostic and treatment procedures … because of all these things, and because the medical profession identifies itself with the natural sciences, medical science has developed a standard for testing tests and treatments and for evaluating the outcomes of those tests (to avoid further confusion, let's call these tests of tests "trials"). This evaluation standard is not unequivocal either: The trials are not always practicable, or well understood. Nor do they settle all disputes, even when the standards for them are closely followed. However, even when standards are only loosely followed, the trials do provide valuable input for public discussions of the potential harms and benefits of the diagnostic and treatment technologies

Testing medical diagnostic technologies

Western medicine, though it claims to be based in science, applies many technologies and treatments that remain untested. In recent years, however, the sub-field of epidemiology has gained influence[168]. Standards have been set, as witness the publication of numerous handbooks[169] all laying out the same basic methodological principles and concepts for evaluating new medical technologies. This is not to say that these standards are always followed, but they are nevertheless sanctioned as the norm. For instance, numerous review articles are published that score medical technology assessment (MTA) studies according to how well they adhere to standards for study design and reporting[170].

principle of Occam's razor does not demand that the diagnostician necessarily opt for the simplest explanation, but instead guides the medical practitioner to seek explanations, without unnecessary additional assumptions, which are capable of accounting for all relevant evidence. And of course, a doctor may opt to toss Occam's razor overboard entirely. "Hickam's dictum" is a modern counterargument to the use of Occam's razor in the medical profession. Put succinctly it states: "Patients can have as many diseases as they like!". (source: http://en.wikipedia.org/wiki/Occam's_Razor#Medicine)

[168] See for instance Ashmore, Mulkay & Pinch (1989) on the rise to power of health economics, a field that extensively applies techniques and results from epidemiology to the assessment of medical technologies.

[169] E.g. INAHTA (2001), Kristensen, Hǿrder & Poulsen (2001), Fine (forthcoming 2006).

[170] e.g. Thacker (1985)

Trials of diagnostic technologies, are designed not only to test for safety, but also to fill a mathematical model for estimating the likelihood of diagnostic error and (conversely) the predictive value of a given diagnostic test outcome. One key element of this model is the incidence or prevalence[171] of the disease or condition targeted by the diagnostic technology. In a given population, how many true cases of the disease are there to be found? Of course, this number is always an estimate and a social construction. By "social construction" we do not mean that it is a fiction or an arbitrary invention. Rather, we emphasize that the interpretation of empirical evidence is a social process -- subject to negotiations and biases, dependent on available knowledge and technologies, and open to re-evaluations. For instance, many diseases represent outer points on some continuum of human variability. The number of cases in a given population will depend on the threshold values assigned as boundaries between the normal and the abnormal. Another problem is that in many cases, no "gold standard" exists for a diagnosis. Even if such a standard exists at a given moment in time, it is historically contingent and may eventually be replaced. Diagnosis depends on the diagnostic technologies in use. Applying a new technology may change the number of cases discovered in a population, leaving in question whether it is this new number, the former number, or some other number perhaps never to be discovered that represents the "true" incidence of the disease. Nevertheless, since there is often at least a temporary consensus on the incidence/prevalence of a disease, at a level of precision adequate for the model, this number is generally accepted as key.

The next two elements are the sensitivity and specificity of the technology in identifying cases. **Sensitivity** means the ability of the technology to correctly identify cases affected by the disease. **Specificity** (also called **selectivity**) means the technology's ability to correctly exclude cases not affected. Various trials are used to arrive at estimates of sensitivity and specificity, the highest valued of these being randomized, controlled, double-blinded, clinical trials with independent expert assessment of patient outcomes. However, methodologists freely admit that no trial is perfectly reproducible. Variable individual user skills, organizational settings, disease criteria, and epidemiological ecologies (e.g. populations with different prevalence levels for the targeted disease) will yield different sensitivity and specificity outcomes. Nevertheless, as is the case with incidence/prevalence, technology assessment studies do tend to arrive at a degree of consensus sufficient for further policy debates.

In fact, it is key to such policy debates that sensitivity and specificity tend to be "tunable" values, depending on how one chooses to set criteria for diagnosis. They are values that tend to trade off against one another. One can opt for high sensitivity by broadening the criteria for initial diagnosis, thus ensuring the inclusion of a maximum number of true positive cases, but at the cost of also subjecting many true negative cases to further diagnostics as (at least temporarily) false positives. Alternatively, one can attempt to avoid false positive cases by applying more restrictive criteria, but at the risk of missing more true positive cases. Ideally the issue of which way to tune depends on how we assess the consequences of missed diagnoses (false negatives) against the consequences of over-diagnoses (false positives). Oversimplifying relative to real world instances: Is it for instance fatal for the patient whose diagnosis is missed yet harmless to the patient who is treated in spite of not having the disease? Then we should opt for maximum sensitivity even at the cost of low specificity. However, if the treatment itself is dangerous and missed cases can be treated even if caught later, we should opt for high specificity even at the cost of low sensitivity.

In these debates, it is assumed that no test is perfect. Sensitivity and specificity are never 100%. That is to say that among all test positive cases, even if most are true positives, there will also be some false positives. Likewise, among all test negative cases, there will be some false negatives. This yields yet another set of values for policy discussion – the positive and negative predictive values of the test.

[171] "Prevalence" means the current number of people or percentage of a population who have the condition in question. "Incidence" means the annual number of people or percentage of a population contracting the condition. These may be quite different numbers for a given condition. For instance, the number of people diagnosed with diabetes in a given year (incidence) may be small, but since they live with the condition for the remainder of a fairly normal lifetime the prevalence of the disease (the sum of incidence rates minus those who have since died) is quite high. For the common cold, the reverse would be true: Many contract a cold in the course of a year, but fewer have a cold at any given time.

Positive predictive value is the percentage of true positives among all test positives, negative predictive value correspondingly the percentage of true negatives among all test negatives.

The predictive values of a test depend, of course, on the precision of the indicators on which the test is based. We generally do not observe the disease "itself", but some indicator(s) of its presence. Some indicators are more closely associated with a given disease than others. A bright line through the shadow of a bone on an x-ray would be a fairly reliable indicator of a fracture, although other (rarer?) explanations may still remain. However a high temperature on a thermometer, though a strong indicator of a fever, is only a weak indicator of any given underlying disease that might be the cause of that fever.

Before moving on to discuss the limits of MTA and then to compare with how forensic technologies are tested, let's just do a thought experiment to show how the entire model works. Let's say we are using an ultrasound scanner to look for Down's syndrome in foetuses. Let's say that 1 in 700 foetuses actually carry the condition, i.e. are true positives; the rest, 99.857…% of the population, are true negatives. And let's say we test 70 000 foetuses (just so as to estimate an even 100 true positives). Now suppose we have fairly precise set of indicators, so that sensitivity is 85% (a sensitivity reported by some, based on skilled ultrasound operators) and let's set specificity higher and say it's 98% (some reports show less, depending on the combinations of indicators applied and the skills of the operators applying them).[172] Now we can fill out the model in the form of a simple table and see what results we get.

Table 1. True and false positives and negatives given prevalence 1/700, sensitivity 85%, and specificity 98%.

	Test positive	Test negative	Total
True positive	85 true pos.	15 false neg.	100
True negative	1398 false pos.	68502 true neg.	69,900
Total	1483	68517	70,000

Positive predictive value = 85/1483 = 5.7%
Negative predictive value = 68502/68517 = 99.9%

Note that the negative predictive value is higher than the selectivity of the test, but the positive predictive value is only a small fraction of the sensitivity of the test. Only 5.7% of test positive cases are true positives, even with a sensitivity of 85% and specificity of 98%. However 99.9% of all negative results are true negatives. The high number (1398) of false positive results is due to the low prevalence of the condition being screened for in the population. Since the vast majority are true negatives, even the slightest inaccuracy in selectivity will yield large numbers of false positives. Even if we set specificity and sensitivity both at 99% (and I know of no tests as precise as that), we would still find more false positives than true positives; we would namely find 99 of the 100 true positives, and (at least initially) misidentify 699 of the true negatives as positive.

Already we can clearly see one of the consequences of "function creep" in medical surveillance: As a diagnostic technology "creeps" from individual diagnostics towards ever broader surveillance, it is applied to larger and larger proportions of the population. This inevitably means that it encounters ever lower prevalence of the disease(s) it is designed to diagnose. While prevalence may be fairly high among patients presenting with symptoms, prevalence in the general population is likely to be dramatically lower. And as prevalence falls so too does positive predictive value fall. A diagnostic technology that is a good predictor of disease when applied to a high-prevalence population may in a low-prevalence population still be a good tool for "acquitting" patients from possible disease, but will have become a very weak and misleading tool for positive diagnostics. The question is what the consequences are for those falsely identified. What routines are in place to control the initial

[172] These numbers were gleaned from the web site of Great Britain's Public Health Genetics Unit, last updated October 2004. http://www.phgu.org.uk/info_database/diseases/downs_syndrome/downs.html#I2

diagnosis? What actions are taken on the basis of the diagnosis once it is (perhaps mistakenly) taken as true?

Some shortcomings in the testing of medical diagnostic technologies

As you can see, this model for assessing medical technologies does not give us exact answers to these questions. What it does do is encourage and enable us to discuss them. However, there are limits to this encouragement, and especially limits to which follow-up questions get invited.

First, and most generally, the medical technology assessment model is based in a natural science paradigm that entails a determinist view of technology. "Technology determinism" refers to the view, or methodological implication, that technologies come from virtually nowhere, that they come to be invented simply because they work, because they accord with natural laws, or because they are among the natural conclusions of basic science research. Once invented, they simply are what they are. They have consequences due to the interaction of what they are and what the bodies are that they are applied to. These consequences can be found through natural science methodologies. And since natural science methodologies are designed to arrive at universal truths – i.e. at conclusions that are true regardless of when, where or by whom they are tested – the safety and effectiveness of these technologies are seen as testable, once and for all, in a time window tightly squeezed between the technology's invention and application.

Unfortunately, this whole chain of assumptions is easily refuted. Technologies do not come from nowhere. They are social products and reflect, in many ways, the social relationships involved in their production[173]. Furthermore, their consequences are social products. The effects of a technology are contingent on the cultural and organizational contexts within which the technology is applied and on the (many and variable) meanings associated with the technology[174]. The standard medical technology assessment paradigm does not address these issues adequately. Thus, the presentation of MTA results does not invite a discussion of them.

What MTA methodologies do attempt to achieve is to separate assessment from its social context. They attempt to limit the effects of interest-based bias. Obviously, a pharmaceutical firm, having invested millions in the development of a new medication or diagnostic test kit, has a vested interest in seeing their product approved for the broadest possible usage. This gives them an incentive to underreport untoward effects and exaggerate benefits. If norms for MTA are followed, this will to some extent discipline against yielding to such incentives. Since temptation has repeatedly trumped voluntary adherence to MTA norms, oversight agencies and disciplinary procedures have been created to enforce them. However, time and again we see instances where these biases slip through the seams of even the most tightly woven control systems[175].

However the separation of MTA from social context also exacerbates a weakness in MTA, namely that it tends to ignore social factors affecting disease, affecting diagnostic and/or treatment results, and affected by disease/diagnosis/treatment. Issues such as power, gender, relationships among professions, patient autonomy and dignity are not seen as irrelevant, but they are seen as messy, difficult to research, even unscientific. Medical researchers tend to apply what we might call a "usual suspects" technique for including social factors in MTA studies. That is, they tend to classify subjects in MTA trials according to a handful of factors one might see as social, e.g. sex, "race", "class"[176].

[173] For instance, in a recent article, Brown et al. (2006) discuss the many structural, political, ideological etc. reasons why breast cancer research has focused on individual risk factors, disease identification and treatment rather than on environmental factors and disease prevention.

[174] For instance, foetal diagnostics may lead to abortion of female foetuses and an overabundance of male infants in the context such as poverty and steep dowry demands in India. In another context, where focus is primarily on diagnosis of congenital diseases, population effects may be very different.

[175] For examples, see Collins & Pinch (2005)

[176] We place the concept "race" in scare quotes in order to distance ourselves from the notion that some variations in human form are normal, non-pathological, genetically inherited traits associated with a specific population that can otherwise characterized in terms of geographical association, nationality, ethnicity, or physical traits such as skin colour. This clustering of traits implies that human variations constitute biologically definable population groups, i.e. "races." To claim such a cluster exists is to claim that race is a biological phenomenon, i.e. to construct "race". Racializing, i.e. claiming the existence of race as a significant biological category, is not the same as discussing race as a

However, medical researchers do not discuss these factors as social, but handle them as biological categories. This is likely to contribute to the further entrenchment and legitimization of biases based on "race", sex, age, etc. while further delaying potential insights into social, economic and environmental causes of disease[177].

Furthermore, MTA norms limit trials to a narrow window between invention and application. The normatively best randomized controlled clinical trial (rct) models involve testing a new technology or treatment against the previously established technology or treatment and (where relevant) a placebo (a presumably harmless "treatment" with no physiological effects). Some (preferably large) number of patients are randomly assigned to each group, voluntarily kept "blind" as to which treatment they are being offered, and their respective treatments are then compared. However, once the new technology has become established as standard, it becomes unethical to withhold it (e.g. through random assignment to a placebo group) until and unless some more promising technology comes along. Thus it becomes difficult to re-test a technology in established usage – even though that technology may have been modified over time, even though it may not have been subjected to such trials when first introduced, or even though the original trials may later have been seen to be flawed.

This exacerbates problems with "function creep" (e.g. "off-label prescription" – the prescription of drugs or other treatments for indications for which they have not been tested or approved; or, as discussed above, the expansion of diagnostics from individual, symptom-based usage to population-wide screening). Once a drug or treatment has been approved – if even for only a single disease and among patients with a narrow range of specific indications – it is available on the market. What we then often see is a gradual expansion of indications for usage, many of them not subjected to testing. This may result in some welcome relief for patients for whom other options have proven unsuccessful. It may result in improved life chances for patients whose disease is diagnosed earlier than had they waited for symptoms to become compelling. It may also result in tragedy.

All of this makes the practice of medicine, and of MTA, a very risky business. Nor is "informed patient consent" a cure-all for the legal risks entailed. It is required, not least since the gross abuses of medical science ethics perpetrated in the name of "research" in WWII concentration camps. It is also a useful tool, not least as a challenge to the researcher to think through what information might be relevant and necessary for prospective patients as a basis for such consent. However, one can never reach a complete overview over all such relevant considerations.

Of course, all these considerations and cautions regarding testing carry over into the settings where medical diagnostic technologies are applied. And as previously stated, caution is especially needed when applying them to monitor the health of entire (sub-)populations. Consider for instance the case when "patients" (including some presumptively healthy individuals submitting to population-wide testing) are requested to release information into large research databases. Many may participate in the tests in the hopes of improving their immediate life chances, or out of more altruistic interests in benefiting medical knowledge and the health of mankind. But what potential pitfalls should they be informed of before making their decision? Do we know the prevalence of the disease(s) being tested for? Do we know the likelihood, and the possible consequences, of false positive results? How can we possibly envision all the potential usages one might make of these data over time? How can we envision whom they might affect, and therefore whose consent it might be appropriate to acquire? How can we envision all the potential invasions into personal privacy? Note, for instance, that privacy is not always well protected when data are presented in anonymyzed tables. Depending on the background data collected (remember here the "usual suspects" method often applied in medical research) whole categories may become stigmatized as at risk for certain diseases. This in turn may affect whole sub-populations' chances of employment or insurance.

socially constructed phenomenon. While doubts have been cast as to the existence of race as a biological phenomenon (Barkan (1992), Gates (1997)), there is no doubt that race still exists in cultural assumptions and practices, where it serves as a mechanism for distribution of social goods and burdens.

[177] For a thorough discussion of these issues as relates to foetal ultrasound screening, see Sætnan (2005).

One policy consequence of all these issues has often been the requirement that data collected for medical (including medical research) purposes only be used for the specific purpose for which it was originally acquired. Any new purpose then requires new information and a new signed consent form from each included patient. This is contested, however, by medical researchers who see this as an overly burdensome requirement that at the very least delays potentially widely beneficial research[178].

Cases in point: regulatory challenges where MTA strengths and weaknesses meet.
All in all, regulating medical technologies and medical surveillance practices can be extremely challenging. Here we will briefly discuss just a few instances where the above-mentioned strengths and weaknesses come together:

- DIY test kits

  More and more, diagnostic tests are being standardized and pre-packaged into kits, many of which are offered directly to (potential) patients. A quick browse at http://www.medibix.com/CompanySearch.jsp?cs_choice=c&clt_choice=t&treepath=16842&stype=i will give you an idea of just how many such kits are available, and for what range of conditions.

  In some cases, home test kits are clearly a boon. People diagnosed with chronic conditions requiring constant monitoring (diabetes is a classic instance) can regain independence and mobility by learning to test and treat themselves. However, other cases may lead to serious invasions of privacy, loss of independence, over-diagnosis, over-medication, etc.

  Do we want to encourage parents to test their teenage children for drug usage, pregnancy, etc.? Or employers to test their employees? Or teachers their students? How might the power relations in these situations limit tested individuals' possibilities to decline testing, or subsequent interventions based on test results? How well informed are these potential kit users as to the possibility of false positive test results? What actions are they likely to take based on test results? How confident are we that they would keep test results confidential? What expectations of confidentiality are already breached at the moment of testing?

  And what about self-testing, e.g. for blood alcohol levels, anthrax, cancer, cholesterol, herpes, HIV (just to mention of few of the kits available on-line[179]). Do we have adequate health service staffing to deal with all the false positives? Are medical personnel prepared to reassure such patients who present with a (possibly false) positive test result? Would people attempt to self-medicate? And what about false negative tests? How many might use their (possibly false) negative HIV test result as a license to have unprotected sex? Or a (possibly false) low blood alcohol result as a license to drive after drinking?

  These are just some of the potential pitfalls in this growing self-surveillance market. In the US, the Federal Drug Administration has published caveats to the public about the very tests they have approved for sale[180]. Is that an adequate means of communicating the risks involved to the potential users? What other forms of regulation might be called for, and when would regulation itself constitute an infringement of the public's privacy and autonomy?

- Handling privacy issues in mass data bases

[178] For a discussion of this see Mund (2005)

[179] Not all the kits listed on-line are marketed for home use, however the scope of the lists illustrates the scope of current possibilities for future home-use tests.

[180] http://www.fda.gov/fdac/features/2001/601_home.html

The Human Genome Project was heralded in with high hopes that new paradigms such as genetic diagnostics and pharmacogenetics[181] would give vast improvements in the effectiveness of medical treatments and at the same time create a whole new and rapidly growing branch of industry. Genes and genealogies became national resources. Citizens were urged to participate out of altruism (mankind's interest in new medical treatment options), nationalism (creation of new growth industries), and self-interest (ranging from genealogical insights to the hope of cures for life-threatening diseases). Potential bio-bank participants were offered standard forms of privacy protection: voluntary participation based on informed consent, promises of limited usage of bio-bank materials, promises that bio-bank research results would be presented anonymously in table form.

As the hype of quick solutions to serious health problems wears thin, it is time to re-evaluate the handling of privacy issues in bio-banks. After all, if privacy is a goal that we trade off against other interests, then the balance in that trade-off may be shifting as our optimism regarding genetics-based treatments fades.

What if the gene paradigm in medical research is not only a limited success, but also at the same time a misdirection of efforts? What if our efforts would have been better spent investigating ecological sources of disease and paths towards prevention? If so, then investments in bio-banks and genetics research represent sunk costs that may bog us down, delaying more productive lines of inquiry. Genetics research may also have taken us down paths we do not wish to pursue, such as the relegitimation of "race" as a biological category. In other words, any assessment of the balance between privacy protection and research promise – whether that assessment be made collectively or individually – may shift over time.

That balance may also shift as we gain experience with the privacy protection regulations that helped create it. Over the years we have seen instances where usage limits placed on bio-bank materials have been exceeded[182]. We have also seen new research agendas emerge, accompanied by debates as to whether informed consent can be presumed or must be re-acquired[183]. We have also seen conflicts over property issues: Who owns our biological materials, the genes therein, and the medical technologies derived from them[184]? Can I withdraw my materials from a bio-bank? Can I withdraw those of deceased relatives? Am I assured access to medical technologies developed on the basis of my bio-bank deposits? Have bio-bank materials been pirated, stolen, acquired and sold without "donor" permission?

Just as trust in monetary banking systems grows and fades so too may trust in bio-banking systems. Trust in bio-banks and their related genetic research agendas varies from country to country, a phenomenon attributed to historical experiences[185]. It may also come to vary according to emerging experiences with existing bio-bank systems.

[181] Pharmacogenetics is often presented as the individual choice or design of medications to mesh with patients' genetically determined susceptibilities and treatment responses. In practice, however, pharmacogenetics often takes the form of racialized prescribing, e.g. where some drugs are seen as appropriate for "blacks" and ineffective for "whites" without testing the for gene-medication matches at the individual level. See for instance Kahn (2005)

[182] For instance, in a weblog on security technology, "Steffo" writes: "Why not just collect DNA from everyone at birth?" - In response to the first post. A bit late but I live in Sweden. :-) In Sweden, almost every citizen, born 1975 or later, have provided a blood sample at birth. The sample is used to test for a genetic disease (PKU: Phenyle-Ketone-Uria). But it is also saved for future medical research in a database. The database does not contain any DNA-profiles, but the blood samples can easily be analysed. There is also identity data provided with each sample. The database is of course not intended for use in criminal investigation, it should only be used for research purposes. However, the temptation to use the database was to great for the police. In the high profile case of the murder of Anna Lindh (the Swedish secretary of foreign affairs) the database was used to identify the murderer. It was not difficult for the police to obtain the sample, they just requested it from the physician in charge of the database. No questions asked. This example illustrates the risks of storing this sort of information: broadening of what is considered acceptable use of the data. From research to criminal investigation. What is the next step? Give the data to insurance companies or to employers? Slowly the public gets accustomed to the new uses of DNA-profiles and privacy and personal integrity erodes." http://www.schneier.com/blog/archives/2005/09/the_beginnings.html

[183] Árnason (2004)

[184] Everett (2003), Pálsson & Rabinow (2001)

[185] Corbie-Smith et al. (2002)

All this points to a need for ongoing, or at least periodically recurring, discussions as to the reasons for participating in bio-banks and the protective rules needed to regulate them. Some comparisons indicate that it may be easier to establish local bio-banks based on locally accepted medical screening programs[186] than to establish nation-wide bio-banks as large-scale initiatives[187]. This may be because large-scale initiatives stimulate large-scale debates through which counter-arguments emerge and are considered. Frustrating as this is for many researchers, it may be a good thing for citizens. Thorough national debates appear to raise issues that need to be raised if participation is truly to be based on informed consent.

- Tracking new pandemics

For a time it appeared that the European tuberculosis (TB) pandemic, rampant from antiquity to the mid-20th century, had been conquered. Some have ascribed this victory to a combination of systematic (in some countries mandatory, population-wide) screening of the populace, contact tracking to identify individuals at risk through contact with diagnosed cases, vaccination, and effective treatments[188]. Others contest the success of this medical paradigm, claiming that improvements in nutrition, sanitary, and working conditions were due at least as much credit[189]. Whatever the reasons behind the success, some of the screening apparatus was dismantled once this success seemed achieved: It no longer made sense to carry the expense of the program or to expose the entire populace to repeated doses (however small) of radiation once the prevalence and virulence of the disease were under control[190].

Now with TB making a resurge, not least in connection with the new HIV pandemic, screening programs are again being proposed for entire populations or for specific population categories (e.g. immigrants, or health workers). Renewed proposals to screen make it again important to evaluate whether it was screening and treatment or other efforts that led to the respite from TB that Europe and North America have experienced. Should screening again be made mandatory? If so, should it be mandatory for all, or only for "high risk" groups? If the latter, how should "high risk" be defined – in terms of risk of contracting the disease and/or risk of spreading it further once contracted? In terms of risk of permanent health loss/death if not diagnosed and treated early, or in terms of the danger of health losses caused by diagnosis and treatment? In terms of risks of and from false negatives, or in terms of risks of and to false positives? And finally, if screening is reinstated, how are data and materials to be handled (i.e. what about the bio-bank issues discussed above)?

Testing forensic applications of medical technologies ...?

So far we have seen that Medical Technology Assessment (MTA) is a valuable but imperfect tool for evaluating and regulating medical surveillance technologies and practices. We now ask what happens when these same technologies "creep" further afield and are used for forensic purposes. A number of technologies used for medical diagnosis have also been applied to forensic purposes – DNA analysis of tissue fragments; analyses of bodily performances such as posture, gait, or facial expression; analyses body parts and images or imprints thereof (e.g. fingerprints, height, weight, bodily proportions). Many of these are now being proposed for surveillance purposes in the form of extensive databases against which identities can be checked. But have the technologies been tested for these contexts? What do we know of their sensitivities and specificities as tools of forensic identification? And what will be their positive and negative predictive values when confronting extremely low prevalences?

[186] Skolbekken et al. (2005)
[187] Salter & Jones (2005), Petersen (2005)
[188] http://en.wikipedia.org/wiki/Tuberculosis
[189] http://www.historieboka.no/o.o.i.s?id=852&fact_id=2381
[190] http://www.metrokc.gov/health/about/history/tb.htm

Forensic identification technologies tend to follow three parallel trajectories – forensic, archival, and diagnostic[191]. That is to say that they are used, or proposed, for three intertwined purposes – to link a suspect to a specific criminal act, to link a person to a criminal record, and to predict whether a given individual is likely to commit criminal acts in the future. All three functions have similarities to medical diagnostics. In medical diagnostics, a specific bodily trait is linked to a person as evidence of past, current or possible future disease. In forensics a person is identified via specific personal traits (e.g. fingerprints, or facial appearance, or DNA fragments) and linked to past, current or possible future criminal acts[192]. Furthermore, both medical and forensic diagnostic technologies lay claim to the adjective "scientific". But there are also differences. So far, no forensic technologies have had any demonstrable success as diagnostic tools, but that has not deterred enthusiasts from proposing and predicting that new technologies – or even old ones – will eventually achieve this goal.

Also so far, no forensic technologies have been subjected to the forms of assessment demanded for medical technologies[193], though the 1993 US Supreme Court decision in Daubert v. Merrell Dow may change that. In the Daubert decision, the US Supreme Court sets five criteria for a forensic technology to be deemed "scientific" – peer review and sound methodology, **a known error rate** [emphasis added], testable hypotheses, application outside of legal proceedings, and general acceptance. For most established forensic identification technologies (e.g. photography, anthropometrics[194], fingerprinting), general acceptance is the only one of these criteria consistently met. This reflects the history of forensic technology "assessment", which has been based in the adversarial format of the courts, where the test of acceptance is whether or not the technology convinces a jury of the defendant's peers, and where repeated such tests accumulate as precedence the weight of which dampens future adversarial attacks. Most of these technologies have been touted as absolute and infallible, with only repeated claims of infallibility and remarkable but spurious demonstrations being offered as proof[195]. Documented cases of misidentification have been discounted as due to dishonesty or incompetence on the part of the investigator, thus maintaining the image of the technology "itself" as "in principle" infallible[196] – a distinction epidemiologists resist in the assessment of medical technologies.

Only the newest forms of forensic identification technologies – e.g. DNA typing and facial recognition – have been submitted to testing that give us some basis for estimating error rates. And even then, the methodologies used for estimating error rates are less precise than those used for medical technologies. For facial recognition systems, tests have been performed in a collaborative program between system manufacturers and the US Department of Defense. This program – the Facial Recognition Vendor Tests (FRVT) – has evaluated system efficiency and effectiveness in experiments replicating three potential usages. In descending order of difficulty these are 1) confirmation of a presented identity (as when someone presents an employee ID at a workplace entrance), 2) identification within a database (as when a suspect is checked for prior convictions under aliases), and 3) watch lists (as when airline passengers are screened to prevent suspected terrorists from boarding). Of these, the watch list function bears the most similarity to screening for disease in a low-prevalence population. For this function the most recent published FRVT, FRVT 2002, shows true positive identification rates for systems tuned at 1% "false acceptance" (= 99% specificity) as reaching 74% indentification (=sensitivity) under ideal conditions, i.e. indoor lighting, recent photographs in the database, standardized angle of face to camera, small image database, etc.[197]. Positive identification rates are higher if higher false identification rates are allowed, e.g. by setting the system to show several near matches from the database, leaving further confirmation to the operator. It is apparent from FRVT texts that a 1% false identification rate is considered an acceptable error rate. The texts do

[191] Cole 2001: 305
[192] What Williams and Johnson (2005: 3) call "bio-surveillance" http://www.dur.ac.uk/p.j.johnson/EU_Interim_Report_2005.pdf
[193] Cole, op. cit.: 284
[194] Although some anthropometric techniques, such as phrenology, have long been abandoned, others (e.g. height, weight, shoe size, eye color) are still in use for forensic identification purposes.
[195] Cole, op. cit.: ch 7-8
[196] Ibid.: ch 11
[197] FRVT 2002, Introna and Wood 2004

not, however, take the next step of showing how 99% specificity and 74% sensitivity affect predictive values in a low prevalence population.

What about DNA? Most of us have been taught since our first school science classes that DNA defines us, determines what we look like, what diseases we are susceptible to, and even to some extent our personalities. Furthermore, since we see ourselves as unique, we tend to assume that DNA identifications too are unique and unerring. All these assumptions are wrong. The Human Genome Project[198] has found that there simply aren't enough genes, or enough variations in gene forms, for single-gene predictors to explain all that we culturally see as differences between individuals[199] – DNA does not define or determine our individuality, at least not in the simple way imagined by some. Furthermore, for forensic identification purposes, only a few small segments of the entire DNA string are tested and only series of repeated base pairs (called "stutters") within the so-called "junk" DNA[200] are shown in the so-called profile. It must therefore be assumed that two people, even two who are not identical twins, may by sheer chance share a DNA profile. Two people may indeed share a given marker (a sequence of fuzzy bar code-like stripes in the analysis printout), or even several markers. Probabilities for two or more persons sharing a given set of these markers have been estimated by multiplying the percentages of persons in worldwide samples carrying each of the markers. If one marker is estimated to be carried by 1% of the population worldwide, another by 0.5% and another by 0.1%, then the probability of a person carrying all three is estimated at 1% of 0.5% of 0.1% or one chance in 20,000,000. However, this assumes that each of these markers is inherited independently and that each is evenly distributed across the world's population. As Cole[201] puts it, "This [is] akin to assuming that the entire population of the Earth mated randomly." Furthermore, this estimate does not account for methodological errors, for errors caused by borderline cases (remember: the "bar codes" are fuzzy, which expands the room left for reader interpretation), etc. And finally, we have yet to see how even such slight errors in rates of sensitivity and specificity might impact on positive predictive values given the extremely low prevalences we would be looking at (e.g. of one specific murderer, or even of some hundreds or thousands of terrorists, in an immense population).

Suppose we applied medical technology assessment concepts and estimated the predictive values of positive and negative results from these tests? What might the numbers show?

Estimating predictive values of forensic technologies.

For facial recognition, the FRVT 2002 results give us almost enough information to fill in the model table and estimate the positive predictive value of a facial recognition identification under ideal conditions. The one factor we are missing is prevalence. This would vary with the specific circumstances we were seeking to address with the technology. Are we looking for terrorists at an airport? Then the prevalence is extremely low. Millions of people pass through airports daily and even on the infamous date 9/11/2001 only a dozen are now thought to have actually been terrorists. Furthermore, their images were not at that time on a watch list database. But just as a demonstration, let's create a fictional set of circumstances that would constitute an ideal situation for testing facial recognition. Suppose (just for mathematical convenience) that 100 convicts have gone AWOL from prison after a day's parole. Suppose we have recent pictures of them on file, and suppose we are quite sure that they are AWOL because they couldn't resist "extending" their parole to catch a Champions League soccer match the next day. That gives us time to set up video surveillance cameras at each entrance to the stadium, with facial recognition installed and only these 100 convicts' images in the database. Let's say the stadium has a capacity of 20,000 and all tickets have been sold (though some have been sold to "scalpers" and we assume the convicts have managed to buy last minute tickets from them). By carefully positioning the cameras at the entrances alongside TV screens showing pre-game programming so that most who enter will turn towards the cameras at about the same angle, we can achieve somewhere near maximum sensitivity and selectivity. The best FRVT results so far show 74% sensitivity when "tuned" for 99% specificity. Now we can fill in our table:

[198] http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml
[199] http://www.ornl.gov/sci/techresources/Human_Genome/faq/genenumber.shtml
[200] I.e. DNA segments not (yet?) known to code for functional proteins and thereby for observable traits.
[201] Cole, op. cit.: 298

Table 2. A scenario for facial recognition identification from a watch list of 100 escaped convicts presumed to be attending a soccer match amongst 20,000 spectators.

	Test positive	Test negative	Total
True positive	74 true pos.	26 false neg.	100
True negative	199 false pos.	19701 true neg.	19,900
Total	263	19727	20,000

Positive predictive value = 74/263 = 28.13%
Negative predictive value = 19701/19727 = 99.87%

The result of our experiment would be that 74 of the convicts would be caught at the stadium gates. Meanwhile, some 199 innocent spectators would be delayed at the gates before their identities were clarified. They might be embarrassed, irritated, maybe even miss seeing the first goal. And 26 of the convicts would slip through the net and catch the game, maybe also pick other spectators' pockets or steal a car from the parking lot, before getting caught. The consequences would not be dire either from the false positives or the false negatives, and we might find that facial recognition is a helpful technology to use under these circumstances.

Of course, this scenario still doesn't answer another question that would have been answered for a medical technology, assuming we had followed recommended procedures and used a randomized controlled clinical trial (RCT). With an RCT we would also be able to estimate how many of these convicts would have been caught simply by stationing a prison guard at each stadium entrance to watch for them, without the aid of video surveillance or facial recognition software. We also have to remember that this scenario represents nearly ideal conditions favouring the technology. What if we were to pose a more difficult scenario for the technology – a lower prevalence population, a larger database with less precise and/or older images, more drastic consequences of false positives and/or false negatives? What if we were looking at major airports for 1000 known or suspected Al Qaeda operatives whose images we had gleaned from grainy videos, some of them several years old, often filmed in bright desert sunshine (which creates sharp contrasts that tend to confuse the facial recognition software). Furthermore, in the videos most of these operatives were bearded, which hides many facial features. With the larger database and the poorer and older images, our sensitivity rate will fall. Let's be generous and say we would have 65% sensitivity. To increase sensitivity, we might be tempted to reduce selectivity, but let's show restraint and keep that at 99% for now.
Now we need some information about the total population we will be screening. Suppose we screen at 10 major gateway airports in Europe and the US. First of all, how many passengers would we be screening?

Table 3: Estimated numbers of passengers annually at 10 major gateway airports in Europe and the US.

Airport	Estimated annual passenger throughput*
London airport Heathrow	68 million
Frankfurt airport, Germany	48 million
Schiphol airport, Amsterdam	40 million
Paris Charles de Gaulle airport	35 million
Kastrup airport, Copenhagen	18 million
John F. Kennedy airport, New York	30 million
Newark Internation airport, New Jersey	30 million
Atlanta International airport, Georgia	80 million
Chicago O'Hare International airport	67 million
Los Angeles International airport	60 million
SUM for 10 major gateway airports	476 million passengers annually

* Years referenced vary depending on data availability. Source: A-Z world airport guide[202]

[202] http://www.azworldairports.com

With this number of passengers, it seems clear that some technological assistance to relieve and/or improve guards' surveillance activities might be useful. But what would the performance of facial recognition be in terms of false positives and negatives? And what would be the predictive value of a positive ID from the facial recognition system? Let's see what the table shows:

Table 3: Estimating predictive values with 65% sensitivity and 99% selectivity with a watch list of 1000 and a total population of 476 million.

	Test positive	Test negative	Total
True positive	650 true pos.	350 f. neg.	1000
True negative	4,759,990 false pos.	471,239,010 t. neg.	475,999,000
Total	4,760,640	471,239,360	476,000,000

Positive predictive value = 650/4,759,990 = 1.37%
Negative predictive value = 19701/19727 = 99.99%

Note the dramatic fall from sensitivity to positive predictive value. Even with a sensitivity estimate of 65% and a specificity held at 99%, the population is so immense and the prevalence of those we are seeking so low that the predictive value of a positive test result is only a little more than 1%. 98.63% of all those detained and subjected to further questioning due to an initial positive identification would turn out to be false positives. Imagine their righteous indignation even if all that these people suffered was embarrassment and delay and perhaps a lost flight. Imagine the consequences if the US were detaining (indefinitely) even a fraction of these people as "enemy combatants", or if police at Heathrow were following a shoot-to-kill policy towards suspected suicide bombers. Note too the rise in negative predictive value, which climbs to 99.999999+%. And yet, 350 terrorists would nevertheless slip through this net, with potentially catastrophic results. Deploying video surveillance with facial recognition is not a good response to this situation. At the very least, supplementary systems will be needed to confirm or disaffirm suspected identities.

When I was demonstrating facial recognition to members of the public, one woman used the opportunity to give an impromptu science lesson to her teenage son, who was less than impressed with the "match" we had found for him in our database of … not suspected terrorists, but movie and sports stars. "What would be a surer way of identifying people?" she asked him. "Fingerprints?" he suggested. "Or DNA," she replied. Well, what about DNA?

As mentioned above, DNA identification is not based on the entire DNA sequence, which might approach being unique for each individual. Rather, it is based on some number of segments of what, at least for now, is considered "junk DNA", i.e. stretches of DNA that are not (at least, not yet) known to code for any proteins or physiological processes or anatomical traits[203]. No claim is made that the sequences mapped are unique to an individual. Sensitivity and specificity values are simply not known. But even if the sensitivity and specificity of the technology were both 99.99%, the prevalence implied when seeking the identity of a single suspect is so low that the positive predictive value of the test dwindles drastically. Again, we will have to resort to a fictional scenario to show how this works:

Let's say that we have a suspect in a murder case. We have found some blood (or spit, or semen) at the crime scene that we are convinced must come from the murderer or an accomplice. This allows us to conduct a DNA test against samples from suspects. Let's say the forensic laboratory tells us that it is 99.99% certain that the evidence is a match to the sample from one such suspect[204]. There are, however, no witnesses to the murder and no personal ties between the suspect and the victim. If indeed this was a random encounter, then the population of alternative suspects is virtually limitless, but let's limit it to the adult population of the city where the murder occurred and let's say this is a fairly small

[203] The specific segments examined and the number of markers considered adequate for making an identification vary from country to country, laboratory to laboratory, and sometimes even from case to case (as when the number of markers found is simply deemed to be adequate, regardless of previous practice).

[204] Actual expert witnesses may use vaguer "figures" such as "in all probability" or "in my opinion", or extremely low approximate error probability figures such as "one in a billion", but are rarely asked to explain how they arrived at them.

city, giving us a suspect population of 200 000. With 99.99% certainty, the chances are only 1 in 10,000 that our one tested suspect who tested positive was in fact not the source of the evidence at the scene of the crime. Put another way, chances are 1 in 10,000 that some other person in the population, if tested, would have tested positive. Had we tested every adult citizen in the town, the model predicts that our results would have looked like this:

	Test positive	Test negative	Total
True positive	1 true pos.	. 0 false neg.	1
True negative	20 false pos.	199,979 true neg.	199,999
Total	21	199,979	200,000

Positive predictive value = 1/21 = 4.76%
Negative predictive value = 199,979/199,979 = 100%

In other words, a negative DNA test seems to be a near perfect tool for acquitting the innocent, but a positive DNA test should be met with far more scepticism than we see occurring in courts or in mass media.

Another issue is in what terms the evidence for a match is presented. Even when probabilities are stated mathematically, the statement can take different forms. Koehler (2001) has conducted a series of studies that illustrate this and its importance in court. Koehler used four different but equally mathematically correct ways of stating a 1:1000 (or conversely 99.99%) DNA match probability:

A. The probability that the suspect would match the blood drops if he were not the source is 0.1%
B. The frequency with which the suspect would match the blood drops if he were not the source is 1 in 1,000.
C. 0.1% of the people in Houston who are not the source would also match the blood drops.
D. 1 in 1,000 people in Houston who are not the source would also match the blood drops.

While the four statements are mathematically equivalent, they are psychologically different and have different effects on a jury. When a statistical match is presented as in statement A, juries tend to be convinced that the suspect's sample in fact matches the evidence. When the match is expressed as in statement D, the jury is far more likely to be skeptical of the match[205].

In fact, it is virtually impossible to state an accurate figure. For one thing, we do not have world-wide whole-population DNA databases from which to calculate accurate frequencies of the various marker patterns. Nor are we arguing that we necessarily should have such databases, as they would entail other serious ethical and methodological problems. Not least is the problem that sloughed off cells carrying our DNA can be practically anywhere in the world for any number of reasons, most of them perfectly innocent and some of them involving intentional false incrimination. If we are all registered in a DNA database, then we are all constantly in a virtual police line-up with staggering possibilities for false positive matches. Furthermore, even if we did have such databases, only in rare cases would we be able to define exactly what segments of the population constituted the relevant reference population of possible suspects.

No easy regulatory solutions

Given the complexity of the issues discussed above, it should now be clear that there are no easy regulatory solutions to the problems we confront when deciding how to use (or not use) medical surveillance technologies. Nevertheless, evaluation and regulation are clearly necessary.

[205] Koehler (2001:4-5)

The United States Centers for Disease Control (CDC) has proposed a framework for the evaluation of medical surveillance systems[206] (i.e. technologies and the practices surrounding them). They recommend that evaluation begin with a thorough description of the proposed system:

- Its specific purpose(s), since evaluation criteria may vary depending on whether a system is intended to e.g. target interventions or reassure the public.
- The stakeholders implicated by the system, including data providers, responsible operating agencies, individuals about whom data might be collected, and agencies responsible for interventions based on system results.
- Detailed description of all operational aspects of the system, including data sources, data flows, privacy and security protections, statistical analysis tools, etc.

System goals should then be elaborated in terms of outbreak detection criteria:

- Timeliness, in terms of a time scale showing onset of exposure – onset of symptoms – onset of registered behaviours (such as contacting a doctor) – and a time frame for when contagion, cure, disability or death might occur. System events (data capture, data processing, application of algorithms, generation of alerts, follow-up investigation, initiation of interventions) should then be marked along the same time scale.
- Validity: What demands are to be placed on precision aspects such as specificity, sensitivity, baseline estimates, accuracy of case reports, and so on?

From these detailed descriptions, one can then plan a validation methodology, including plans for re-validation and system modification as one gathers experience with the system.

In this report, we hope we have shown three additional aspects of system evaluation and regulation:

1. That sensitivity, specificity, prevalence, and positive and negative predictive values alone do not provide a complete picture of the effectiveness and acceptability of a surveillance system. Public trust and willingness to participate are vital. Furthermore, one should not (and hopefully cannot in the long run) command public trust and participation in a system that does not deserve such trust, that puts the public's interests in privacy, autonomy, and/or dignity at risk.

2. That evaluation and regulation should therefore be open processes in which the public is invited to participate.

3. That aspects such as sensitivity, specificity, prevalence, predictive values, and their relationships to issues of security, privacy, autonomy and dignity can be presented in ways the general public can understand.

References

Aftenposten (16.11.2005) (http://www.aftenposten.no/nyheter/iriks/oslo/article1150858.ece)

Árnason, Vilhjálmur (2004) "Coding and Consent: Moral Challenges of the Database Project in Iceland", Bioethics 18(1): 27-49.

Ashmore, Malcolm, Michael J. Mulkay & Trevor J. Pinch (1989) Health and Efficiency: A Sociology of Health Economics. Open University Press

Barkan, E. (1992). *The retreat of scientific racism: Changing concepts of race in Britain and the United States between the world wars*. New York: Cambridge University Press.

Beck (1986) *Risikogesellschaft - Auf dem Weg in eine andere Moderne*. Translated 1992 as: *Risk Society: Towards a New Modernity*. London: Sage

[206] CDC Working Group, 2004.

Blume, Stuart S. (1991) *Insight and industry : on the dynamics of technological change in medicine*, Cambridge, MA: MIT Press.

Boneham, MA and JA Sixsmith (1982) “The voices of older women in a disadvantaged community: issues of health and social capital”. Social Science and Medicine 62(2):269-79.

Bowker, Geoffrey C. and Susan Leigh Star (1999) *Sorting Things Out: Classification and its Consequences.*

Brown, Phil, Sabrina McCormick, Brian Mayer, Stephen Zavestoski, Rachel Morello-Frosch, Rebecca Gasior Altman and Laura Senier (2006) “’A Lab of Our Own’. Environmental Causation of Breast Cancer and Challenges to the Dominant Epidemiological Paradigm”. *Science, Technology, & Human Values*, 21(5): 499-536.

Cartwright, Lisa (1995) *Screening the Body: Tracing Medicine's Visual Culture*. Minneapolis and London: University of Minnesota Press.

CDC Working Group (2004) “Framework for Evaluating Public Health Surveillance Systems for Early Detection of Outbreaks”. http://www.cdc.gov/MMWR/preview/mmwrhtml./rr5305al.htm

Cole, S.A. (2001) *Suspect Identities*. Cambridge, MA: Harvard University Press.

Collins, Harry and Trevor Pinch (2005) *Dr. Golem: How to Think about Medicine.* Chicago: Chicago University Press

Corbie-Smith, Giselle, Stephen B. Thomas and Diane Marie M. St. George (2002) “Distrust, Race, and Research” Archives of Internal Medicine, Vol. 162: 2458-2463, and Vol. 163: 1068

Denmark (2005):
http://denmark.dk/portal/page?_pageid=374,610566&_dad=portal&_schema=PORTAL&ic_nextitemno=1&ic_itemid=882291
Complete text of White Paper in Danish: http://www.stm.dk/publikationer/terror/index.htm

Everett, Margaret (2003) “The social life of genes: privacy, property and the new genetics”, *Social Science & Medicine* 56: 53-67.

Facial Recognition Vendor Test 2002 http://www.frvt.org/FRVT2002/default.htm

Fine, Allan (forthcoming 2006) *Health Care Technology Assessment Handbook*. Jones & Bartlett Publishing.

Gates, E. Nathaniel (1997) *The Concept of “Race” in Natural and Social Science*. New York: Garland.

INAHTA (2001) A Checklist for Health Technology Assessment Reports.
http://www.dimdi.de/static/de/hta/methoden/sammlung/inahtachecklist.pdf

Introna, Lucas D. and David Wood (2004) “Picturing Algorithmic Surveillance: The Politics of Facial Regognition Systems”, *Surveillance & Society*, 2(2/3): 177-198. http://www.surveillance-and-society.org/cctv.htm.

Kahn, Jonathan D (2005) “Pharmacogenetics and ethnically targeted therapies: Racial drugs need to be put into context”, *British Medical Journal*, 330: 1508

Koehler , J.J. (2001) ”The Psychology of Numbers in the Courtroom: How to Make DNA Match Statistics Seem Impressive or Insufficient” *Southern California Law Review*. 74: 1275-1306

Kristensen, FB, M Hørder & P Poulsen (2001) *Metodehåndbog for Medicinsk Teknologivurdering*, Copenhagen: Statens Institut for Medicinsk Teknologivurdering.

Mund, Claudia (2005) “Biobanks – Data Sources without Limits?”. http://www.privacyconference2005.org/fileadmin/PDF/mund_e.pdf

Norwegian rail (2005): http://www.nsb.no/internet/no/Nyheter/article.jhtml?articleID=29884&language=no

Pálsson, Gísli, and Paul Rabinow (2001) “The Icelandic genome debate”, Trends in Biotechnology, 19(5): 166-171.

Petersen, Alan (2005) “Securing our genetic health: engendering trust in UK Biobank”, Sociology of Health & Illness, 27(2): 271-292

Salter, Brian and Mavis Jones (2005) “Biobanks and bioethics: the politics of legitimation”, Journal of European Public Policy, 12(4): 710-732

Sætnan, Ann Rudinow (2005) ”All Foetuses Created Equal? Constructing Foetal, Maternal and Professional Bodies with Obstetric Ultrasound”, in Morgan, Brancth and Kvande (eds.) *Gender, Bodies and Work*. Aldershot: Ashgate Publishing: 139-150.

Skolbekken, John-Arne. (1995) The risk epidemic in medical journals. Soc Sci Med 1995;40: 291-305.

Skolbekken, John-Arne, Lars Øystein Ursin, Berge Solberg, Erik Christensen & Borgunn Ytterhus (2005) ”Not worth the paper it’s written on? Informed consent and biobank research in a Norwegian context”, *Critical Public Health*, 15(4): 335-347

http://www.muckraker.org/pg_one_investigation-1206-9-0.html (Reasonable doubt? CNN special in collaboration with Center for Investigative Reporting)

Tagg, John (1993) The Burden of Representation

Thacker, SB (1985) 'Quality of controlled clinical trials. The case of imaging ultrasound in obstetrics: a review', British Journal of Obstetrics and Gynaecology, 92: 437-444.

Expert Report:
Public Services

Charles D. Raab
School of Social & Political Sciences, University of Edinburgh, UK
c.d.raab@ed.ac.uk

Introduction

This report illustrates how new departures in the public services, in Britain as elsewhere, are raising concerns about privacy invasion through surveillance, and considers the challenges they present to regulators in limiting or eliminating these adverse effects. As we shall see, the collection, use and communication of large stores of personal data held on citizens are central to the functioning of the public services. Different data sets may be matched against each other to identify persons and suspicious patterns of activity. The data may also be 'mined' – analysed in great depth by sophisticated technologies to reveal patterns that may require further investigation. The surveillance that is involved in the public service can be usefully thought of in terms of 'dataveillance', 'the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'.[207] That term, a variation of 'surveillance', emphasises the importance of databases, rather than visual or auditory means of watching over people, in the practices of states. Dataveillance does not only happen in the public sector, and it also may be combined with other surveillance mechanisms.

Sometimes, the collection and linkage of databases – even for ostensibly beneficial, 'public interest' purposes – has been judged excessive and the lack of transparency and regulation have been severely criticised. Perhaps the most notable instance of this was the Canadian Government's Longitudinal Labour Force File, which linked a vast amount of federal and provincial administrative data on Canadian citizens, including information about social assistance, income tax, immigration, employment services, and unemployment insurance. As many as 2,000 pieces of information on about 34 million Canadians were involved in this surreptitious, weakly regulated, public-service-related research programme. Following its exposure, public outcry, and strong action from the federal Privacy Commissioner, it was dismantled in 2000 with the requirement that much more stringent privacy protection, including encryption and disidentification, as well as stronger accountability and transparency, be incorporated into any such future sharing of information.[208]

Electronic government has been an international trend that is not confined to advanced Western societies.[209] Within these 'customer-focused' approaches to better service-delivery,

[207] Clarke, R. (1987 [1991]) 'Information technology and dataveillance' http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html Accessed 1/09/06

[208208] Todd, D. (2001) *Politicizing Privacy: 'Focusing Events' and the Dynamics of Conflict.* Unpublished Master's Thesis, University of Victoria, BC, Canada, 58-86; see also http://www.hrsdc.gc.ca/en/cs/comm/news/2000/000529_e.shtml Accessed 1/09/06

[209] See Heeks, R. (ed.) (1999) *Reinventing Government in the Information Age: International Practice in IT-Enabled Public Sector Reform.* London: Routledge; Prins, J. (ed.) (2001) *Designing E-Government: On the Crossroads of Technological Innovation and Institutional Change*. The Hague: Kluwer Law International.

including 'one-stop' government,[210] simplifying the collection and communication of personal data has been seen as crucial for efficiency, effectiveness, and customer satisfaction. For many years, British government, like many others, has been interested in developing new approaches to providing public services through the use of advanced information and communications technologies (ICTs), both as instruments to be used within and across service-providing agencies, and at the interface with the citizen.[211] Electronic 'information-age' government (e-government) has been the headline for these innovations in central and local government, promising to revolutionise the way in which public administration and policy-making works, both within state organisations and in their relations with the public across the increasingly 'virtual' counter. This campaign can be traced through a long line of proposals, White Papers and other departures, promoted through centrally-led technical and policy initiatives and strategic frameworks;[212] the 2005 White Paper, *Transformational Government – Enabled by Technology*,[213] is the latest in a long line. The potential implications for the way citizens are served and conduct their relations with government, whether in paying taxes, getting a wide variety of benefits, applying for licenses and passports, asking for information, or in other ways, are very great.

If they achieve the aims that government wants, modern developments in the provision of public services can bring undoubted benefits to citizens and to the state. But the information resources that are considered necessary for integrated or proactive services, and their side-effects, are worrisome in terms of privacy and related values such as unjust inferences made on the basis of personal data, the ability to control one's information, and the preservation of human dignity in the face of potential exposure or embarrassment.[214] They pose severe challenges to existing forms of privacy regulation, inspiring a search for fresh solutions and settlements of the tensions over the way personal data re used,[215] and for ways of limiting surveillance and making it more accountable. This brief report will first outline some of the main developments in public services that implicate surveillance and privacy. It will then comment upon them and look to the future. Finally, it will highlight the challenges facing regulators.

Key Developments

'Public services' is a category with blurred edges in contemporary society, both in Britain and abroad. In the modern state, many services that were traditionally provided by public authorities are now provided through a sometimes complex combination of public, private, voluntary-sector and market mechanisms, and sometimes by only one of these types. These patterns vary across countries, for historical, political and other reasons. For instance, some services have traditionally been mainly privately provided, as in the case of health care in the USA. Elsewhere, as in eastern Europe under former regimes, the state has held a monopoly of service provision. In many countries, including Britain, there is a trend towards more integrated, 'joined-up' public services, often through partnerships and teamwork across several agencies. Increasingly, a variety of local partnership arrangements bring together a

[210] Hagen, M. and Kubicek, H. (eds.) (2000) *One-Stop-Government in Europe: Results From 11 National Surveys.* Bremen: University of Bremen; Petrie, A., Brewer, N. and Bellamy, C. (2000), 'England and Wales', in Hagen, M. and H. Kubicek (eds.), op cit. n. 4

[211] Bellamy, C. and Taylor, J. (1998) *Governing in the Information Age.* Buckingham: Open University Press.

[212] See Central Information Technology Unit (CITU), Cabinet Office (2000) *e-Government: A Strategic Framework for Public Services in the Information Age.* London: Cabinet Office; Performance and Innovation Unit (PIU), Cabinet Office (2002) *Privacy and Data-Sharing: The Way Forward for Public Services*. London: Cabinet Office; Margetts, H. (1998) 'Computerising the Tools of Government?', in Snellen, I. and van de Donk, W. (eds.) *Public Administration in an Information Age: A Handbook*. Amsterdam: IOS Press; and other literature cited in Raab, C. (2001) 'Electronic Service Delivery in the UK: Proaction and Privacy Protection', in Prins, J. (ed.), op cit. n. 3.

[213] Cabinet Office (2005) *Transformational Government – Enabled by Technology* (Cm 6683). London: The Stationery Office.

[214] 6, P. (1998) *The Future of Privacy, Volume 1: Private Life and Public Policy*. London: Demos.

[215] Performance and Innovation Unit (PIU), Cabinet Office (2002) op cit. n. 6.

variety of agencies and professions so that their skills can be better focused on providing services to individuals in a more integrated way.[216]

One effect of this key development is that the boundaries that were once thought to have provided certain, albeit fragile, safeguards to privacy and limits to surveillance are called into question, often leaving both the public and the service-providers bewildered about how personal information is, and should be, managed. Personal data flow into new channels, through organisations that never before had access to them, and whose traditions of confidentiality and privacy protection may differ substantially from each other, and from those of agencies in the public sector. These new developments raise serious questions about who trusts whom with what data, because, to make a success of these innovations in public services, information about individuals must be shared, pooled or made accessible to those service-providers who need to know it. Research findings help to cast light on this, although differences across surveys suggest that that they cannot be conclusive. In any case, a 2003 survey conducted by MORI for the Department for Constitutional Affairs[217] found that 60 percent of a sample of the British public said they were very or fairly concerned about personal data-sharing in the public services; 22 percent were very concerned, and only 12 percent were unconcerned. Lack of control over the data and lack of knowledge about what was done with it were apparently the most important factors explaining these levels of distrust. On the other hand, opinion was much more evenly divided when people were asked to respond to scenarios involving information-sharing between specific public agencies, and the levels at which people trusted the public services with their personal information were fairly high. The survey findings, however, varied according to age, social class, geography and other variables which may be important to take into consideration in particular instances where government contemplates extensions of public-service surveillance, which it has done in very recent years. Moreover, as will be mentioned below, young children are increasingly becoming a policy target, yet extremely little attitude research is available to show their levels of trust, concern, or acceptance of information processing that has privacy implications for them.

One problem for the public services is deciding who needs to know it, for what purpose, when, and how much. Much of this information may be highly sensitive, perhaps especially where young children or persons with mental-health or addiction problems are involved. There are important issues concerning how traditional understandings about confidentiality, and the crucial ingredient of trust, can be transferred to the new ways of joint working and information sharing. The mechanisms and ground-rules – including legal powers – for such integrated use of personal data are gradually being established, although unevenly and often with difficulty and uncertainty concerning the precise arrangements to be put in place. These arrangements include gaining individuals' consent where necessary, and establishing procedures for control and accountability. Problems are posed for the public and for privacy regulation, because it is less easy to 'follow the data' and to make sure that it is being collected and handled responsibly and within the law.

As we have just seen, better integration overcomes the boundaries between services that provide benefits to citizens, such as health, education, housing, social welfare and social care. It also aims to provide smoother working among public agencies that apply sanctions, controls and punishment, such as licensing, policing, probation, prisons and the courts. Policy-makers and those on the front line in the public services largely determine what kind of, and how much, dataveillance should take place; in other words, the dimensions of privacy

[216] 6, P., Raab, C. and Bellamy, C. (2005) 'Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I'. *Public Administration* 83 (1): 111-133; Bellamy, C., 6, P., and Raab, C. (2005) 'Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II'. *Public Administration* 83 (2): 393-415.

[217] Department for Constitutional Affairs (2003) *Privacy and Data-Sharing: Survey of Public Awareness and Perceptions.* London: Department for Constitutional Affairs. http://www.dca.gov.uk/majrep/rights/mori-survey.pdf Accessed 1/09/06

protection or invasion. This is because, in all areas of the public service, these new ways of working, in addition to more familiar ones, have important implications for the way large quantities of personal data flow in and across organisations, raising new issues concerning what information – and how much – needs to be used, who is responsible for protecting the data, who should have access to the databases and on what terms, how information should be collected, and so on.

But the distinction between 'benefits' and 'sanctions' itself is not hard-and-fast, because, for example, when it comes to preventing fraud or catching fraudsters in the welfare state, action takes place that brings both systems together. While combating fraud may be a law-enforcement and criminal justice matter, it is also a matter for a number of other public services and brings their holdings of personal data into play as anti-fraud tools. A recent Home Office consultation paper,[218] seeking new powers against organised and financial crime, highlights this, complaining that 'data sharing with other parts of the public sector is highly patchy, while sharing across the public-private divide is rarely even attempted'.[219] To help prevent and combat fraud, it calls for an improvement in these flows of information, including – with regard to Suspicious Activity Reports – matching data between the new Serious Organised Crime Agency (SOCA) and the databases of a host of government bodies, including Her Majesty's Revenue and Customs, the Driver and Vehicle Licensing Agency, the Department for Work and Pensions, and the Passport Service. It also argues for 'targeted and proportionate' data mining exercises across the public and private sectors where there are strong suspicions of criminal activity, although it also wishes to see that privacy rights are protected.[220] The paper makes much of the requirement for proportionality in its proposals for data mining and for introducing 'serious crime prevention orders'; how data mining is to be made 'proportionate' is still a matter for discussion, but establishing and policing the rules is likely to involve important inputs from the Information Commissioner.

Combating fraud has, for many years, involved state organisations in the intensive use of personal data, within a framework of limitations and safeguards. The sprawling system of social benefits, provided through many agencies, has been open to identity theft, 'double dipping' and other illegal activities. In the 1990s, government and parliament began to take a more serious interest in this problem, calling for strong measures that would include the use of data sharing and data matching in order to detect and prevent fraud. The Social Security Administration (Fraud) Act 1997 gave powers to do this, followed by another Act in 2001 authorizing access to individuals' bank and savings accounts and utility company records, and – in some cases – to private sector payrolls. Under the 1997 Act, the Department for Work and Pensions (DWP) conducts many routine matches of personally-identifiable data, including records of housing benefit, social security, national insurance, taxation, as well as gas, electricity and telephone records. DWP proactively checks claimants' identity and dependents with other public bodies. There is also a very large data-matching exercise carried out every other year by the Audit Commission under the National Fraud Initiative (NFI). The purpose is to help detect fraudulent and excessive payments made to claimants from public funds.[221] Housing benefit fraud is still the primary problem, but the NFI is now very wide-ranging in the information it accesses. Data from local and health authorities' payroll and pensions records are used, along with records on tenants, housing benefits, social security files and information on asylum seekers. Estimates of the monetary volume of incorrect payments vary greatly, but are supposed to be in the low billions of pounds, while the results of eliminating them have been measured only in much lower amounts, estimated to have been £126 in 2004-5, including Scotland.[222] This is a tiny fraction of what is paid out in benefits,

[218] Home Office (2006) *New Powers Against Organised and Financial Crime* (Cm 6875). London: The Stationery Office.
[219] ibid., 12.
[220] ibid., 13.
[221] http://www.audit-commission.gov.uk/nfi/ Accessed 1/09/06.
[222] Audit Commission, *National Fraud Initiative 2004/05*. http://www.audit-commission.gov.uk/nfi/downloads/NFI_2004-05Summary.pdf. Accessed 1/09/06

and includes overpayments, which are not fraudulent. Although fraud is fraud, questions have been raised about the proportionality, transparency and other privacy implications of data-intensive methods of plugging the hole in public expenditure.

Surveillance to combat fraud has occasionally stimulated concern, for different reasons, by welfare and human rights organisations, the Information Commissioner, trade associations, parliamentary bodies, and even by the then Inland Revenue, who were worried about the effect that a disregard for confidentiality might have on tax administration. Anti-fraud information techniques seemed disproportionate; they also were said to invade privacy in ways that were unfair because of inaccurate and outdated information, and to fall foul of the European Convention of Human Rights and the Human Rights Act 1998. Anti-fraud dataveillance activities rely on legislative permissions that vary in their explicitness. Ministers were forced to agree that data-sharing powers created by the legislation would not be implemented until acceptable codes of practice were devised. These codes were published in 1998 and 2002 respectively. For the NFI, these issues are covered by an updated code of data-matching practice for England adopted in 2006,[223] and by separate ones for other parts of the United Kingdom.

Another key development can be seen in these as well as other public service activities: the increasing emphasis on a precautionary, targeted, risk-limiting approach to social policy. Increasingly, government aims to anticipate and prevent the social problems of specific groups or categories of citizens, and not merely to respond to problems once they occur. An important current emphasis in policy is the identification of risks and the ability to target interventions on people who are considered to be at risk or to pose risks for others. Analysis of information of various kinds, including data on identifiable individuals, is important for this. A wide variety of policies are part of this drive.[224] Risk-based approaches, based on assessments of individuals, families and neighbourhoods, are found in child protection and mental health, as well as in the criminal justice field of public protection. Such initiatives, and others that, for example, home in on public-service fraudsters, young offenders and children in need of the SureStart ‘early years’ programme, make intensive use of data about individuals. Based on the belief that social, economic and personal problems are often concentrated in certain areas, the development of ‘neighbourhood statistics’ responded to the need for better data for intelligence-led, tailored and targeted interventions co-ordinated across several agencies.[225] Public health is also oriented towards identifying communities and individuals at risk. As in the sanctioning side of public services, the extensive and intensive use of surveillance and dataveillance is considered essential if policy interventions are to be ‘intelligence-led’. This trend continues, despite the many costly delays and difficulties that British government has experienced with the functioning of the information systems, technologies and databases on which economical, effective and efficient public services depend.

The field of child protection is a particularly prominent generator of surveillance and of the extensive sharing of information. Worries about children at risk of physical and psychological abuse have been very much in the foreground of public and political concern. Whenever a failure in preventing significant harm is traced to a failure in data sharing – as in the report written after the tragic death of Victoria Climbié[226] or in the investigation that followed the Soham murders[227] – the social services and policing are urged to increase their efforts towards

[223] Audit Commission (2006) *Code of Data Matching Practice 2006*. http://www.audit-commission.gov.uk/nfi/downloads/Code_Data_Matching_2006.pdf Accessed 1/09/06
[224] 6 *et al*. (2005) op cit. n. 10.
[225] Social Exclusion Unit, Cabinet Office (2000) *Report of Policy Action Team 18 on Better Information*. London: Social Exclusion Unit, Cabinet Office; Department for Work and Pensions (2001) *United Kingdom National Action Plan on Social Exclusion 2001-03*. London: Department for Work and Pensions.
[226] Laming, Lord (2003) *The Victoria Climbié Inquiry: Report of an Enquiry by Lord Laming* (Cm 5730). London: The Stationery Office.
[227] Bichard Inquiry (2004) *The Bichard Inquiry Report.* London: Home Office

collecting and sharing information, even including ‘soft’ data and allegations about possible offenders. This is done in order to help take precautions to reduce the risks that certain individuals may be exposed to or may present, even though information was available but ignored or wrongly interpreted in many cases that resulted in tragedy.[228] False negative judgement errors – failing to take action which later proves to have been warranted – is not now tolerated. Rather, ‘better safe than sorry’ stands as a motto that supports the considerable rise in social-care referrals for child abuse, the maximum use of personal and other data, and that gives a green light to the precautionary surveillance of groups, categories and individuals by the public services.

The ‘safety-first’ motto also helps to support the concerted development of a wide-ranging information strategy in fulfilment of the policy objective to safeguard children in a comprehensive and precautionary manner.[229] This involves efforts to combat social exclusion and to deal with young offenders, and, especially, interventions in the education sector. It includes new departures such as the children’s database, or ‘information sharing index’ for 150 local areas, that will include data on all children in England and Wales up to the age of 18 years. The purpose is wider than child protection, and is aimed at a more holistic purpose relating to children’s welfare and the provision of services: the indexes will identify each child and show whether they are receiving the relevant services. The database is to include basic details plus unique identifying numbers and contact details for parents, schools, health carers and other professionals who supply additional needs and who may have important information or assessments to share. This idea, which featured prominently in the 2003 Green Paper, *Every Child Matters*[230] and was legislated for in the Children Act 2004, is intended not only to bolt the door against future tragedies, but also to fulfil a much wider care-agenda commitment that children’s needs are being provided, thus involving the education and health services as well.

But this development has raised concerns about surveillance: that too much data will be collected, that it will be open to unauthorised access and disclosure, and that other privacy-invasive dangers will arise. Against the tendency that the children’s database illustrates, it is not easy to say how seriously it is considered that harm may be done through the excessive collection and sharing of data or through jumping to the wrong conclusions on the basis of allegations, inaccurate data, or erroneous, de-contextualised interpretations. Following the Climbié and Soham events, false positive judgement errors – taking action where it later turns out not to have been warranted – are now condoned again in social policy and practice, even though families and whole communities had earlier been stigmatised and seriously disrupted as a result of errors by overzealous social work staff that led to children being taken into care on the basis of what later turned out to be unsubstantiated allegations, as in the 1991 Orkney[231] and Cleveland[232] child-abuse affairs. Beyond child protection as such, persons have been denied employment on the basis of incorrect information, or of recorded suspicions, about their identity and past behaviour.[233]

Massive investment has also gone into creating changes in the use of personal information in health care. The National Health Service (NHS)’s IT programme, now branded *Connecting for Health*, is thought to be the largest one of its kind in Europe, and commitments have been made far into the future.[234] For the past ten years or so, there have been great efforts to co-

[228] Raab, C., 6, P., Birch, A. and Copping, M. (2004) *Information Sharing for Children at Risk: Impacts on Privacy*. Edinburgh: Scottish Executive, ch. C.

[229] FIPR, 2006

[230] H.M. Treasury (2003) *Every Child Matters* (Cm 5860). London: The Stationery Office

[231] Clyde Report (1992) *Report of Inquiry into the Removal of Children from Orkney in February 1991*. Edinburgh: HMSO.

[232] Cleveland Report (1988) *Report of the Inquiry into Child Abuse in Cleveland 1987* (Cmd 412). London: Her Majesty’s Stationery Office.

[233] For a much more detailed discussion of the question of children’s databases and privacy, see the ‘Database Masterclass’ http://www.databasemasterclass.blogspot.com/ Accessed 1/09/06. Discussion of the Scottish eCare programme, which in part also concerns the sharing of personal data for children’s services, see Raab ***et al.*** op cit. n. 22.

[234] The Wanless Report (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report*, London: H.M. Treasury.

ordinate, and to develop further, the computerisation of patients' records, moving ultimately towards a comprehensive national digital database of all personal health records. The NHS 'spine' of data on each patient[235] is at the centre of the NHS Care Records Service, containing a limited amount of essential information that can be combined with a larger amount of locally-held care information. In addition, the programme involves national databases with patient records supplied by local NHS bodies, including data on notifiable diseases and information held for clinical audit. Pathology and other test records can be filed electronically. Plans and partial developments also include booking appointments, prescriptions, electronic transfer of patients' records between GP practices, and other functions. Electronic patient records are held and transferred securely, for they are encrypted with a public-key system, and are subject to rules that allow personnel in each NHS function to look at only those data that are relevant to that function. There have been some local pilot schemes in which patients manage their own records through the use of smart cards.

Although the NHS's plans have been beset by a great number of problems, delays and implementation failures, it is easy to see how the new ways in which information is, and will be, used, give rise to questions about the privacy and surveillance implications. Nowadays, when 'best practice' in health care involves other services as well – social care, among others – the question of keeping control over patients' data, as well as the accuracy and quality of those data, have become major issues. Health data are regarded as 'sensitive', although some are more sensitive than others. Many professionals worry whether traditional assumptions about confidentiality can be maintained when it comes to, for instance, making 'single shared assessments' of certain patients who are dealt with by social care as well as by health professionals, or where data on mental-health patients may require that data be shared with yet other agencies, sometimes including the police. For nearly ten years, a system of 'Caldicott Guardians', named after the author of a report that looked into the confidentiality of identifiable patient data in the NHS,[236] has been in place. This means that every NHS body has a designated person who oversees confidentiality, controls access to patient information, helps to develop protocols for information-sharing across organisations, and works to ensure good practice concerning patient data. This system is part of a wider 'information governance' framework in the NHS, and is now also being used in social care agencies. But whether or not the 'guardian' system has worked well – the results have been patchy and there are many shortcomings, owing to factors including the complexity of 'eHealth' information technologies and information flows, inadequate resources and training, and weak institutional role support[237] – controversies over the disclosure of health data have arisen in the context of anti-terrorism, crime-fighting and Audit Commission investigations. The Department of Health has formed a confidentiality strategy and a code of privacy and confidentiality practice,[238] and the Information Commissioner has produced guidance for the health sector when anxiety developed over the sharing of NHS data with other agencies.[239]

The most prominent surveillance initiative in recent years, in many countries, has been identity (ID) cards; these schemes are detailed and discussed elsewhere in this Report. In Britain, and stretching over a wide – and, as a recent House of Commons Select Committee report[240] has complained, disturbingly unclear – range of functions, ID cards has been the most controversial British issue involving potential threats to privacy through the surveillance involved in the establishment and use of the National Identity Register (NIR) that will be

[235] http://www.connectingforhealth.nhs.uk/delivery/programmes/spine Accessed 1/09/06
[236] Department of Health (1997) *Report on the Review of Patient Identifiable Information* (The Caldicott Report). London: Department of Health.
[237] NHS Scotland (2004) *A Review of the EWork of Caldicott Guardians in Scotland*. http://www.confidentiality.scot.nhs.uk/publications/Caldicott%20Review.pdf Accessed 1/09/06.
[238] Department of Health (2001) *Building the Information Core: Protecting and Using Confidential Patient Information.* London: Department of Health; Department of Health (2003) *Confidentiality: NHS Code of Practice.* London: Department of Health.
[239] Office of the Information Commissioner (2002) *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998.* Wilmslow: Office of the Information Commissioner.
[240] House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence*. Sixth Report of Session 2006-06, 20 July 2006, HC 1032. London: The Stationery Office

under the Identity Cards Act 2006. While ID cards will serve traditional Home Office functions regarding law enforcement (broadly speaking), immigration and asylum, national security and counter-terrorism, they are also intended to 'secure the efficient and effective provision of public services' in ways that still sketchy, but that potentially involve a large array of departments and agencies which relate to specific service fields. A key element is the provision of a unique reference number for each person, facilitating the integration of a vast number of data sources. Moreover, indications that government foresees interaction between the public and private sectors in the use of the ID card, including access to the NIR, adds further concerns about limitations and privacy safeguards for this potential extension of surveillance. This Report is not the place to go over this ID card scheme in detail, but it is sufficient to say that it will powerfully shape dataveillance plans and activities across these public services, even if the signs, so far, are that there is a lack of co-ordination and lagging development amongst the organisations that are involved in public-service systems using personal data.

Critical Commentary and Future Directions

Better and more detailed information about identifiable persons, easier availability of personal data to a range of service providers, are essential if patients, clients, pupils, claimants, taxpayers and others are to receive the high-quality services they have rightly come to expect in Britain today. Meeting their needs depends on the application of the latest ICTs, and on revamping the way case records are collected, processed, stored and communicated. It also depends on training staff at all levels to integrate new information systems into their daily work routines, often in direct contact with members of the public.

New developments in the provision of public services and in related state functions, and the surveillance activities that they depend upon, have been controversial for many reasons, both practical and ethical. Intensified dataveillance is becoming a normal feature in the modern state, and may, in itself, be justifiable – and justified by those who promote them – in the public interest. These activities may often be explicitly empowered by parliament. What makes them problematic is their manipulation of large quantities of personal data in ways that may overstep the mark established by data protection principles and laws (parliament, once again), and by other constraints and guidelines about how information is to be collected, collated and communicated. We may become accustomed to being surveilled, our activities and movements tracked and also anticipated, without noticing it, and – especially in the public services – without the ability to opt in or opt out, or to understand fully what happens to our data. We may well accept as 'reasonable' the limitations on privacy that we might otherwise reject if we were to consider what being a citizen should be. It is far from certain that the political situation will, at the end of the day, allow privacy rights to stand up strongly to the claims of government organisations made in the 'public interest', even if the public interest seems clear and of greater importance. If surveillance is meant to be 'proportionate', a lot depends on how that terms is interpreted, and on who interprets it. A lot also depends on the safeguards that surround the new, intrusive developments.

However, in promoting new plans and programmes, government has also, from time to time, recognised the question of privacy and the dangers of surveillance. It has therefore attempted to bring to the surface the important question of public trust in the information processes of 'information age government', including public-service provision both online and in other ways. Sometimes the 'down-side' has not been considered in anything like the depth that the presumed benefits have been. But privacy issues have been important in the debates about trust, although not so prominent or so influential as was hoped for by those who have been worried about the surveillance potential of the new, more integrated and extensive, use of databases and like. When the Performance and Innovation Unit produced its report in 2002 on privacy and data-sharing,[241] it went further towards trying to provide solutions that would both enable personal data to be used and shared, and that would also enhance the protection of privacy. However, putting its recommendations into practice has, for the most part, fallen behind, overtaken by events and new initiatives which have made the prospects of good privacy protection in the public services look more remote unless countervailing safeguards can be built into these initiatives, or applied to them afterwards.

There are now new initiatives for squaring the circle between the public services and the protection of privacy. One of the latest big proposals[242] pays some heed to the issues, and there is also a new Ministerial Committee on Data-Sharing – MISC 31[243] – with a remit to 'develop the Government's strategy on data-sharing across the public sector'. This includes some renewed thinking about the safeguards that can be put in place so that data-sharing, which is at the heart of surveillance in the public sector, can take place fairly, lawfully, and in keeping with other requirements for privacy and data protection. It is far too soon to say whether these efforts will achieve more success than their predecessors have done. One important question is how strong these current data-protection requirements actually are to regulate pubic-sector surveillance.

Challenges to Regulators

It is not enough for government to decree a privacy-protective solution to these problems without a heavy input of co-operation from all the organisations involved in providing services to the public, whether on the benefits or the sanctions side of the public services, as outlined earlier. These organisations exist in a large network that includes central and local government, the professions, voluntary bodies and commercial firms that supply services to the public and that process personal data in doing so. How to get them all 'on side' in understanding the surveillance issues, and in taking privacy seriously while still retaining the capacity of the public sector to perform its functions, is no mean task. Joined-up public services mean joined-up surveillance. This may be beneficial, but the challenge is to meet its negative aspects with joined-up privacy protection.[244]

In this sense, we all participate in shaping the outcomes of regulation, since it is the decisions made by those who are subjected to surveillance, by those who practice surveillance, and by those who are officially responsible for creating and applying the rules – government, parliament, the Information Commissioner, the tribunal and the courts – that will determine how well privacy can be protected and how surveillance can be controlled. Among the key problems is to see how far the systems of regulation that have grown up through legislation, common law, common sense, ethical norms, and opposition can be applied to the new policy initiatives and new ICT-led processes for the public services, and to what extent new approaches need to be developed. There are those who say that the classical principles of privacy and data protection, which are built into the Data Protection Act 1998 and virtually every other Act of its kind, including international conventions and the like, are now increasingly irrelevant in a joined-up, online world in which the flows of personal data are so much more complex, bewildering, and unaccountable than before. They argue, very plausibly, that surveillance makes greater inroads on people's lives and fortunes than the invasion of their privacy as such, On the other hand, others say that the principles are still valid and useful, although they may require new practical instruments to put them into effect, along with new roles, new institutions, new powers, new regulatory techniques – including, prominently, privacy impact assessment conducted with a wide range of searching questions,

[241] Performance and Innovation Unity (Cabinet Office) op cit. n. 6.
[242] op cit. n. 7.
[243] http://www.cabinetoffice.gov.uk/secretariats/committees/misc31.asp Accessed 1/09/06
[244] Raab, C. (2003) 'Joined-up surveillance: The challenge to privacy', in Ball, K. and Webster, F. (eds.) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press.

beyond privacy compliance – and new relationships between the regulators and the regulated. It may be crucially important for regulators to be able to influence policy at an early stage. That depends upon the possibilities available to them in their role descriptions, the willingness of policy-makers to open their plans to early scrutiny, and the ability of regulators to create opportunities for themselves to make, and to publicise, observations on policy plans before they are too firmly set. All these matters, which overarch all domains covered in these expert reports, have been addressed in greater detail in the main Report.

Some of the future will probably be taken up by debates and discussions about these views and proposals. But there will also need to be some revisiting of the main concepts involved in surveillance and in privacy protection, in order to see their practical implications. These are listed in no order of priority here, and the list is not exhaustive:

- *risk*: what it is in any given situation; how it can be measured; and how it can be reduced or managed;
- *trust*: who needs to trust whom with what information; how trustworthiness can be established; and how much trust is needed;
- *equity*: who gets what privacy in regard to public services; who is subjected to surveillance; and what can be done about the disparities between the privacy 'haves' and 'have nots';
- *proportionality*: how do we know when it exists or does not exist; who shall decide; and how much disproportion is acceptable or oppressive;
- *the 'need to know'*: who needs to know what personal data, when and why; how can reliable access controls be implanted into information systems; and how can audit trails and accountability procedures be established;
- *transparency*: how can the public know what is done with their data; how can they participate in decisions about this; how can they hold others to account.

There are no prizes awarded for adding several more concepts to be looked into. But there will certainly be no prizes, either, for attempting to change regulatory systems for limiting surveillance without looking into all these, and more, and drawing practical lessons from them.

Expert Report: Telecommunications

Nicola Green
Department of Sociology, University of Surrey, UK.
n.green@surrey.ac.uk

Introduction

Telecommunications are one of the infrastructural factors that have come to define the very shape of modern life in contemporary western societies. Telecommunications technologies now underpin everything from the economic or political life of entire societies, to the rhythms of everyday life for individuals. As such, they are central to contemporary social relations of surveillance, including the monitoring, regulation and control of information and communication, informational power and privacy rights, and the monitoring and sorting of individuals via their telecommunications practices. Telecommunications technologies are also in a period of rapid expansion and change, simultaneously intensifying in their scope and reach, as well as shifting in their form, to create 'hybrid' technologies that combine aspects of multiple technological systems.[245] This rapid technological change has created a sense of uncertainty surrounding the regulation of surveillance practices associated with telecommunications, as the organisations with such a remit have multiple and overlapping briefs and activities, which impact upon the status and use of the information derived from telecommunications surveillance practices. This section of the report therefore aims to identify some of the key current developments in the surveillance of telecommunications, outline some of the existing technological and organisational uncertainties, and thereby ascertain some of the challenges and dilemmas facing regulatory bodies in this area.

Any discussion of *telecommunications surveillance* must begin with a consideration of the kinds of technologies, processes and interactions that might be encompassed by such a phrase. 'Telecommunications' as a concept has itself been used in wide-ranging ways, both referring to the infrastructural technologies used to communicate, as well as to how those technologies are made functional, and how they are used. Included within definitions of telecommunications are the infrastructural technological processes of communication – for example, the transmission, emission or reception of information-bearing electrical or electromagnetic signals between remote systems via infrastructural media. The term is also used to refer to the systems and devices through which telecommunications are achieved – the telegraph, the telephone, or radio, for example. Finally, the term encompasses the communicative process and product – which includes the exchange of 'data', 'messages' or 'information'. The communicative assemblage falling under the umbrella of 'telecommunications' was until quite recently restricted to a relatively narrow range of devices and their operation and interaction – for example, coded messages achieved via telegraph, voice calls made via fixed-line telephony, textual transmission via facsimile machines, or the transmission of messages via radio waves. More recently however, the definition of the term 'telecommunications' has itself expanded rapidly alongside the intensive development of information and communications technologies, and the re-organisation of social life around changing communicative infrastructures. Included in current

[245] Uncertainties also lie in the 'expanding mutability' of the devices, not only the ways the technologies change over time, but the ways they can be used for unintended purposes. See Norris, C, and Armstrong, G (1999) *The Maximum Surveillance Society: The Rise of CCTV* Oxford: Berg.

definitions of telecommunications are not only analogue but digital signal formats, and telecommunications includes not only fixed line telephony with voice calls and faxes, but the new systems of mobile telephony that include a range of communicative functions such as voice, text, images, sounds, and location-based information. The term also now encompasses the huge range of communicative functions, both synchronous and asynchronous, enabled by large scale digital and computing systems such as the Internet, whether those are enabled through fixed-wire or wireless devices of different types.

What the expansion of the term makes clear however, is that the form and content of any communicative exchange – whether that is defined as 'signal', 'data', 'message' or 'information' – is as central to telecommunications as the technological systems in place to enable it. Any consideration of *telecommunications surveillance* must therefore consider the social organisation and regulation of communicative exchange, as well as the technological mechanisms that enable the monitoring of telecommunications systems. In a social as well as technological definition then, surveillance in telecommunications refers to the degree to which individuals, organisations and corporate bodies are able to monitor, sort and store information about the occurrence and content of telecommunications exchange, both between technological devices, and between technological devices and people.

As the above definition implies, the social map of telecommunications surveillance in the UK now references an extensively complex and interconnected range of technologies, social actors, organisations and processes that defy any simple rendering of what constitutes 'telecommunications surveillance'. For the purposes of clarity therefore, this section of the report will restrict itself to two-way telecommunications systems including fixed-line and mobile telephony (and related technologies), as well as Internet communications of various sorts.[246] Similarly, discussion of specific infrastructural telecommunications systems defined technologically – such as RFID, or routing systems –are addressed elsewhere in the report. This section will rather focus thematically on telecommunications technologies in two main domains – surveillance of aforementioned telecommunications by the state, and by corporate organisations.

Key Developments

This section provides a background and overview of the range of telecommunications surveillance practices currently undertaken by a number of state and corporate organisations in the UK, the changing technologies to which those practices pertain, and key developments within the field. Historically, the telecommunications infrastructure in the UK was dominated by fixed line copper cable telephony, hosting a number of services such as voice calls, answer-phone services, and facsimile transmissions. Because fixed-line telephony was initially run under state provision by the General Post Office, the provision of both hardware and service (and therefore information about telecommunications use) was concentrated in a single supplier. The single most likely source of surveillance of copper cable telephony was 'wiretapping', most often associated with state law enforcement.

Three key developments have seen a radical transformation of this system, the full results of which have yet to be seen – the simultaneous expansion and convergence of telecommunications technologies, the development of information storage and processing capacity, and the diversification of telecommunications markets.

[246] Public and commercial broadcast television and radio will not be addressed here. While technically 'telecommunications' systems currently regulated by Ofcom, they have had a largely separate technological and organisational history to other telecommunications systems such as telephony, and are less central in issues of surveillance than are two-way communications systems.

Convergence and Divergence of Telecommunications Technologies

Throughout the last two decades, technological development and change has led to more diverse technologies employed for telecommunications. To name just a few, radio frequency devices now enable large-scale cellular or mobile telephony,[247] optical fibre cabling enables high-speed digital fixed internet connection, and a combination of both enable wireless computing. The development of each of these technologies has entailed the diversification not only of technologies, but of the functionalities they deliver. Mobile telephony delivers not only voice calls but text, image and video messaging, as well as location-based services.[248] Internet technologies enable both asynchronous communications such as email, bulletin boards and newsgroups, as well as synchronous communications such as chatrooms, instant messaging and webcam/video messaging.[249] Furthermore, current changes in the technologies of communication entail the convergence of technologies, and their interoperability. Internet connection can now be made via a range of devices, including handheld devices and mobile phones, and with the advent of VoIP (voice over internet protocol), voice calls can now be made via the desktop computer.

With the development of each of these different technologies have come the mechanisms for their surveillance – for any of these technologies to 'work,' they require the exchange of signals or data between technological devices, and any exchange of data itself generates the mechanisms for the capture, monitoring and storage of information about that exchange. In mobile telephony, for example, the location of a mobile device can be ascertained simply by triangulating the signal of the device with its reception by a number of different base stations as the signals are 'handed over' from one to another – this information can thereafter be stored, and the data mined for relevant profiling. The import of this simultaneous convergence and divergence is that with the growing ubiquity and embeddedness of these communications technologies, their extensivity and the intensification and speed of data flows deriving from them, the concomitant potential for surveillance of them grows ever wider. As telecommunications technologies become more interconnective, extensive and intensive, the gathering, storing and mining of information derived through them grow exponentially. How this surveillance occurs in telecommunications, and the implications it has, will be explored below.

Information Processing and Storage Capacity

One of the greatest single contributors to the expansion of surveillance of telecommunications has been the capacity to gather, process and store huge amounts of information. With the conversion in telecommunications from analogue to digital signalling systems across most communications technologies, information about the occurrence and content of communications becomes available for scrutiny and manipulation in ways previously unavailable. The hybrid components and systems that comprise operable and interoperable telecommunications networks, when coupled with the economic, social and institutional structures required for their ongoing deployment and use (see diversification of markets, below), could potentially hold at least unintended consequences (if not intended expansions) in data gathering and storage activities. It is not only the act of gathering data by either the state or corporate entities that is of concern in and of itself, but rather the act of gathering data alongside the social meaning that is attributed to it. How that data is organised, categorised and given meaning, and how the meanings attributed to the data are attributed to people, is where the negative effects of surveillance practices can potentially be seen.

The gathering, distribution and use of data generated by mobile phones, how that data is stored and manipulated, and how the categories of that data are attributed to people, is

[247] Radio also enables RFID (radio frequency identification) for tracking goods, services and, potentially, people. See Infrastructure and Built Environment Expert Report

[248] Location-based services in mobile telephony include global satellite information and positioning systems.

[249] Internet functionalities such as web pages and web logs are excluded here as they are ostensibly 'published', and therefore freely and publicly available as a matter of course.

employed here as an illustrative case study in telecommunications surveillance. Of particular interest in mobile telecommunications is the differentiation (or not) between the storage and monitoring of those data considered 'transmission' information, necessary for communications to take place (and largely generated *automatically*), and those data that might be considered 'personal' information such as name, address and payment details, thereby falling under the auspices of relevant Data Protection legislation.

Mobile phone network operators and service providers gather and store a wide range of data as a matter of course. The advent of mass market digital mobile telecommunications has prompted the widespread circulation of what is known as traffic data – largely a-signifying transmission information necessary for digital mobile communications to take place. The Information Commissioner, following the European Commission's Telecommunications Directive (97/66/EC), has defined traffic data as data which: *(a) are in respect of traffic handled by a telecommunications network provider or a telecommunications service provider; are processed to secure the connection of a call and held by the provider concerned.* In the same advice, traffic data is said to constitute personal data when: … *the data subject is a subscriber to, or user of, any publicly available telecommunications service or, in the case of a corporate subscriber, would constitute such personal data if that subscriber were an individual.* By contrast, billing data, including information such as the subscriber's name and address, as well as the length, duration, time and place of their calls,[250] is by definition personal data, and hence can only be processed by explicitly authorised agents. Because all this information is in any case carried in the traffic data, the Information Commissioner has sought to clarify the distinction between traffic and billing data, advising that:

Because data processed to establish calls (known as traffic data) could potentially contain personal information which should therefore only be stored for limited purposes and retention periods, the Regulations provide for the protection of individual and corporate subscribers with regard to the processing of such data. Traffic data must be erased or dealt with in such a way that they cease to be personal data on the termination of the call in question.

The difference between billing data and traffic data is therefore whether or not the data is erased or anonymised at the end of the call. If the data is retained, without anonymising, then it qualifies as billing data – which as personal data is fully regulated by relevant data protection legislation, and its collection, retention and manipulation is restricted to registered data controllers with the informed consent of the data subjects to whom the data applies. If, on the other hand, the data is *retained but anonymised*, then it qualifies as traffic data, and its collection and processing are not restricted by data protection provisions. If anonymising call data entails stripping it of the subscriber's name and address details, all other information, including the time, date, location and duration of the call, the phone numbers involved, and potentially the content of the communication, can be retained, shared, mined, even bought and sold.

[250] 2 The Information Commissioner's advice is that: Billing data is defined as follows:
(a) the number or other identification of the subscriber's station;
(b) the subscriber's address and the type of the station;
(c) the total number of units of use by reference to which the sum payable in respect of an accounting period is calculated;
(d) the type, starting time and duration of calls and the volume of data transmissions in respect of which sums are payable by the subscriber and the numbers or other identification of the stations to which they were made;
(e) the date of the provision of any service not falling within sub-paragraph (d);
(f) other matters concerning payments including, in particular, advance payments, payments by instalments, reminders and disconnections.
Billing data may be any one or all of the above.

The distinction between non-identifiable 'traffic data' in telecommunications, and personally identifiable billing data, is particularly important in the corporate processing of information (see the diversification of markets below). It is, however, largely irrelevant for agencies of the State such as law enforcement, as far as questions of security and law and order are concerned. The effect of the Regulation of Investigatory Powers Act (2000) is to make telecommunications traffic and billing data available on request to UK law enforcement organisations. Under the RIP Act, a senior officer is required to ask a telecommunications operator for traffic data (and each force has to nominate a single point of contact for processing the requisite paperwork). The Interception Commissioner may exercise oversight after the fact on data requests, but the investigating officer in any case need only justify the request to a senior officer who is empowered to make that request. By the end of 2002, the BBC was reporting that law enforcement bodies had made over 400,000 requests for traffic data from mobile network operators.[251] It is worth noting that the BBC here quotes unnamed police sources as being 'frustrated' that traffic data is not always available because data is typically only held – in line with the telecommunications companies' data protection obligations – for six months. The BBC report also cites a forensic engineer arguing that traffic data can link suspects to crimes, quoting him as saying "if a person makes a mobile call, potentially while involved in commission of a criminal act, it is possible to determine from [the traffic data] where the radio footprint would have been made." For this forensic engineer, and the unnamed police sources, there is no differentiation between the mobile as a device and the mobile user. As if to drive the point home, one of the justifications for the Anti-Terrorism, Crime and Security Act, according to the Home Office, is that

Given the increased threat and changing nature of the terrorist networks, intelligence on the movements and actions of terrorists is vital to ensuring the security of the UK. In particular communications data is an important investigative tool: allowing investigators for example to establish links between suspected conspirators (itemised bill) or to ascertain the whereabouts of a given person at a given time, thereby confirming or disproving an alibi (cell site analysis).[252]

Whilst billing data by definition allows for the identification of individual users, the use of cell site data – i.e. traffic data – to categorically establish an individual's (as distinct from a device's) location and activity would appear to contradict claims as to the non-personal character of traffic data. For the law enforcement community, any claims that the mobile handset has no relationship to the user, and that the collation and processing of pseudonymised traffic data has no data protection implications, appears to be inoperative.

The *routine* and *automated* collection of data on such a scale applies equally to the fixed line telephone[253] and internet communications (internet telecommunications data being held on servers by Internet Service Providers). Furthermore, in February 2006, an EU directive on Data Retention and UK legislative initiatives from the Home Office have proposed to require not only mobile telecommunications companies, but those offering both fixed line telephony and Internet services, to retain data collected for up to two years in order that they be available for scrutiny by law enforcement bodies.

It is therefore not only the practices of collecting and processing telecommunications data that have important social effects and regulatory implications, but the scale of such collection, the discourses significant social actors employ to describe and justify how telecommunications data is processed and collected, and the categories and meanings assigned to that data (and

[251] 'Phone firms "flooded" by crime checks'. *BBC Online*, 20 Dec 2002. Available at: http://news.bbc.co.uk/1/low/uk/2592707.stm

[252] See: http://www.homeoffice.gov.uk/oicd/antiterrorism/ria_antiterrorism.htm

[253] The fixed-line telephone system extends the status of 'personal data' to the telephone number because it is associated with a particular residence, and that residence may be identified with a postcode, also categorised as personal data under DPA legislation.

thereafter people). This is as important in the data gathering and data retention activities in the corporate telecommunications sector as it is in the data mining activities of law enforcement.

Diversification of Telecommunications Markets

Alongside the diversification and convergence of both technologies and functionalities in telecommunications, the diversification of telecommunications markets have vastly extended the number of actors involved in the production, distribution and consumption of telecommunications technologies, therefore also vastly extending the potential agents of surveillance in the corporate telecommunications sector.

The early 1980s saw the creation of British Telecommunications (BT) as a separate entity, its almost immediate privatisation, the opening up of market competition in the telecommunications industry in the provision of technology and services to consumers, and the creation of the Office of Telecommunications as the industry regulator. From this point, the fragmentation of organisational responsibilities between telecommunications network operators, service providers, content providers, and technology developers, meant that the range of organisational agents potentially retaining and mining telecommunications data has risen exponentially. There is little doubt that such data is in itself of value to the telecommunications industry – the use of such data in mobile telecommunications is again an illustrative case in point.

Telecommunications companies (Network Operators, Internet Service Providers, Content Providers) routinely gather and manipulate the personal data they hold about their own customers in a similar vein as do other private sector organisations, to sort and categorise those customers as consumers.[254] Additionally however, for the private sector the distinction between restricted billing (personal) data and fully archivable traffic data is important. The value chains that support, for example, telecommunications marketing campaigns, such as those conducted via mobile phones, are extensive. Marketing campaigns might include a host of small companies acting as consultants to organisations working on everything from client branding, to mobile technology and data, which interact with network operators and service providers. A single mobile SMS (short message service, or text) campaign can involve the brand consultants, its creatives who construct the user interaction, the application developer who creates the SMS interface, the application operator who runs the infrastructure that the SMS interface runs on, the application infrastructure provider who sends the actual text messages, and the network operator along whose network the text message is sent. Similar chains apply to internet telecommunications, and these organisational chains can also interact across different technologies – as would be the case, for example, in marketing campaigns involving services such as downloadable ringtones. Traffic data can move along these value chains, from the network operator to the application providers and operators, all the way back to the brand. At each point in these chains, the traffic data is captured and archived by the companies involved, sufficiently comprehensively that mining of this data can be listed on their books as a tangible asset. However, because the data has been anonymised – stripped of any subscriber name or address, but archivable by unique phone number (and in the case of opt-in mobile campaigns, also potentially by six-digit postcode) – companies without a billing relationship with the consumer are neither registered as data controllers, nor under data protection constraints as to their use of their traffic databases. As one telecommunications company executive put it:

We do not initiate SMS's ourselves… we send them on behalf of people who ask us to send them, therefore we know nothing at all about the permissions underlying these SMS's. We know nothing about the level of consent people have given, and we don't hold the personal information in any way, except interestingly enough we have huge registers. In reality we

[254] See Consumption and Profiling Expert Report

keep every keep every message that gets sent. So I actually know every message that has been sent to every phone over the last two years.[255]

Because the relationship between the mobile phone user and their phone number is *indexical*, the respondent's company was under no obligation to either register as a data controller or to delete their traffic data logs. The mobile phone is therefore regarded by consumers and the telecommunications industry as a personal communication device in so far as it is assumed to be connected to a particular individual (hence the value of the 'huge registers' and 'keeping every message that is sent'). This ability to enable interaction with users is what makes mobile data economically *valuable*. At the same time, the mobile phone number as *index* is treated as a non-individuated, non-personal piece of information. The index is nevertheless sufficiently precise to allow data mining techniques to precipitate personal data out of the supposedly non-personal data.

Telecommunications surveillance by corporate entities therefore potentially *sorts* consumers by their economic value to the organisation, and may do so on the basis of ostensibly a-signifying transmission data, as well as the billing data protected under Data Protection legislation. An additional complicating factor is that these value chains are potentially *global*. In the case of both mobile telephony and Internet provision, network operators and Internet Service Providers operate transnationally, with either subsidiary or contract organisations transmitting data between them. The challenge facing regulatory bodies therefore becomes even more complex.

Key Regulatory Issues and Challenges

The EU Data Retention Directive of 2006 lends urgency to a re-examination of relevant Data Protection legislation and the mechanisms through which it categorises data as 'personal'. Legislative initiatives from the Home Office to significantly extend the length of time for which data should be retained may mean that the mechanisms of state surveillance, and the extensive data-gathering practices of widespread telecommunications industry actors, may coincide in unprecedented ways.

One of the considerable difficulties facing telecommunications regulators is that different regulatory, state and organizational actors in the UK have diverse and overlapping remits. For example, telephone communication (depending on the communication) could be regulated under the auspices of three different regulatory bodies – the Office of Communications [Ofcom], the Independent Committee for the Supervision of Standards of Telephone Information Services [ICSTIS] or the Information Commissioner in the case of personal information and Data Protection. It might even be possible that it would fall under the remit of the Office of Fair Trading or the Advertising Standards Authority. In the case of Internet Communications, it is even more unclear where regulatory powers and responsibilities lie, especially given the globally distributed nature of the technology. All of these bodies have different remits, from regulating the abuse of personal information, to encouraging organisational competition in the telecommunications sector. Furthermore, these bodies treat data as 'information' or 'communication' – or as 'traffic' and 'personal' data – in different ways. With the increasing convergence and divergence of technologies, the greater reach and invisibility of telecommunications infrastructures, and the transnational character of telecommunications, the responsibilities and powers of these organisations, and their regulatory mechanisms, become increasingly confused, and the privacy implications of data-gathering more difficult to assess. Should, for example, Voice over Internet be treated as a phone call, and regulated as such? What regulatory organisation would have responsibility for

[255] Quoted in Green, N and Smith, S. (2003) ''A Spy in your Pocket'? The Regulation of Mobile Data in the UK' *Surveillance and Society* 1(4) 573-587.

ensuring the protection of the resulting data? Would it even be possible to regulate the use of this data across national boundaries?

In the extensive value chains surrounding data transmission, transmission data remains largely unregulated. Legislative measures have granted extensive powers to law enforcement bodies to scrutinise not only transmission data, but also personal data, the details of which are retained for ever-increasing periods of time. Even in commercial settings, transmission data is considered to be 'neutral' in terms of data protection, but nevertheless has considerable economic value. How transmission or traffic data currently circulate however, remains largely opaque to the data subjects to whom it pertains. There is little transparency or accountability with respect to this data on the part of for-profit organisations, no specific informed consent for these data to flow to numerous different organisations, and little or no choice in the matter for the data subjects concerned.

The telecommunications industry is ostensibly self-regulating, and there do exist a number of codes of practice, and codes of ethics, pertaining to different industry organisations encouraging compliance with Data Protection. These include those of the Direct Marketing Association, the Internet Telephony Service Providers Association, the Mobile Data Association or the Network for Online Commerce, to name a few. There are also consumer bodies organised to act on behalf of consumers and protect their interests (although this is largely after the fact) such as the Office of the Telecommunications Ombudsman, or Trading Standards authorities. There are few penalties for non-compliance in a self-regulating environment however, and there can be considerable economic rewards for quietly ignoring relevant legislation. Where Data Protection clearly applies, regulatory bodies can intervene and apply penalties for non-compliance. Where Data Protection is perceived not to apply however, as is currently the case in traffic or transmission data, organisations (in ever greater numbers) are entirely free to gather, store and manipulate what data they will (and are now required to retain it for longer periods of time). This clearly leaves the sector open to 'function creep' in the surveillance of telecommunications data, and where the state and corporate sectors are each extensively involved, data subjects have little power with respect to the ways their data are collected, stored, shared, bought or sold.

Expert Report: Workplace

Kirstie Ball
Open University Business School, UK.
k.s.ball@open.ac.uk

Introduction

Surveillance in the workplace refers to management's ability to monitor, record and track employee performance, behaviours and personal characteristics in real time (for example, internet or telephone monitoring) or as part of broader organizational processes (for example, drug testing in recruitment). Using the results of monitoring, conclusions can be drawn about employees' performance which have implications not just for their behaviour inside the workplace, but sometimes their lifestyle outside it. The range of techniques used varies from computer and telephone logging, to drug testing, mystery shopping, closed circuit television, mobility tracking and electronic recruitment. The widest range of monitoring techniques is found in the service sector, although manufacturing and some primary industries also monitor their employees. Whilst comprehensive figures as to the extent of employee monitoring do not exist, it is acknowledged that the internet is largely responsible for an increase in employee monitoring in the last five years. Proofprint and Forrester (2006) surveyed 294 US companies and found that more than a third with 1,000 or more workers employed people to read through other employees' outbound e-mail in search of rule-breaking[256]. 75% of US companies monitoring worker communications and on the job activities[257] and it has been estimated that 27 million online employees are monitored worldwide[258]. The gambling, retail, logistics and contact centre industries are noted for the exacting and extensive employee surveillance techniques they employ. Moreover because these industries have low union density, consistent opposition or resistance to surveillance is not widespread. Unions publish voluntary codes of practice for their members, but, with some exceptions, surveillance techniques are rarely the subject of collective bargaining.[259]

Any discussion of workplace surveillance begins with the idea that surveillance and business organizations go hand in hand, and that employee monitoring is nothing new. Clocking in, counting and weighing output and payment by piece-rate are all older forms of workplace surveillance. Business organizations are hierarchies, and hierarchies function by superordinate positions monitoring and controlling positions below them in the hierarchy. The word 'supervisor' – a common job title for those in charge of work processes - means 'overseer', and since the earliest theories of management, controlling and monitoring has been understood to be a central part of the task.[260] Histories of early large scale organizations emphasise how the development of information 'systems' gave businesses the ability to police their internal structures on a grand scale, and gain competitive advantage.[261] More

[256] Proofprint and Forrester (2006) Outbound Email and Content Security in Today's Enterprise. May 2006. http://www.caslon.com.au/privacyguide22.htm Accessed July 06
[257] Business Week July 10, 2000
[258] Schulman A (2001) The extent of systematic monitoring of employee email and internet use. www.sonic.net Accessed July 06
[259] CCTV in North America
[260] Henri Fayol (1916) *General and Industrial Management* Trans C Storrs 1949. London: Sir Isaac Pitman and Sons.
[261] Beniger, J R (1986) *The Control Revolution: Tecnological and Economic Origins of the Information Society*. Cambridge MA: Harvard University Press.

recently, a combination of available technologies and management culture which emphasises individual measurement and management has resulted in an extension and intensification of individual monitoring, rather than that of a group, department or business unit.

The implication is that surveillance at work is, first, a necessity and, second, a normal, taken for granted element of working life. Employees expect to have their performance reviewed, objectives set, and information gathered on their activities and whereabouts – indeed this is good management practice. Controversies generally arise when employee monitoring goes beyond what is reasonable or necessary: when employers use intrusive monitoring to delve into the lives employees lead outside work, and when they demand exacting and precise information as to how employees use their time. As such, workers can simultaneously support some of the protective aspects of surveillance and oppose some of its more intrusive aspects. This makes understanding resistance to surveillance difficult, when it comes to identifying what is legitimate and what is not. A further concern is the lack of specific policy provision by employers, a lack of audit or review as to how employee information is used, and a subsequent lack of awareness of monitoring practice and policy on the part of employees. The following pages will explore the form, function and consequences of employee monitoring, as well as exploring some of their regulatory implications.

Key developments

This section will begin by reviewing the range of surveillance practices undertaken by organizations. It will then explain the reasons why organizations monitor their employees, and discuss some of its less savoury consequences. Whilst surveillance is always applied for the benefit of the business, and is hence not politically neutral, it is shaped by various contextual factors, and these will also be presented. Finally, some future developments will be discussed.

The diagram overleaf shows the range of surveillance practices which occur in the workplace. The practices focus on measuring employee performance, their behaviours or their personal characteristics. Monitoring of performance and behaviours as part of ongoing production processes is more likely to take place in real time. The monitoring of personal characteristics is more likely to occur as a one-off event as a way of controlling access to the organization. This may take the form of physical access to organizational premises, or access to roles within the organization through recruitment. The monitoring of personal characteristics is more pervasive because of the conclusions employers can draw about the lifestyles of their employees, and this raises questions as to the extent to which employers have a right to use this information. A further aspect of workplace surveillance which is illustrated by this diagram is function creep. Whilst this will be discussed later in the report, the diagram clearly highlights how one particular surveillance technique can reveal more than one kind of information about employees. For example, use of mystery shoppers will not only tell managers how well retail staff are performing their tasks, but will also reveal information about how they behave towards customers and each other.

Whilst the diagram focuses on techniques and tools which can be used by management, other forms of surveillance exist in the workplace which are just as pervasive and much less easily identifiable or regulated. Sewell (1998) highlights how, with the rise of team working, peer surveillance (watching one's colleagues' performance, behaviours or characteristics interpersonally) reinforced through social norms and culture is growing.[262] Surveillance techniques used in peer-to-peer evaluation lend rationality to the assessment process. Self-discipline and self-surveillance are also central to management systems which aim to

[262] Sewell, G (1998) The discipline of teams: The control of team-based industrial work through electronic and peer surveillance. *Administrative Science Quarterly* 43 (2) pp 397 - 428

‘empower’ their staff and encourage them to be enterprising, creative and innovative. This means that organizations now use a raft of surveillance-based techniques that are not only embedded within specific tools, but also within the social processes of managing. Surveillance in the workplace not only produces measurable outcomes in terms of targets met or service levels delivered, but also produces particular cultures which regulate performance, behaviours and personal characteristics in a more subtle way.

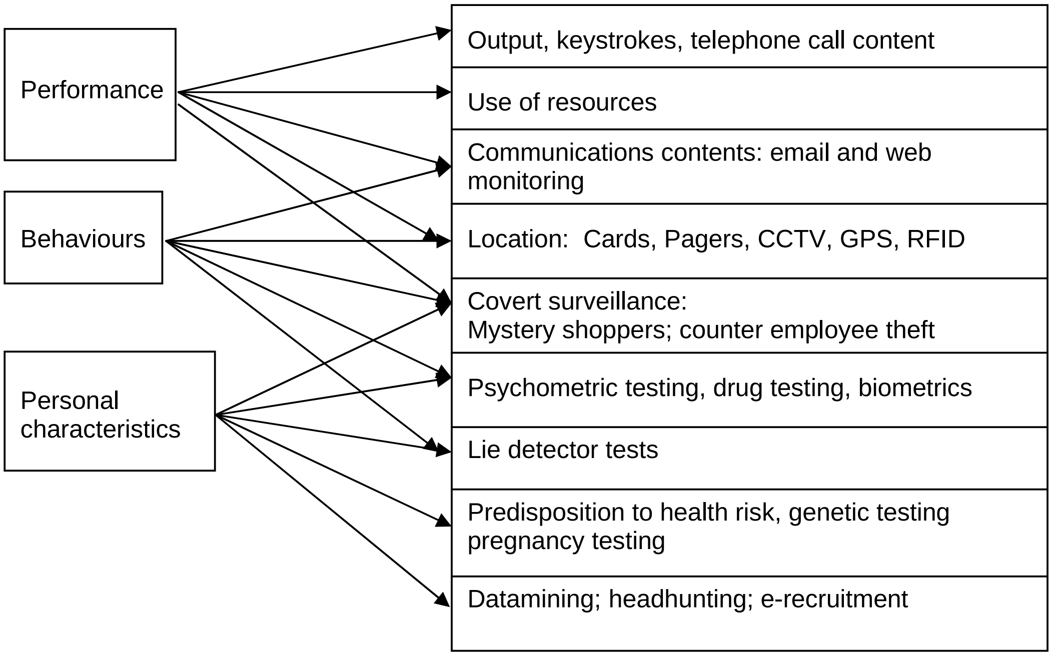
Performance
Behaviours
Personal characteristics
Output, keystrokes, telephone call content
Use of resources
Communications contents: email and web monitoring
Location: Cards, Pagers, CCTV, GPS, RFID
Covert surveillance: Mystery shoppers; counter employee theft
Psychometric testing, drug testing, biometrics
Lie detector tests
Predisposition to health risk, genetic testing pregnancy testing
Datamining; headhunting; e-recruitment

Figure one: The range of employee surveillance techniques used by organizations (adapted from Regan 1998[263]).

Surveillance in the workplace is developing in three directions: the increased use of *personal data, biometrics* and *covert surveillance*. The use of actual and potential employees’ *personal data* has grown in recent years with the widespread use of Human Resource Information Systems.[264] Within organizations, survey evidence has indicated that electronic employee records are used in fairly routine ways and the data are not subject to a great deal of analysis or manipulation. However, with internet based recruitment on the rise, some companies now engage in data-mining of CV databases and electronic snooping on potential candidates and competitors’ websites.[265] Third party providers have now emerged who will conduct these kind of searches for employers. Increasingly covert means are being used to search for potential applicants by accessing user chat rooms, or gain covert access into organisation’s intranets (termed “flipping”). E-recruitment is growing in the UK, but in 2004 only 7% of the total recruitment market was internet based.[266] In the US there are 20 million CVs stored in databases and the US internet recruitment industry has attained the dubious accolade of being the second largest source of income for providers after pornography.[267] Whilst RFID tags are controversial in themselves when used for location tracking,[268] the tags are also linked to records in time and attendance databases, which are typically part of larger Human Resources

[263] Regan, P (1998) Genetic testing and workplace surveillance: Implications for privacy. In Lyon, D and E Zureik (eds) *Computers, Surveillance and Privacy.* Minneapolis: University of Minnesota Press.
[264] Ball, K., (2001) 'The use of Human Resource Information Systems: a survey', *Personnel Review*, vol. 30, no. 6, pp. 677-693
[265] Searle, RH (2002) Organizational justice in E-recruiting: Issues and controversies. *Surveillance and Society* 1 (2)
[266] Corsini, S (2001) Wired to hire *Training* 38 (6) 50 - 55
[267] Kay, AS (2000) Recruiters embrace the internet *Information Week* Iss 778 pp 72 -76
[268] http://www.theregister.co.uk/2005/07/19/rfid_gmb/ accessed July 06

databases. Recent research has highlighted that the uses of these data are not made clear to employees, policies outlining their use are not in place, and information practices are not subject to any third party audits or checks.[269]

The same is true if *biometric information* (e.g. retina and iris scans, electronic fingerprinting, hand geometry, and drug and alcohol testing) is to be used for access control, recruitment or promotion purposes. Biometrics are now seen by employers as one of the ways in which the identity of employees can be authenticated, and as a way of managing health and safety in the workplace. Like e-recruitment, drug and alcohol testing is growing in the UK and is used where employees are in safety-critical jobs (eg driving vehicles). In the USA it is far more widespread but has recently started to decline because of the lack of evidence that it improves safety or productivity. Because drug testing is seen by many as a violation of bodily privacy it deters many from applying for jobs where they are likely to be tested. Moreover drug tests do not distinguish between heavy and recreational drug users and abstinence a few days before the test will usually yield a negative result.[270]

Informing and involving employees in monitoring practice is difficult if an organization wants to employ *covert surveillance* techniques to monitor internet activity, service levels or competitor behaviour. Particularly with the emergence of the blogosphere, organizations are keen to protect themselves from defamation, and employees' web activities are checked for offensive or libellous content, sometimes even when they are posted on private servers outside company time. Cases are now beginning to be heard by employment tribunals from applicants who have been dismissed for blogging about their employer.[271] The Electronic Frontier Foundation has now published a set of guidelines telling bloggers how to preserve their anonymity so they can avoid being fired.[272] Employers' capacity to record and store employee communications raises privacy concerns, first because private conversations may contain confidential information (e.g. a credit card number), second because this information may be stored on offshore servers which fall under different jurisdictions, and third because of the relative coverage and broadcast of relevant policy. Appropriate policy is difficult to define in respect of covert surveillance. There is some debate as to whether organizations are required to provide a general notice to staff that they may be subject to it, or whether this can be avoided altogether. In Australia, for example, employers are required to get permission to conduct covert surveillance on employees from a magistrate. In the UK, under RIPA 2000, if the business is protecting a 'legitimate interest' it can covertly intercept employee communications, although it does have to comply with Data Protection Act requirements too. In the case of mystery shopping, for example, opinion is split between those who argue that the practice is unethical because of the levels of deceit, compromise and the lack of consent involved.[273] Others argue that employers need to present the results of mystery shopping to staff, to raise awareness of it in a way which will not compromise the research.[274]

At a more general level, and given that surveillance is central to organizational life, there are three main reasons why employers monitor their employees:

- To maintain productivity and monitor resource use;

[269] Balkovich, E., T. K. Bikson, and G. Bitko. (2005). *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace*. Washington DC: Rand Corporation, Report

[270] Drug tests merely indicate the presence of various recreational drugs. Commentators refer to them as 'intelligence tests': to fail one the candidate would need to be very stupid!

[271] http://commentisfree.guardian.co.uk/catherine_s/2006/07/sec_gets_dooced.html accessed July 06

[272] http://www.eff.org/Privacy/Anonymity/blog-anonymously.php accessed July 06

[273] Shing, MNK and Spence, L (2002) The limits of competitive intelligence: Is mystery shopping ethical? *Business Ethics: A European Review* 11 (4) pp 343 - 353

[274] Wilson, AM (2001) Mystery shopping: Using deception to measure service performance *Psychology and Marketing* 18 (7) 721 - 734

- To ensure security by protecting corporate interests and trade secrets. Email, internet monitoring and information access control are all deployed against risks of defamation, sabotage, data theft, and hacking.
- To protect the company from legal liabilities. The results of employee monitoring can provide evidence in legal actions and monitoring can become a risk management tool.

Businesses, therefore, use employee monitoring to limit cost and risk, protect value and maintain quality. Excessive monitoring, however, can be detrimental to employees for the following reasons:

- Privacy: the collection of employees' personal information and other information about their lives can compromise privacy if employees do not authorise the disclosure of their information and it is broadcast to unknown third parties.[275]
- Function creep: employee monitoring technologies can sometimes yield more information than intended, and management must avoid the temptation to extend monitoring practice without consulting employees first. This is particularly important if the information is being used in decisions about pay or promotion.
- Creativity: if employees realise their actions and communications are monitored, creative behaviour may be reduced if employees are worried about monitoring and judgement.
- Social control: Exacting surveillance sends a strong message to employees about the kind of behaviours the employer expects or values. This can produce 'anticipatory conformity'[276] – employees behaving in a docile and accepting way, and automatically reducing the amount of commitment and motivation they display. Trust levels are also at risk of being reduced.[277]
- Resistance and sabotage: excessive monitoring can sometimes produce the behaviours it was designed to prevent. If workers perceive surveillance practices as an intensification and extension of control, it is likely that they will try to subvert and manipulate the boundaries of when, where and how they are measured.[278] This has been well documented in call centres. Here, workers are extensively monitored not only in terms of their quantitative outputs, but also their qualitative manner on the phone, and their overall competence. They work their way around surveillance by:
  - manipulating measures by dialling through call lists, and leaving lines open after the customer has hung up
  - pretending to talk on the phone
  - providing a minimal response to customer queries
  - misleading customers

  Where call centre managers are under surveillance, they sometimes collude with workers to produce the desirable results.

Research has widely acknowledged that the relative effects of surveillance on employees are not a foregone conclusion and are shaped by a number of factors. These factors concern the

[275] The extent of email monitoring and the privacy and ethical it raises, for example, are discussed in lay terms by Lloyd, J (2006) Management Email monitoring brings Big Brother to mind. *Receivables Report for Americas Health Care Financial Managers* 21 (1) pp 6 - 7

[276] Zuboff, S (1988) *In the Age of the Smart Machine* New York: Basic Books

[277] A qualitative study by Alan Westin in 1992 – see note 22 for the full reference – observed that poor management communication and their failure to implement monitoring in a participatory way damaged trust relations. However, there have, as yet, been no systematic studies which measure the trust impact of increased surveillance. This is primarily because of difficulties in measuring trust as a variable. Studies of call centres, however, demonstrate that intense surveillance increases resistance, sabotage and non-compliance with management. For examples see Frenkel S et al (1998) Beyond bureaucracy? Work organization in call centres. *The International Journal of Human Resource Management* 9 (6) and Callaghan, G and Thompson, P (2002) We recruit attitude: The selection and shaping of routine call centre labour *Journal of Management Studies* 39 (2)

[278] For an empirical example of factory workers damaging a new CCTV system see McCahill and Norris (1999) Watching the workers: Crime, CCTV and the workplace. In: P Davis, P Francis and V Jupp (eds) *Invisible Crimes: Their Victims and their Regulation.* London: Macmillan

way in which supervisors and managers design work in such a way as to limit or balance the emphasis on monitoring, and how they relate to their employees during the monitoring process. Stanton (2000) outlines how task design, supervisory style, and employee cognition of monitoring are all important. He also shows how the organizational characteristics can affect how monitoring is carried out.[279]

Aspects of *task design* concern whether the employee has a choice in the pace and timing of their tasks or not. Further, monitoring which is constant is likely to have more of an adverse effect than if it is intermittent and at regular intervals. Monitoring also has to be appropriate for the task: if the task is easily measurable, then it is easily monitored, and any aspects which are difficult to measure must be evaluated in other ways. Similarly if the employee is measured as part of a group, rather than as an individual, monitoring will be less stressful for the individual. More importantly, the person doing the monitoring should be tuned in to the psychological and emotional states of the employees rather than passing any blanket judgement based on figures alone. [280][281] [282] [283]

Supervisory style is extremely important. Keeping an open mind as to performance fluctuations is a good starting point as previous research has shown that if a supervisor rates an employee negatively using monitoring, they are less likely to revise that judgement.[284] As such, the results of monitoring should be balanced by other wider feedback processes, such as appraisal and coaching.[285] Assigning a heavy workload to monitored tasks will result in stress, as will an approach to feedback which punishes, rather then develops staff in the event of performance shortfalls.[286] Supervisors also need to communicate monitoring criteria clearly,[287] and ensure employees are adequately trained so that they have a fair chance of hitting their targets.[288] Involving employees in the design and implementation of monitoring systems[289] will ensure that it has a better chance of being accepted, and being absolutely clear about where the monitored information goes and how long it is kept for helps.[290] Nevertheless Marx et al (1988) warns against the persuasive rhetoric used by managers to

[279] Stanton, J (2000) Reactions to employee performance monitoring: Framework, review and research directions *Human Performance.* 13 (1) pp 85 - 113

[280] Stanton, JM and BarnesFarrel, JL (1996) Effects of electronic performance monitoring on personal control, satisfaction and performance. *Journal of Applied Psychology* 81 738 - 745

[281] Niehoff, BP and Moorman, RH (1993) Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behaviour. *Academy of Management Journal* 36 527 - 556; Aiello, JR and Kolb, KJ (1995) Electronic performance monitoring: A risk factor for workplace stress. In SL Sauter and LR Murphy (eds) *Organizational Risk Factors for Job Stress* pp 163 – 179. Washington DC: American Psychological Association; Lund, J (1992) Electronic performance monitoring: A review of the research issues *Applied Ergonomics* 23, 54 - 58

[282] Aiello, JR and Kolb, KJ (1995) Electronic performance monitoring: A risk factor for workplace stress. In SL Sauter and LR Murphy (eds) *Organizational Risk Factors for Job Stress* pp 163 – 179. Washington Dc: American Psychological Association; Chalykoff, J and Kochan, T (1989) Computer-aided monitoring: Its influence on employee job satisfaction and turnover *Personnel Psychology* 42, 807 - 829

[283] Aiello, JR and Kolb, KJ (1995) Electronic performance monitoring: A risk factor for workplace stress. In SL Sauter and LR Murphy (eds) *Organizational Risk Factors for Job Stress* pp 163 – 179. Washington Dc: American Psychological Association; Brewer, N (1995) The effects of monitoring individual and group performance on the distribution of effort across tasks. *Journal of Applied Social Psychology* 25, 760 - 777; Larson, JR and Callahan, C (1990) Performance monitoring: How it affects work productivity. *Journal of Applied Psychology* 75, 530 - 538; Brewer, N and Ridgeway, T (1998) Effects of supervisory monitoring on productivity and quality of performance. *Journal of Experimental Psychology: Applied*, 4, 211 - 227

[284] Kulik, CT and Ambrose, ML (1993) Category and feature-based processes in performance appraisal: Integrating visual and computerised performance data. *Journal of Applied Psychology* 78 (5) pp 821 -

[285] Amick, BC and Smith, MJ (1992) Stress, computer based work monitoring and measurement systems: A conceptual overview *Applied Ergonomics* 23, 6 - 16

[286] Carayon, P (1993) Effects of electronic performance monitoring on job design and worker stress: results of two studies. *International Journal of Human Computer Interaction* 6, 177 - 190

[287] Nebeker, DM and Tatum, BC (1993) The effects of computer monitoring, standards and rewards on work performance, job satisfaction and stress. *Journal of Applied Social Psychology* 23, 508 - 536

[288] Ibid.

[289] Westin, AF (1992) Two key factors that belong in a macroergonomic analysis of electronic monitoring: Employee perceptions of fairness and the climate of organizational trust or distrust. *Applied Ergonomics* 23, 35 – 42.

[290] Aiello, JR and Kolb, KJ (1995) Electronic performance monitoring: A risk factor for workplace stress. In SL Sauter and LR Murphy (eds) *Organizational Risk Factors for Job Stress* pp 163 – 179. Washington DC: American Psychological Association

gain acceptance of monitoring practices.[291] Also, if employees' job security is threatened then it is unlikely that more monitoring will be welcomed.[292]

Cognitive factors refer to employees' predispositions towards monitoring itself. If employees have a prior level of trust in their supervisors, monitoring is less likely to be stressful.[293] However if employees perceive monitoring as something which is invasive of privacy,[294] is unreasonable[295] or places too much emphasis on reward[296] – in other words if they feel they have a lot to lose or gain by monitoring - then the opposite effect will occur. Supervisors should also be careful how they emphasise the importance of monitored tasks in relation to other, non-monitored tasks. This applies equally to different elements of the same task, and the relative intensity of monitoring between different tasks.[297]

Broader *organizational factors* extend beyond the realm of the task and address the things that might cause an organization to monitor its employees closely in the first place. Attewell (1987) argues that when an organization is competing in a mature product market with mature technologies, and competing on the basis of price, and producing high quantities of similar goods there is more of an incentive for it to keep a close eye on resource use and employee activity[298]. Similarly, if there is an abundant supply of labour and low unionisation (as in the case of some call centres), close monitoring is likely to meet with less opposition and resistance. If the organization's culture does not support a developmental approach to its employees, then it is likely that work and monitoring will be punitive and militaristic.

Whilst many of these findings were generated through the study of performance monitoring technologies it is likely that they could be applied to the use of any surveillance technique at work. Principles concerning task design, communication and supervision, employee expectations and the organization's position represent a set of parameters by which the operation of any workplace surveillance technique can be understood. Moreover, they present a set of practical guidelines by which managers can shape surveillance in a way which is less harmful to worker health and well being. It may also indicate to regulators the aspects of workplace surveillance which may be tackled by codes of practice, or be included in a privacy impact assessment. Indeed new developments in workplace surveillance which extend it beyond organizational and personal boundaries make guidelines for good practice all the more salient.

Critical commentary and future directions

The previous discussion concerning the key developments in workplace surveillance techniques highlighted a number of basic points:

- Organizations and surveillance go hand in hand
- Workplace surveillance takes technological and social forms
- Workplace surveillance is primarily implemented to protect company assets

[291] Marx, G T (1990) The Case of the Omniscient Organization. *Harvard Business Review*. March – April pp 4 - 12

[292] Hales, TR et al (1994) Musculoskeletal disorders among visual display terminal users in a telecommunications company *Ergonomics* 37, 1603 - 1621

[293] Strickland, L (1958) Surveillance and trust *Journal of Personality*. 26, 245 - 250

[294] Office of Technology Assessment (1987) *The Electronic Supervisor: New Technologies, New Tensions*. Washington DC: US Congress Office of Technology Assessment

[295] Niehoff, BP and Moorman, RH (1993) Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behaviour. *Academy of Management Journal* 36 527 - 556;

[296] Brewer, N (1995) The effects of monitoring individual and group performance on the distribution of effort across tasks. *Journal of Applied Social Psychology* 25, 760 - 777

[297] See note 15

[298] Full reference Attewell.P (1987) Big brother and the sweatshop: Computer surveillance in the automatic office *Sociological Theory* 5 pp 87 - 99

- Workplace surveillance has the potential to affect employee well being, work culture, productivity, creativity and motivation detrimentally
- Managerial attention to task design, supervisory processes, employees' expectations about monitoring, and an appraisal of the company's operating environment can mediate its downsides
- Personal data gathering, internet and email monitoring, location tracking, biometrics and covert surveillance are all areas of development

This section of the report integrates these points into a discussion of the broader issues with which this project is concerned: issues (privacy, ethics and human rights; choice, power and empowerment; transparency and accountability; social exclusion) and processes (data flow; social sorting; function creep; technology) common to all surveillance practices.

Privacy; ethics and human rights issues are endemic to workplace surveillance. For example does the public nature of blogging trump any employee privacy rights, even if an employer discovers an employee blog through the covert surveillance of their internet activity outside the workplace? Moreover does the lack of due consultation on the introduction of biometric surveillance, or indeed any kind of surveillance which crosses new bodily or personal boundaries, mean that employees have to comply with it? When discussing privacy issues in this domain, it is important to focus on the full range of privacy concepts: privacy and the human body, privacy in social relations, and privacy and personal space as well as information privacy[299]. It is also important to consider fully the implications of disclosure: whether the employee had given their authority for boundaries relating to their body, social relationships, personal space and information to be crossed; and whether they were aware of who was going to be party to that information. As well as challenging privacy rights some of these employment practices also challenge rights concerning the freedom of expression. Surveillance also has particular employment ethics implications. Using the concepts of distributive and procedural justice surveillance practices are likely to be more controversial if they undermine existing processes of consultation, and have an impact on the relative distribution of reward. [300] [301]

Allied to questions of distributive and procedural justice are questions of c*hoice, power and empowerment*. Of particular interest in the employment relationship is the role of surveillance (and its intensification) within the effort-reward bargain between employer and employee.[302] This is significant because of the way in which modern management discourse emphasises the importance of metrics, evaluation and review in practically every area. So, if an automatic upgrading of an access control system to biometrics is perceived by employees as an intensification and extension of control, their attitude and motivation to work may well be adversely affected. Ensuring adequate and responsible consultation is a bare minimum if employment relations are not to be adversely affected. This is also the case for call centre employees have little control over work pacing, system speed or task design and yet can be disciplined if the system indicates they are not complying with agreed standards. A more sinister facet of choice, power and empowerment arises when we step back and look at who is usually the subject of monitoring. In the early 1990s The US National Association of Working Women conducted a survey of call centre workers and ran a telephone helpline for stressed out workers. [303] They concluded that surveillance is generally (but not always) used

[299] Privacy International and Electronic Privacy Information Center, (2003) *Privacy and Human Rights 2003. An International Survey of Privacy Laws and Developments*

[300] Distributive justice refers to the equity of reward (material or otherwise) for effort and punishment for non effort and procedural justice refers to matters of of employee voice, communication, trust, involvement and mutual responsibility between management and workers for performance

[301] Ball, K., (2001) Situating workplace surveillance: ethics and computer based performance monitoring *Ethics and Information Technology*, vol. 3, no. 3, pp. 211-223

[302] The effort-reward bargain is the compromise made amount an employer is prepared to pay as against the view of the employee about how much s/he is worth and hence the effort they put into their work

[303] Nine to Five (1986) *Computer Monitoring and Other Dirty Tricks*. Cleveland: National Association of Working Women

at the bottom of organizations to cover high volume service and manufacturing operations, and because of the nature of occupational structure, then electronic monitoring is said to cover disproportionately large amounts of female and minority workers. When female workers felt unfairly treated under this technology, they frequently used images such as rape or sexual abuse to describe how they felt. Ultimately the intensification of workplace surveillance confers massive benefits on the employer, but relatively little benefit on the employee.

To promote the *transparency and accountability* of surveillance practices it is nearly always advisable for employers to explain, either through training, workshops or policy, the extent of the surveillance measures being used, what is done with the data, and for how long the data will be kept. Access control technologies are particularly interesting, because of their connectivity with personnel systems. For example, in the case of one relatively new technology, RFID tagging for access control, research demonstrates how it is relatively easy for companies to overlook the requirement for explicit policy on data use. One study found that only one organization in their sample used RFID simply to control access.[304] Other uses included compliance with work rules about hours, monitoring absence levels following a merger of two companies, as well as attendance behaviour. Several things were apparent from the cases. First, that linkage with other personally identifiable data is commonplace – and it's typically integrated with other forms of surveillance data. Second that linkage with video cameras was also commonplace. Third, that linkage of RFID data with personnel records helps allegations of misconduct. Fourth that linkage with medical records is motivated by public safety requirements. Fifth, that access control records are maintained indefinitely. Sixth, that employees were not likely to know about policies with RFID access control and finally, security and public safety concerns outweigh privacy concerns.

Whilst it is difficult to draw conclusions about workplace surveillance and s*ocial exclusion*, mainly because of the pre-existing occupational and social structural determinants of labour markets, one area of workplace surveillance is beginning to stratify opportunities for employment: e-recruitment. Sifting through large volumes of CVs and searching for potential candidates raises the question of discrimination in two ways. First, that, in a similar manner to traditional recruitment processes, e-recruitment is subject to decisions the biases and 'rules of thumb' used by recruiters when they face complex choices between a range of candidates.[305] Left unchecked, such biases may develop into the exclusion of particular groups of candidates from recruitment processes through the use of particular keywords, and hence leaves the organization open to discrimination claims. Keyword searches are now routinely being used as selection tools, and observe that the use of particular keywords varies between recruiters, and hence yields different results.[306] Whilst it may be argued that eliciting the right results with particular keywords is indicative of the professional expertise and tacit knowledge of the recruiter, it may also reflect their own biases. Further complexity arises when one considers that CV writing skills vary so much between candidates. The use of standard forms goes some way to remedy this problem, as well as the use of multiple words to search for a qualification, as well as tight policy regulation of the practice.

Second, it is discriminatory in the sense that certain social, economic and ethnic groups do not have easy access to the internet. Hence a concentration on e-recruiting effectively excludes these groups from the labour market altogether. Whilst many niche websites have now developed, initially its use was directed towards white, male middle class occupations in IT and engineering.[307] There is a strong temptation for companies to standardise and formalise e-

[304] Balkovich, E., T. K. Bikson, and G. Bitko. (2005). *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace*. Washington DC: Rand Corporation, Report

[305] Tversky, A and Kahneman, D (1974) Judgement under uncertainty: Heuristics and biases *Science* 185 (4157) pp 1124 - 1131

[306] Mohamed, AA, Orife, J and Wibowo, K (2002) The legality of key word search as a personnel selection tool *Employee Relations* 24 (5)

[307] Sharf, J (2000) As if g-loaded adverse impact isn't bad enough, internet recruiters can be expected to be accused of 'e-loaded' impact. *The Industrial-Organizational Psychologist.* 38:156

recruitment processes which will yield 'more of the same' rather than a diverse set of applicants. Indeed Marconi Capital revised its e-recruitment strategy when they found that it didn't attract the ethnic or social mix of people they wanted and it has also been reported that women were more likely to deselect themselves from online recruitment processes because of its impersonal nature.[308] [309] The UK disability rights commission investigated 1000 websites and found that 81% failed to satisfy the most basic web accessibility guidelines, which means that 8/10 websites in the UK exclude 1.3 million people of working age applying for jobs online.[310] Explicitly using varied recruitment channels, advertising on diversity websites, and reflecting diversity requirements are key steps organizations can take.

The experience of workplace surveillance exhibits some common processes with other areas of surveillance. Internet and email surveillance, and e-recruitment trigger new *data flows* into the organization about its labour markets, the activities and interests of its employees, and even cause new connections to be made between customer and employee data. Whilst e-recruitment has *social sorting* implications, this area is also of relevance in the call centre industry. Call centres now rank order customer accounts according to their relative spend. The higher the spend, the greater the customers value is to the organization, and so when these customers call for service, they are routed into shorter queues and answered by more skilled employees. Moreover, the customer profile is seen as critical when recruiting call centre employees, who are now assessed for social and lifestyle competencies which match those of the market segment they are serving. *Function creep* is a concept which has occurred a number of times in this discussion. Anecdotal accounts of workplace surveillance and recent research both document how it is relatively easy for management to use one surveillance technique in a number of ways. In a similar manner to other areas, the *technology* used for surveillance in the workplace is gradually decreasing in size, and increasing in processing power. There is now a growing ability to track actual and potential workers beyond the boundaries of the workplace in real time, either by the attachment of a physical transmitter about the person, or by the predictive conjecture of data analysis. Moreover organizations are now seeking to probe the bodies of workers for authentication, security and safety purposes.

Regulatory issues

Regulating workplace surveillance raises a number of dilemmas for regulators. The first concerns the question of whether workplace surveillance can be the target of regulation at all. The second concerns the extent to which certain parts of management practice can be the target of regulation, and the third concerns the legal frameworks which should actually be applied. After reviewing these three dilemmas some ideas regarding the development of Privacy Impact Assessment will be presented.

Whether workplace surveillance should be regulated at all infers a dilemma often discussed in legal circles concerning workplace privacy. This dilemma is whether to take a *property based* or *rights based* approach to regulation. The former argues that everything that happens on company property and in company time is a legitimate target for management and control, essentially giving management the right to monitor as they wish. The latter refers to establishing privacy as a worker right which can be protected from management control. A third way, proposed by the Victorian Law Reform Commission in Australia is the recognition that there are various privacy *interests* that need to be protected. In other words that privacy in the workplace is not an inalienable right but neither is it completely appropriable by management.

[308] Smethurst, S (2004) The allure of online *People Management* 10 (15) pp 38 - 40

[309] Czerny, A (2004) Log on turn off for women *People Management* 10 (15) p10

[310] See note 49

The second point concerns the elements of management practice which should be subject to regulation. Earlier in the report it was suggested that watching the workforce is more appropriate where companies are trying to protect themselves from legal liability. This is the current rationale behind the acceptability of drug testing, for example,[311] and is frequently the reason for the installation of CCTV in the workplace.[312] Function creep, however, can cause these technologies to be used in ways beyond that for which they were originally installed. If a technique was originally used to monitor employee theft and then becomes a vehicle for monitoring performance, legal justifications for surveillance are replaced by organization-specific justifications. This raises the question of whether micro-management techniques should ever be the subject of regulation. Furthermore, many of the adverse impacts of workplace surveillance are intangible (for example, increased social control, decreased trust relations, increased resistance and sabotage), and hence difficult to identify in any objective sense. However it is these consequences which prove most problematic for businesses and employees in that they are likely to cause increased turnover, decreased job satisfaction and problems with productivity and quality.

The final dilemma concerns how a surveillance-based regulatory framework would dovetail with other legal frameworks which are currently applied to work. In the UK, for example, regulation navigates territory between legislation concerning workplace consultation and collective bargaining, Data Protection legislation concerning the use of personal data, human rights legislation concerning the rights to privacy and freedom of expression, RIPA's Lawful Business Practice regulations concerning the interception of communications and case law concerning the implicit and explicit terms of the employment contract. Crucially, key regulatory concerns should be associated not just with protecting the data which are the inevitable outcome of employee surveillance, but also ensuring the surveillance processes are fair, transparent, open to challenge and do not impinge on the dignity of individual employees.

Current DPA guidelines for assessing the impact of workplace surveillance concern proportionality (i.e. whether the surveillance is adequate, relevant and not excessive), as well as identifying its adverse impacts, available alternatives, and existing business obligations. In terms of populating an impact assessment and thoroughly addressing adverse impacts, the author recommends reference to the 1996 ILO guidelines on surveillance. Whilst it is acknowledged that these are incorporated into the UK Employment Code, other jurisdictions developing regulation in this area could use this as a starting point. There are two concerns with current regulatory frameworks, however. The first major limitation is that current guidelines for assessing the impact of workplace surveillance rests on too narrow a definition of privacy. Whilst information privacy is very well covered, the implications of workplace surveillance for bodily privacy, privacy of social relations and privacy of personal space are nowhere to be found. The second is that regulation based on notice, such as in the Workplace Surveillance Act (NSW) 2005 (Australia), and in the United States' case law offers inadequate protection for employees as employers can claim compliance merely by exhibiting the correct signs in public areas.

Moreover, because of the more intangible effects of workplace surveillance on employees, it is recommended that impact assessment be conducted longitudinally. As such it is a management toolkit could be developed to accompany a PIA. This toolkit would contain standardised survey instruments to assess the impact of surveillance on workplace culture, trust and communication levels, turnover and absence levels. In addition it would also contain a manual recommending consultation and communication techniques concerning surveillance, and outlining best practice in performance management. This could be

[311] http://www.yourrights.org.uk/faqs/workplace-faqs/employer-wants-to-drug-test.shtml accessed July 06

[312] McCahill, M and Norris, C (1999) Watching the workers: Crime, CCTV and the workplace. In: P Davis, P Francis and V Jupp (eds) *Invisible Crimes: Their Victims and their Regulation.* London: Macmillan

accompanied by blended online and training resources to assist companies in their compliance endeavours, and to enable them to comprehend fully the impact of surveillance practices on their employees.