

## Foreword

The last several years have been characterized by global companies building up massive databases containing computer users' search queries and sites visited; government agencies accruing sensitive data and extrapolating knowledge from uncertain data with little incentive to provide citizens with ways of correcting false data; and individuals who can easily combine publicly available data to derive information that – in former times – was not so readily accessible.

“Social Implications of Data Mining and Information Privacy: Interdisciplinary Frameworks and Solutions” addresses precisely these issues. Cultural differences can possibly lead to differing expectations of how information is handled and ideas of to whom information belongs. European countries, most notably Germany, Austria, and Switzerland, share the view that personal information belongs to the person in question, whereas in the United States, information belongs to the company who generated or collected it.

Establishing an ethics-framework for data mining is crucial. Politics often uses drastic examples of relatively rare crimes, such as terrorism or child pornography, to introduce legislation that may later be extended to cover minor crimes or to surveil political opposition. In the corporate world, effective CRM may very well infringe on personal privacy; it is, however, needed to provide customers with the services they expect. While many complain about “companies that know everything about their costumers,” we expect call centers, for instance, to know about our entire previous communication, about payments, and so forth. When companies morph into corporations and jointly offer services, we want them to provide services for which they are required to share our data. We resent however, the idea that they exchange data or might use it for other purposes.

Data privacy and integrity gain in importance because many people use computers almost continuously and – more importantly – computers remain connected to the Internet all the time. In cities, Internet access is a commodity infrastructure similar to water or power. Jurisdiction needs to take these changes into account, too. Legal frameworks react and evolve as society changes. Such frameworks must reflect the standards that citizens expect and fit them, as such, into the context of existing laws.

I wish all readers many enjoyable and fascinating hours with this book and congratulate the editor and authors on their excellent work!

*Dr. Edgar Weippl*  
*Austria*

*Edgar R. Weippl (CISSP, CISA, CISM) is science director of Secure Business Austria and university assistant at the Vienna University of Technology. His research focuses on applied concepts of IT-security and e-learning. Edgar has taught several tutorials on security issues in e-learning at international conferences, including ED-MEDIA 2003-2007 and E-Learn 2005. In 2005, he published Security in E-Learning with Springer. After graduating with a PhD from the Vienna University of Technology, Edgar worked for two years in a research startup. He then spent one year teaching as an assistant professor at Beloit College, WI. From 2002 to 2004, while with the software vendor ISIS Papyrus, he worked as a consultant for an HMO (Empire BlueCross BlueShield) in New York, NY and Albany, NY, and for Deutsche Bank (PWM) in Frankfurt, Germany.*