Sci Eng Ethics (2009) 15:125–127
DOI 10.1007/s11948-008-9106-1

BOOK REVIEW

Safeguards in a World of Ambient Intelligence; David Wright, Serge Gutwirth, Michael Friedewald, Elena Vildjiounaite, Yves Punic (eds)

Springer Science + Business Media B.V., Dordrecht, The Netherlands, 2008, 291 pp. ISBN 978-1-4020-6621-0, e-ISBN 978-1-4020-6662-7

Neelke Doorn

Received: 13 October 2008 / Accepted: 15 October 2008 / Published online: 26 November 2008

The European term Ambient Intelligence (AmI)—or equivalently ubiquitous and pervasive computing (US) or ubiquitous networking (Japan)—reflects a vision of the future of ICT in which intelligence is embedded in virtually everything around us. People are surrounded by electronic devices that are capable to recognize and respond to individuals' actions. Invisibly and unobtrusively, this "internet of things" (Schoenberger 2002) will serve to support people in carrying out their everyday life. It bears the promise of making life easier, more comfortable and more secure. This future vision of a "brave new world of Ambient Intelligence" (p. 1) calls for a critical reflection on the potential risks of such a society. *Safeguards in a World of Ambient Intelligence* provides such a reflection.

The book grew out of the EU sponsored SWAMI project (an acronym of Safeguards in a World of Ambient Intelligence), which started in February 2005 and which was carried out by five European partners, namely Fraunhofer Institute for Systems and Innovation Research (Germany), the VTT Technical Research Centre of Finland, Vrije Universiteit Brussel (Belgium), the Institute for Prospective Technological Studies (IPTS, Spain) of the EC's Joint Research Centre, and Trilateral Research and Consulting (UK). This European orientation remains visible throughout the book.

In the preface it is stated that the book has four key objectives. First it aims to be a warning. Second, it aims to illustrate the threats and vulnerabilities by means of four 'dark scenarios.' Third, it sets out a structured methodology for analyzing these scenarios and fourth, it identifies a range of safeguards against the threats and vulnerabilities identified. These objectives are all met, be it in varying degrees of success.

N. Doorn (✉)
Department of Technology, Policy & Management, Delft University of Technology,
PO Box 5015, Delft 2600, GA, The Netherlands
e-mail: N.Doorn@tudelft.nl

The core of the book deals with four scenarios which are built around (1) the AmI family; (2) travel and health AmI systems; (3) data aggregating; and (4) AmI risk society. These are discussed in terms of the issues of concern—privacy, identity, trust, security and inclusiveness (or the opposite: the digital divide)—and the prevailing legislation. The second half of the book is dedicated to a discussion of threats and vulnerabilities, potential safeguards and a short section on recommendations for stakeholders.

The start of the book is promising. It provides an elaborate overview on the different kinds of enabling technologies that can be considered AmI and a useful inventory of the visions of AmI as reflected in other projects (both EU sponsored, as American and Japanese projects), the different tools that can be developed in order to bring these vision into reality and the most important players worldwide.

From a methodological point of view the book is excellent. It gives an elaborate description of how to construct scenarios, with ample attention to the demands of both technical and reality reliability. In order to fulfill this reliability demand the four scenarios are carefully supported with secondary literature. A well-worked out methodology for analysis of the scenarios is provided as well, which could almost directly be applied to other emerging technologies.

It is somewhat disappointing that in the analysis itself the attention is almost solely focused on juridical aspects and legislation. Besides the fact that this gives the book an unmistakably European character, which somewhat undermines its usability outside the European region, it also misleadingly gives the impression that legislation is the most important tool to deal with technological risks. However, regulatory frameworks and law often lag behind, which calls for ethical reflection while technologies are being developed.

This focus on legislation and juridical aspects returns throughout the book. In the discussion of the safeguards, for example, three types of safeguards are discussed: technical, socio-economic and legal/regulatory safeguards. More than half of the space is dedicated to legal and regulatory safeguards. Socio-economic safeguards are discussed only marginally which is somewhat surprising given current insights in Science and Technology Studies (STS) that technology is partly shaped by social context (Pinch and Bijker 1984). This suggests that socio-economic measures accommodate a wealth of efficacious safeguards. It is a pity that the authors did not use the opportunity to elaborate on these but focused on legal/regulatory safeguards instead. The same holds true for the chapter with recommendations for stakeholders, which, again, has a strong bias towards juridical measures. The focus is on the European Commission and the Member States with an emphasis on legislation. Other stakeholders are discussed only briefly.

A second critical point is the fact that the issues of concern are discussed only very briefly. Although the authors admit that, e.g., "the notion of privacy is unstable, complex, difficult to fix" (p. 144), they do not attempt to provide a more thorough analysis. This is a serious drawback of the book. The way we conceive of matters like privacy, identity, etc., will most probably be highly influenced by the technology, which calls for a critical reflection on the terms themselves. The concepts get their meaning in interaction with the technology so the concern for privacy cannot be discussed without a clear-cut vision on the values that lie behind this notion of privacy. Why and how does AmI pose a threat to privacy? What underlying values are at stake? The same holds for the other issues of concern.

This omission comes up again in the discussion on threats and vulnerabilities, where the authors make a distinction between threats (the potential for one or more unwanted consequences that could be harmful to a system or person) and vulnerabilities (a flaw or weakness in the system's design, implementation, operation or management that could cause a threat). They argue that AmI does not pose radically new threats but rather increases them by the degree of embeddedness and scale. In their discussion of the threats the authors lean heavily on the Information Society Technologies Advisory Group (ISTAG) report of 2001 (Ducatel et al. 2001). This work done by ISTAG is generally considered starting point of AmI research carried out at the EU level. It is therefore a little disappointing that the authors were not able to proceed really further in terms of threats identified but stuck to the same threats. In the discussion of the vulnerabilities the moral concerns identified in the analysis of the four scenarios return, which somewhat blurs the analytical distinction between the threats and the vulnerabilities. The text on vulnerabilities itself is informing though.

Taking it all together the book provides an interesting starting point to reflect on AmI and the way this new technology will influence our future society. The authors provide a thorough overview on the relevant juridical frameworks and identification of potential gaps in (international) law and directives. Since regulatory frameworks and law are known to often lag behind, ethical reflection is needed while technologies are being developed. Although the book does not provide the reflection itself, it does provide a good starting point for ethicists who would like to take up this challenge.

References

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., & Burgelman, J.-C. (2001). *Scenarios for ambient intelligence in 2010*. Seville: Institute for Prospective Technological Studies (IPTS).

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artifacts - or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*(3), 399–441. doi:10.1177/030631284014003004.

Schoenberger, C. R. (2002). Internet of things. Forbes Magazine, March 18 2002.