Book Review for Surveillance & Society

David Wright, Serge Gutwirth, Michael Friedewald, Elena Vildjiounaite and Yves Punie editors (2008) *Safeguards in a World of Ambient Intelligence*. London, Springer.

291 pp. Hardback $159.00 (US), £91.00 (UK). ISBN-978-1-4020-6661-0.

Martin Dodge[1]

Pervasive computing and the subtle surveillance of everything

Computers and software code are widely recognised as powerful tools in contemporary surveillance practices. Significantly their agency is now changing as the social and spatial disposition of computers diffuses into almost all aspects of everyday life. Computers, that increasingly don't look like computers, are permeating our domestic spaces and accompany us throughout the day, mediating our interactions and facilitating quotidian activities. And this is just the beginning, so it is argued, of the next wave of digital technological development, the so-called pervasive computing revolution, which according to Anne Galloway (2004: 384-5), 'seeks to embed computers into our everyday lives in such ways as to render them invisible and allow them to be taken for granted.' Such computing that is active-in-absence will summon much more subtle forms of software surveillance of our everyday lives.

How do we begin to make sense of what pervasive computing might mean for the practices of surveillance? How will the ubiquitous monitoring of everyday activities by code effect the constitution of social life, personal identities and political equality? How will corporations try to exploit the opportunities offered by new streams of much more intimate information about our behaviour? How should government respond, if at all? And how can scholars across surveillance studies begin to engage to, firstly, *describe* this fast moving field of technological development and, secondly, to begin to *explain* the myriad of implications and, thirdly, perhaps map out a set of progressive *responses* to

[1] Geography, School of Environment and Development, University of Manchester.
mailto: m.dodge@manchester.ac.uk; blog: http://cyberbadger.blogspot.com/

challenge the underlying logics of pervasive computing and conceivably mitigate some of the iniquitous effects of subtle surveillance of everything.

The edited volume, *Safeguards in a World of Ambient Intelligence* (2008), is one of a range of books that beginning to provide social science scholars a toolbox of descriptions, explanations and responses to pervasive computing[2]. The book emerged out of applied research from a 2005 pan-European project and is published by Springer as part of their ‘ethics, law and technology’ thematic series. The team of five editors of the book are drawn from a range of backgrounds including law, electrical engineering, media regulation and the social sciences. Their focus is on the social implications of ‘ambient intelligence’, shortened in the book to the friendly acronym AmI, which is alternative term for pervasive computing. (The AmI badge is closely associated with industrial research support by the Philips consumer electronics corporation and one of their senior staff provides a foreword in the book.) AmI they define as a ‘brave new world’ in which ‘computers monitor our activities, routines and behaviours to predict what we will do or want next’, and where we will be ‘surrounded by easy-to-use interfaces that are embedded in all kinds of objects and by an everyday environment that is capable of recognising and responding to individuals in a seamless, unobtrusive and invisible way’ (p .1). The underlying political position of the book defaults, rather unthinkingly, to utopian determinism, seeing the trajectories of digital technological development as inevitably set. There is a distinctly neoliberal perspective engrained in the book that means AmI *must* happen, as they say: ‘we are convinced that Europe must go “full steam ahead” in developing the necessary technologies and architectures in order to remain competitive against our rivals in the United States, Japan, Korea and elsewhere.’ (p.8). Basically they read into AmI beneficial outcomes for the large majority of European consumers, assuming that the harsh edges of rapacious corporations and risks of unscrupulous government officials can be rounded down with self regulation, cleverly engineered public policy and well framed legislation – this being the ‘safeguards’ agenda alluded to in the

[2] Other noteworthy books include, Greenfield (2006), McCullough (2005) and Mitchell (2004).

book’s title. Yet from past experience with earlier rounds of computerisation in other domains of society it is not clear to me quite how, in reality, such policy and legal ‘safeguards’ will really deliver a harmonious accommodation with avowedly profit-driven pervasive computing and conventional notions of privacy.

The book’s content tends to be factual rather than philosophical, with the description of the ‘brave new world’ of AmI divided into three main sections: future-looking scenarios, discussion of threats and vulnerabilities and then setting out possible safeguards followed by shorter chapter of recommendations. The most interesting part of the book, in my opinion, is the first section in which the editors run through what they call ‘dark’ scenarios with the aim to ‘show things that could go wrong in an AmI world… expos[ing] threats and vulnerabilities as a way to inform policy-makers and planners’ (p. 33). Hypothetical scenarios are viable methodology for thinking about likely pathways and potentialities of technologies that are just coming into being and speculating on the varying contexts of their implementation (it is a interpretative ‘trick’ I have used myself; cf. Dodge and Kitchin, 2009) and has value in some respects for surveillance studies. But such scenarios need to be hard-headed, honest and rigorously written, and they are tough to construct in ways that are plausible. The danger is that scenarios descent into stereotypes, or focus on unlikely or extreme situations. They are also open to accusations that they are merely ‘analysis by anecdote’, with the risk that, consciously or unconsciously, the scenarios are constructed to complement preconceived agendas and are thus little more than marketing models.

The dark scenarios of pervasive computing presented in this book do not quite work in that they are too neat and narrowly drawn, tending towards soap opera’ish plotting and events, along with corny dialogue. The central characters in the scenarios are all financially affluent and socially capable – just like the smiling, contented consumers typical of corporate IT advertising. As such the scenarios do not really penetrate to the heart of issues to reveal the messy, conflicted and imperfect world in which technology unfolds. Furthermore, the analysis and interpretation of the scenarios is uneven and dominated by dry discussion based on how events would be interpreted under current EU legislation.

In terms of overall presentation and readability the book is also weak. It feels like it has been written by committee (it has five editors and ten authors are listed on the frontispiece) with a disjointed and inconsistent style. The text never seems to really flow and, as is the way with some technology books, it is distractingly peppered with acronyms, italicised words, emboldened phrases, text boxes, bullet point lists and excessive footnotes. The chapters are continuously broken apart into small sections, some of which do not link to each other. The result seems almost calculated to break sustained narrative needed for considered analysis. There is also a significant degree of overlap and repetition between chapters; I think a more thorough overarching editing could have cut at least a quarter of the text and made for a tighter, more insightful book.

Overall, *Safeguards in a World of Ambient Intelligence* is a somewhat useful contemporary review of developments in pervasive computing but is beleaguered in a morass of details on technologies, lists of projects and a welter of legislation. Consequently it largely fails to tease out the larger conceptual themes into a convincing narrative. As such the lasting value of this volume is, in my opinion, going to be limited. So there is still a pressing need for someone to write a definitive socio-technical analysis of pervasive computing and the changing landscape of privacy and power that is emerging. Perhaps a reader of this journal will produce such a monograph to provide the descriptions, explanations and set of responses to the coming of subtle surveillance of everything.

References

Dodge M. and Kitchin R. (2009) Software, objects and home space. *Environment and Planning A,* in press.

Galloway A. (2004) Intimations of everyday life: Ubiquitous computing and the city. *Cultural Studies* 18(2): 384-408.

Greenfield A. (2006) *Everyware: The Dawning Age of Ubiquitous Computing* (Peachpit Press, Berkeley, CA).

McCullough M. (2004) *Digital Ground: Architecture, Pervasive Computing and Environmental Knowing* (MIT Press, Cambridge, MA).

Mitchell W. (2004) *ME++: The Cyborg Self and the Networked City* (MIT Press, Cambridge, MA).