Spies in the Information Economy: Academic Publishers and the Trade in Personal Information

David Murakami Wood[1]

Department of Sociology, Queen's University, Canada
Email: dmw@queensu.ca

Introduction

Academics work within a complex network of institutions, and publishers are prominent in this network. But publishers are no longer the simple entities they once were in the Gutenberg galaxy. As the Reed Elsevier controversy shows, academic publishers can now be merely parts of large impersonal transnational information brokers, whose interests can extend from humanitarian medical journals to the provision of conferencing facilities for the arms trade[2]. It is not surprising that commercial publishers should seek to 'add value' to whatever assets they have and can obtain. However, it is not so much the raw materials (data) or material products of old-fashioned information sharing (books and paper journals) that provide this added value, but various forms of combination, mixing and

[2] This centres around Reed Elsevier's subsidiary, Reed Exhibitions, http://www.reedexpo.com/ the self-described 'world's leading events organiser,' and its involvement in promoting the arms trade through its defence export exhibitions. It was Richard Smith, former editor of the Lancet and the other doctors and medical researchers whose campaign really worried Reed Elsevier (see Dyer, 2007). Some geographers played a supporting role. Despite promises to withdraw from this trade, the company had still not done so by the end of 2007 (*Sunday Times*, 2007)

manipulation of data, including the growing trade in the products of surveillance: information about individuals and groups.

Information is a commodity because it provides advantage and, coupled with categorisation, can generate new knowledges (Bowker and Star, 1999). The generation, ordering and circulation of such knowledges do not simply serve the purposes of power but are the very things that constitute it. This understanding of the nature of information was used to develop new ideas of how subjectivity could be managed in institutions, exemplified by the apparatus of the Panopticon (Foucault, 1977), and it was in this context that Giddens (1985) and Dandeker (1990) argued that surveillance was a key pillar of modernity. However in the new form of capitalism charted by Castells (1996-8), the circulations of information themselves provide the sources of profit, and the databases that store this information, the apparatus of 'new surveillance' (Marx, 1988) in a 'control society' (Deleuze 1991). James Rule (1973) sketched out their potential at around the same time that Foucault was working on its prehistory, but it wasn't until Clarke (1988) coined the term 'dataveillance', that we started to get a sense of what this would mean.

Dataveillance does not displace surveillance, rather it intensifies and changes it. Computer databases enable the automated storage and categorisation of information. The effects are manifold but most importantly the humane objectives of panoptic surveillance become indirect or are entirely stripped away (Lianos, 2001, 2004): whereas the Panopticon was concerned with 'soul-training', post-panoptic surveillance requires no intention to generate a particular subjectivity, rather it is concerned only with the maintenance of orderly flows. This does not mean that databases are apolitical, but these politics are often hidden in the development of the algorithms that make up database software (Graham and Wood, 2003).

Databases do several things. They allow the ability to 'mine' data, to make associations between different bits of information to create entirely new knowledge of the individual or group (Gandy, 1993). Data mining, can be defined as "a process which has as its goal the transformation of raw data into information which can be utilized as strategic intelligence within the context of an organisation's identifiable goals" (Gandy, 2006: 364). Often called 'Knowledge Discovery in Databases' (KDD) (see: Pridmore, 2006), this reflects the crucial distinction that Gandy highlights between data mining and simple information retrieval.

Databases make associations through the combination of different data. These associations can then be correlated to existing knowledge of behaviour, or to existing categorisations. For example, changing patterns of purchasing on a debit card can indicate lifestyle changes or pay increases, even pregnancy or sexuality. The accumulated categorisations of individuals and groups form the basis of profiles, used to compare one individual or group to another. In policing, this

manifests itself in 'categorical suspicion,' where individuals are suspect because of the resemblance of their profiles to other existing criminal profiles (Norris, 2003). This can also mean categorical exclusion, and the profound sociospatial consequences that can accentuate disadvantage have been examined by several scholars (e.g.: Thrift and French, 2002; Graham and Wood, 2003; Burrows and Ellison, 2004; Burrows and Gane, 2006).

It is in profiling where both the profit and the interest to political parties and security agencies are to be found. The felt necessity of constructing more accurate 'profiles,' more than the identification of already known criminals and terrorists, lies behind the proliferation of security schemes. There is no space here to go through all of these – as I finish this piece, the latest to be announced include the US 'server in the sky' programme (Bowcott, 2008) and the EU's proposed requirements for international travellers to provide 17 additional pieces of personal information (Traynor, 2008). These will not be the last.

Political criticism of surveillance has mostly been concerned with the relationship of state and citizen, and particularly where the state is felt to overstep the boundaries of normative or constitutional values, in particular those of accountability and privacy (see: Bennett and Raab, 2006). However the control society is also a product of the same crises that have also produced new neoliberal governmentality, wherein citizens are made responsible (and must pay) for things that were previously provided by the state (Rose, 1996). Here we can see the emergence of the 'personal information economy' (Elmer, 2004) and the organizations that facilitate it. The state continues to be one such organization, but one amongst many, and the ways in which it works are increasingly managerial and contractual. Surveillance becomes generalized, and surveillance relationships are transformed through media, becoming *synoptic* (the watching of the few by the many – Matthiesen, 1997) and *lateral*, with citizens not simply the subjects of surveillance by both state and private corporations but involved in watching them and each other for fun and profit (see: Andrejevic, 2005). This does not just attack privacy but starts to generate new relationships that do not accept privacy as normative. In many ways, we are all required to be spies. However, we are not all possessed of the same capabilities for surveillance. The reconfiguration of power/knowledge is where we now turn.

Publishers as Spies in the Information Economy

This all seems some distance from the world of academic books and journals, but it is not. Take the case of Reed Elsevier[3]. A major division of this

[3] Reed Elsevier's main website it at http://www.reedelsevier.com/ Its front page emphasises the scholarly, with the slogan, 'Inspiring Discovery' and gives no hint of its involvement in the trade in personal information.

growing transnational knowledge broker is LexisNexis[4]. LexisNexis is a company that most would think of as providing a newspaper clippings service. However, LexisNexis, through its Risk and Information Analytics Group[5], is a major player in the data mining business and one which is associated with a number of companies and systems of dubious repute. It has gradually acquired many other major business associated not only with KDD for business and private use, but also with government contracting: RiskWise in 2000 (Business Wire, 2000), Seisint in 2004 (LexisNexis, 2004) and ChoicePoint (2008)[6]. That these businesses were all American is reflective simply of the commodification of personal information in the United States in comparison to many other nations.

The latter two companies are particularly interesting, and their histories are well covered in investigative journalist, Robert O'Harrow's 2005 book, *No Place to Hide*. Seisint was the company that produced the Multistate Anti-terrorism Information Exchange Program (MATRIX). MATRIX was an advanced form of psychogeodemographic profiling (Pridmore, 2006) designed to combine information from state and commercial databases to connect existing suspects or indicate new ones. It acted as a kind of American states-level version of the US national Total Information Awareness (TIA) programme. Both programmes were eventually publically abandoned as overly intrusive, although it would be surprising if they did not continue in some covert form.

ChoicePoint[7] was even bigger. It had a huge set of super-computer based databases which it used for everything from insurance fraud, through its Comprehensive Loss Underwriting Exchange (CLUE) and employee-screening, pre-screening and drug-testing. Its main asset is a very complex set of KDD algorithms called Non-Obvious Relationship Awareness (NORA). As with Seisint, ChoicePoint has been subcontracted by a part of the US government, in this case the Justice Department in 2003, to link up and extend many of its dataveillance systems.

---

[4] LexisNexis's website is at http://www.lexisnexis.com/ It is a typically glossy corporate production, claiming to be "a leading global provider of business information solutions to professionals."

[5] According to the group's website http://risk.lexisnexis.com/ it "delivers actionable intelligence to help you make critical business decisions with confidence and speed."

[6] At the time of writing the takeover had not been completed, and this website http://lexisnexisupdate.com/ promised to keep the situation updated.

[7] http://www.choicepoint.com/

Private corporate spies are now better equipped and more efficient than states at this kind of intelligence work, and O'Harrow argues, effectively outsourcing state surveillance helps governments avoid legal constraints. This does not mean that they are any more competent. After its acquisition by LexisNexis, Seisint was involved in a huge loss of personal data in 2005 with records on over 310,000 US citizens stolen from the firm. There is apparently no evidence of any fraud or identity theft as a result of this, however in 2005, ChoicePoint admitted the loss of over 163,000 records and according to the US Federal Trade Commission investigation that followed there were more than 800 consequent confirmed cases of identity theft (USFTC, 2006). The company was forced to pay a total of $15 Million in fines and compensation. However perhaps even more concerning is that ChoicePoint was the owner of DBT, the company behind the mistaken or deliberately fraudulent removal of thousands of largely black voters from the electoral roles in advance of the 2000 US presidential election (USCCR, 2001).

Reed Elsevier therefore now owns probably the largest and most sophisticated data-mining operation in the world, servicing both state and corporate components of the emerging surveillance society (Lyon, 2001; Murakami Wood *et al*, 2006). It screens workers, checks the backgrounds of migrants, scans electoral rolls, determines the potential risk and profitability of people worldwide. The company could in theory have effective control over many areas of personal life from the relatively trivial like how much junk mail one gets to the most serious such as whether can get a job, health insurance or vote.

Ethical Places in the Academic Network

There are three broad sets of responses for academics confronted with publishers becoming if not 'Big Brother' then at least one of several little ones. The first is total acceptance. This can be on two grounds: moral or pragmatic. The moral case derives from the contention that the social good produced by these systems in terms of the combating of terrorism and crime, and perhaps from the convenience of increasingly accurate personalised marketing, outweighs the social bad of decreasing privacy and accountability. The pragmatic case is that nothing can be done. The latter can be dismissed as simple technological fatalism, but, the former is the current standpoint of increasing numbers in governments in the post-911 era.

The second is engagement. Here one recognises the end of normative privacy and pervasive surveillance, but with three different orientations: firstly, increased regulation of state, private and individual collection and use of such data; secondly, greater or total transparency - for all the information and the tools to use it to be available to everyone; or finally, the encouragement of personal information economies. The regulation argument is advocated by many involved in data protection as a profession and by senior academics involved in the study of privacy (c.f.: Bennett and Raab, 2006).The transparency argument derives from the

most libertarian theory of information – that it 'wants to be free'. This is advocated by Transparent Society thinkers (Brin, 1999) and the social entrepreneurs of the Open Source movement (c.f.: Stalder, 2001). The market argument is the logical extension of the commodification of more and more intimate aspects of personal life. It would allow control to those who either have the knowledge or the resources to engage someone or something else to manage their own personal information economy. Those without resources would be forced to derive what value they could from their own information, the virtual equivalent of selling a kidney. The irony is that those most desperate to sell their information would be those least likely to be of interest to profilers. Markets in personal information would tend to accentuate information inequality (Turrow, 2006).

Finally, there is the response of active resistance or subversion. This can vary from an Luddite anti-technological impulse through Ellulian caution[8], the 'sousveillance' or 'equiveillance' of Steve Mann *et al*. (2003) and others like the Surveillance Camera Players[9] or the Guerilla Geographers[10] who hold up technological, cultural or spatial mirrors to surveillance, to the illicit manipulation of data itself. Such efforts tend to concentrate on obvious visible public space surveillance like CCTV rather than dataveillance. One can see forms of system hacking as an equivalent for networked databases however, despite fervent hopes amongst some academics and the fear-mongering of police, the practice of hacking appears in general to be motivated mostly by self-promotion within an inward-looking subculture rather than either progressive political or criminal motivations.

It is difficult to see any emerging mass movement or single radical ethical position around personal information or surveillance, indeed there may be totally contradictory but equally radical and progressive impulses behind resistance, regulation and transparency. Whilst it may be clear that exhibitions promoting the arms trade are ethically wrong and therefore resistance necessary[11], the ethics of the personal information economy are far less obvious and more complex. However there is an increasing reliance by states and companies on automated sorting of populations by categorization systems whose bases and rationales are opaque, that are subject to both contingent and systematic, and often uncorrectable, errors, and

---

[8] David Lyon is one major analyst particularly influenced by the thinking of Jacques Ellul – noting in *Surveillance after September 11* (2003) that his work is still worth considering, despite his detractors.

[9] http://www.notbored.org/the-scp.html

[10] http://guerrillageography.blogspot.com/

[11] Although even here of course there was a split between those advocating boycott and critical engagement.

that are potentially or actually corrupt and damaging to social trust, personal privacy and civil liberties.

In this context, at the very least an ethical production and consumption decision must surely be unavoidable: buying the products of or producing for such companies remains ethically dubious. We do not have to accept the inevitability of the dominance of the information economy by impersonal and amoral transnational information brokers. Other companies must be better choices. Yet the very technologies of interconnected computing and databases that allow data-mining also allow us to develop our own systems of production, distribution and consumption: journals like *ACME* and *Surveillance & Society*, *C-theory* and others are vibrant evidence of this. This is not a 'geographical' message, but it is a message for geographers as critical scholars, who should, if nothing else choose to support and encourage these efforts.

And beyond the ethics of scholarly engagement, the geographies of surveillance remain relatively poorly developed with sociological ideal-typical notions like 'the surveillance society' still predominating over the investigation of surveillance in places, and the surveillant construction of spaces, with a handful of geographers actively involved. There is both room and requirement for more engagement and critical research.

References

Andrejevic, Mark. 2005. 'The work of watching one another: Lateral surveillance, risk, and governance' *Surveillance & Society*, 2(4): 479-497. http://www.surveillance-and-society.org/articles2(4)/lateral.pdf [accessed 10 April 2008]

Bennet, Colin and Charles Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. New Edition. Cambridge MA: MIT Press.

Bowcott, Owen. 2008. 'FBI wants instant access to British identity data: Americans seek international database to carry iris, palm and finger prints,' *The Guardian*, Tuesday January 15 2008 http://www.guardian.co.uk/uk/2008/jan/15/world.ukcrime [accessed February 23 2008]

Bowker, Geoffrey and Star, Susan L. 1999. *Sorting Things Out: Classification and its Consequences*, Cambridge MA: MIT Press.

Brin, David. 1999. *The Transparent Society*. New York: Perseus.

Burrows, Roger and Ellison, Nick. 2004. 'Sorting Places Out: Towards a social politics of neighbourhood informatisation', *Information, Communication and Society* 7(3): 321-336.

Burrows, Roger and Gane, Nicholas. 2006. 'Geodemographics, Software and Class', *Sociology* 40(5): 773-791.

Business Wire. 2000. 'LEXIS-NEXIS Acquisition of RiskWise, International Dramatically Expands Risk Management Services,' 7 September 2000 http://findarticles.com/p/articles/mi_m0EIN/is_2000_Sept_7/ai_65062899 [accessed 23 February 2008]

Castells, Manuel. 1996-8. *The Information Age: Economy, Society and Culture (3 Volumes)*. Oxford: Blackwell.

Clarke, Roger. 1988. 'Information technology and dataveillance,' *Communications of the ACM* 31(5): 498-512.

Dandecker, Christopher. 1990. *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. New York: St. Martin's Press.

Deleuze, Gilles. 1990. 'Post-scriptum sur les sociétés de contrôle', *L'autre journal* 1; trans Martin Joughin (1992) 'Postscript on the societies of control', *October* 59: 3-7.

Dyer, Owen. 2007. 'Boycott publisher because of holdings in arms trade, readers told,' *British Medical Journal* News 334:389, 24 February. http://www.bmj.com/cgi/content/full/334/7590/389-c [accessed 23 February 2008]

Elmer, Greg. 2004. *Profiling Machines: Mapping the Personal Information Economy*. Cambridge MA: MIT Press.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. Harmondsworth: Penguin.

Galloway, Alexander. 2004. *Protocol: How Control Exists after Decentralization*, Cambridge MA: MIT Press.

Gandy, Oscar H. Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.

Giddens, Anthony. 1985. The Nations-state and Violence. Cambridge: Polity Press.

Graham, Stephen and David Wood. 2003. 'Digitising surveillance: Categorisation, space, inequality', *Critical Social Policy*, 23(2): 227-248.

LexisNexis. 2004. 'LexisNexis Completes Acquisition of Seisint, Inc.' Press Release 01 September 2004 http://www.lexisnexis.com/about/releases/0730.asp [accessed 23 February 2008]

Lianos, Michalis. 2001. *Le Nouveau Contrôle Social: Toile institutionnelle, normativité et lien social*. Paris : L'Harmattan-Logiques Sociales.

Lianos, Michalis. 2003. 'After Foucault' (trans. David Wood,) *Surveillance & Society* 1(3): 412-430.

Lyon, David. 2001. *Surveillance after September 11*. Cambridge: Polity Press.

Mann, Steve, Jason Nolan and Barry Wellman. 2003. 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments,' *Surveillance & Society*, 1(3): 331-355. http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf [accessed 23 February 2008]

Marx, Gary T. 1985. 'I'll be Watching You: Reflections on the New Surveillance,' *Dissent*, Winter: 26-34.

Mathiesen, Thomas. 1997. 'The Viewer Society: Michel Foucault's "Panopticon" Revisited' *Theoretical Criminology* 1(2): 215-33.

Murakami Wood, David (ed.), Kirstie Ball, David Lyon, Clive Norris, and Charles Raab. 2006, reissued 2007. *A Report on the Surveillance Society*, Wilmslow, UK: Office of the Information Commissioner. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf [accessed 23 February 2008]

Norris, Clive. 2003. 'From personal to digital: CCTV, the Panopticon and the technological mediation of suspicion and social control', in David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge, 249-281.

O'Harrow, Robert. 2005. *No Place to Hide*. New York: Free Press.

Pridmore, Jason. 2006. Consumption and Profiling. Expert Report for *A Report on the Surveillance Society*, Wilmslow UK: Office of the Information Commissioner. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_appendices_06.pdf [accessed 23 February 2008]

Rose, Nikolas. 1996. 'The death of the social? Re-figuring the territory of government', *Economy and Society*, 25(3): 327-56.

Rule, James B. 1973. *Private Lives, Public Surveillance: Social Control in the Information Age*, London: Allen Lane.

Stalder, Felix. 2002. 'Privacy is not the antidote to surveillance,' *Surveillance & Society* 1(1): 121-124. http://www.surveillance-and-society.org/articles1/opinion.pdf [accessed 23 February 2008]

Sunday Times. (London) 2007. 'Business Digest: Reed fails to sell arms fairs' (30 December 2007) (Online, no page numbers). http://business.timesonline.co.uk/tol/business/industry_sectors/media/article3107403.ece [accessed 10 April 2008].

Thrift, Nigel and Shaun French. 2002. 'The Automatic Production of Space', *Transactions of the Institute of British Geography* .Vol 27, No. 3 pages 309-335.

Traynor, Ian. 2008. 'Government wants personal details of every traveller: Phone numbers and credit card data to be collected under expanded EU plan,' *The Guardian*, Saturday February 23 2008. http://www.guardian.co.uk/uk/2008/feb/23/uksecurity.terrorismandtravel [accessed February 23 2008]

Turrow, Joseph. 2006. *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge MA: MIT Press.

United States Commission on Civil Rights (USCCR). 2001. *Voting Irregularities in Florida During the 2000 Presidential Election*, June 2001. http://www.usccr.gov/pubs/vote2000/report/main.htm [accessed 23 February 2008]

United States Federal Trade Commission (USFTC). 2006. 'ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress.' http://www.ftc.gov/opa/2006/01/choicepoint.shtm [accessed 23 February 2008]