

## Preface

Security has become a key issue in modern life, both in the physical and the virtual worlds. For the physical world, the need for security was always there, even though in very small isolated and peaceful communities, like a hamlet where everyone knows each other, security might seem a far-fetched concern. However, in the virtual world, for good or evil there are no small isolated communities: global connectivity implies that we are all within reach of (probably unknown) remote malicious parties. Therefore, it is today beyond dispute that the information society is not viable without a certain degree of security; no entity (organization or individual) likes to engage in a transaction which might render it vulnerable to attacks. For example, no shop would sell on-line if payment systems were not secure and/or buyers could penetrate the shop's backoffice.

While the information society has to stay secure to survive, it must respect privacy to stay human. Just as organizations do not like insecurity, human beings need some privacy to feel comfortable. Privacy is not exactly secrecy: it rather means that an individual should be given the means to control what information about her is disclosed, as well as when and to whom it is disclosed. Being privacy-friendly in the information society is in many respects parallel to being environment-friendly in the physical society. In principle, neither of both properties has much commercial appeal: just as being environmentally friendly tends to increase manufacturing costs, being privacy-friendly implies that the ability of service providers to profile users (*e.g.* in view of customer relationship management or with more dubious aims) is substantially reduced. However, in the same way that green products are earning ever larger market shares, privacy-preserving services will follow the same trend as the awareness of consumers about potential abuses and about their own rights increases.

There are reasons for optimism: individual privacy is mentioned in the Universal Declaration of Human Rights (1948) and data privacy is explicitly protected by law in most Western countries. Now the challenge is to turn

laws into technologies and to have those technologies deployed, without significant losses in security, functionality or operational efficiency. For the time being, though, the development of privacy technologies is still very dependent on sponsorship and awareness campaigns by the public sector, unlike the development of security technologies.

This book edited by Dr. Solanas and Dr. Martínez-Ballesté has the virtue of embracing both privacy and security technologies. Furthermore, its scope is very broad, thanks to the contributions of international experts in several different areas of information and communications technologies, not just security and privacy experts. Hence, it can be especially useful for readers with a general background in ICT to grasp the challenges, the solutions and the ramifications of adding security and privacy to ICT systems . The initial part is an introduction putting privacy and security in context. Then there is a part devoted to privacy, consisting of chapters going from methodology to specific applications like statistical disclosure control and medical databases. The final part comprises several chapters covering different aspects of security research.

Having had the pleasure to do research with the co-editors and with several chapter contributors of this book for a number of years, I can only recommend this work to anyone interested in the intertwined areas of security and privacy.

Tarragona, January 2009.

*Prof. Dr. Josep Domingo-Ferrer*  
*Chairholder*  
*UNESCO Chair in Data Privacy*  
*Department of Computer Engineering and Mathematics*  
*Universitat Rovira i Virgili*  
*Tarragona, Catalonia*