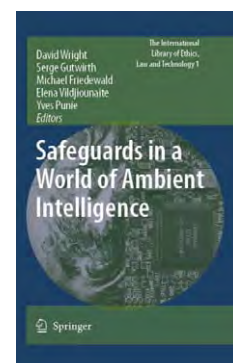


## Book review

# Safeguards in a world of ambient intelligence: *A social, economic, legal, and ethical perspective*



Egon L. van den Broek\*

Human-Centered Computing Consultancy, Vienna, Austria

URL: <http://www.human-centeredcomputing.com/>

E-mail: [vandenbroek@acm.org](mailto:vandenbroek@acm.org)

**Abstract.** The book “Safeguards in a world of ambient intelligence” is unique in its kind. It discusses social, economic, legal, technological and ethical issues related to identity, privacy and security in Ambient Intelligence (AmI). It introduces AmI and, subsequently, makes it vivid by describing four scenarios. Threats and vulnerabilities as well as safeguards are identified, which stress the already common aspects of current IT and AmI. The book is a little EU-biased but is otherwise well balanced and excellently structured.

Keywords: Ambient Intelligence (AmI), ethics, moral issues, legal issues, social issues, scenarios, complexity

**Safeguards in a World of Ambient Intelligence** (The International Library of Ethics, Law and Technology, Vol. 1) by D. Wright, S. Gutwirth, M. Friedewald, E. Vildjiounaite, and Y. Punie, Dordrecht, The Netherlands: Springer Science + Business Media B.V., 2008/2010, ISBN: 978-1-4020-6661-0 (hardcover) / 978-90-481-8786-7 (softcover).

*“It is not enough that you should understand about applied science in order that your work may increase man’s blessings. Concern for man himself and his fate must always form the chief interest of all technical endeavors.”*

Albert Einstein (1931; 1879–1955)

\*Additional affiliations: Human Media Interaction (HMI), Faculty of EEMCS, University of Twente, Enschede, The Netherlands; Karakter University Center, Radboud University Medical Center (UMC) Nijmegen, Nijmegen, The Netherlands; and Statistics and Surveys Section, Policy Analysis and Research Branch, United Nations Office on Drugs and Crime (UNODC), Vienna, Austria.

## 1. Introduction

In general, social, economic, legal, and ethical issues do not go well together with technology. Ubiquitous computing and Ambient Intelligence (AmI) have not yet changed this. However, par excellence, AmI is a suitable paradigm to bring both ethics and technology closer together: “*Although it is debatable whether ubiquitous computing introduces anything fundamentally new, it might come to exacerbate many of the ethical problems that arise as a result of our increasing dependence on computer technology.*” [6] (p. 8; cf. [2,4,5]). Taking this into consideration, the “Safeguards in a World of Ambient Intelligence (SWAMI)” EU project (2005–2006) was timely [3]. The book reviewed here followed a (freely available) SWAMI deliverable and, as such, is a result of this project. After its initial release in 2008, as an expensive hardcover, two years later, in 2010, a much cheaper softcover edition was published. The book identifies and analyzes social, economic, legal, technological, and ethical issues related to identity, privacy and security in AmI. As such, it is the first book that took up this challenge.

## 2. In touch with AmI

The authors start their book with providing an executive summary (p. xxi–xxvii). This summary provides an honest and well structured overview of the book. However, it also illustrates that the implications of all that is discussed in the book is hard to capture in only seven pages. So, it encourages the reader to continue.

The book starts with a gentle introduction that sketches the book's crucial elements. Noteworthy is the historical parallel that is drawn between ubiquitous computing and AmI. Chapter 2 provides an overview of AmI. The first half of this chapter delivers what it promises. However, starting from the discussion on scenarios, the authors lose themselves a little in an overview of research agendas, projects, prospects, and related topics, all with bias towards the EU, where other initiatives should have been mentioned as well [5]. Subsequently, a chapter of more than 100 pages is devoted to four scenarios. Since the work of Carroll [1] on the use of scenarios in software and product development, this has become an important research method for human-centered computing, which brings possible problems to the surface that would otherwise have remained hidden [5,6]. It indeed makes some issues vivid and, consequently, stresses their importance.

As is stated in [4]: *“The ubiquitous combination of coupled databases, data mining, and sensor technology may start to cast doubt on the usefulness of our notion of ‘privacy’. Ethical analysis and reflection, therefore, is not simply business as usual. We need to give computers and software their place in our moral world. We need to look at the effects they have on people, how they constrain and enable us, how they change our experiences, and how they shape our thinking.”* (p. 50). So, the focus should be on people; see also [5,6]. This is exactly what is done with the use of scenarios in Chapter 3. The two chapters that follow identify the risks, based on the four scenarios (or threats and vulnerabilities; Chapter 4) and present possible solutions (or safeguards; Chapter 5). These two chapters present an impressive taxonomy on these issues and, as such, form the book's center of excellence.

Perhaps the most striking conclusion of Chapter 4 is that the threats and vulnerabilities identified are not unique or new. The authors conclude that *“Our privacy has been eroding for a long time.”* (p. 143). It is a bold statement but they are right (cf. [2,4])! The same holds for our loss-of-control, which has started long ago and seems to be unstoppable. Chapter 5 iden-

tifies three classes or categories of safeguards: technological, socio-economic, and legal and regulatory. Currently, most of us are already familiar with such safeguards. Think for example of the anti-virus software and firewalls, security mechanisms in financial transactions, and the new legal issues that emerge from our rapidly digitalizing societies. These safeguards need to evolve to be able to remain useful in a highly dynamic society augmented with AmI.

The book ends with two brief chapters with some recommendations for stakeholders (Chapter 6) and general conclusions (Chapter 7). The specific recommendation for the different stakeholders have little added value. In contrast, the conclusions are concise, to the point, as conclusions should be, which provides the book with a worthy end.

## 3. Conclusion

*“Safeguards in a World of Ambient Intelligence”* is no edited volume but a balanced integral book. The book came out of an EU project that aimed to identify and analyze social, economic, legal, technological and ethical issues related to identity, privacy and security in AmI [3]. Recent (non-EU) initiatives stress its timeliness [5]. Scenarios are used as a starting point [1]. On the one hand, this may cause readers to lose their interest; on the other hand, this sketches implications of AmI that otherwise would have remained unveiled [5,6]. This book is unique in its kind and, as such, a valuable reference work. Compared to other recent (edited) handbooks [2,4], its specific focus and structure determines its value.

## References

- [1] J.M. Carroll, *Making Use: Scenario-Based Design of Human-Computer Interactions*, The MIT Press, Cambridge, MA, USA, 2000.
- [2] L. Floridi, *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, Cambridge, UK, 2010.
- [3] M. Friedewald, Safeguards in a World of Ambient Intelligence: Outline of a research agenda on the European level, *Lecture Notes in Computer Science* **3450** (2005), 63–69.
- [4] K.E. Himma and H.T. Tavani, *The Handbook of Information and Computer Ethics*, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2008.
- [5] K.D. Pimple, Computing ethics: Surrounded by machines, *Communications of the ACM* **54**(3) (2011), 29–31.
- [6] J.H. Søraker and P. Brey, Ambient Intelligence and Problems with Inferring Desires from Behaviour, *International Review of Information Ethics* **8**(1) (2007), 7–12.