Foreword

In public debates about **potential impacts** of contemporary Information and Communication Technologies (ICTs), **invasion of "privacy" and misuse of personal data** are often regarded as being amongst the most evident negative effects of ICTs which should be carefully analysed and controlled. Computing experts and informaticians often use the term **"data protection"** as synonymous with "privacy" although this usage is somewhat misleading: the main task is NOT to protect the data but it is the **task to protect the personal sphere** represented by the data and their relations associated with a person (sometimes called the "data shadow" of a person's privacy).

Indeed, the term "data protection" tends to hide basic problems which have to be solved to technically protect the "data shadow" of a person's "private sphere". While "data protection" assumes that data have been taken and stored, an analysis of person's privacy concerns may require that related data should on no account be taken and stored. Therefore, the term "data protection" is too technically reductive to be used synonymously for privacy.

The consistent inadequate usage of the term "data protection" is another illustration of the validity of Joseph Weizenbaum's metaphor (in his book "Computer Power and Human Reasoning") according to which computer scientists tend to search for some solutions in the light of a lantern, whereas the key lies in the shadow. Indeed, it is comparably easy to describe how to technically protect data, whether related to a person, an enterprise or any other entity. Several models exist for restricting access to any data, either on a "discretionary" or "mandatory" basis (DAC, MAC), either built into the kernel of an operating system ("Reference Monitor") or into some outer shell. Some models may also distinguish between the roles a user of stored data actually plays (RBAC), and a refined model may also include tasks which a user actually has to perform upon such data (a valuable contribution of the author of this book). "Auditing" provides adequate means to control whether personal data are used according to prescriptions, such as rights of users or capabilities of related IT processes. All these models are quite easily implemented (although it is also easy to switch such technical protection off).

Beyond such technical methods, models, and tools, it is significantly more difficult to describe **basic requirements and means to protect the "data shadow" of a person**. Some such requirements can be found in the privacy laws which have been passed in several countries, though on different levels. Some degree of harmonization is available in the European Union, based on its Data Protection Directive, but there still exist many problems in the exchange of personal data with areas with different (or no) legal requirements.

Requirements for privacy protection may depend upon the legal basis of privacy in a particular country. In Germany where privacy is regarded as some quasi-constitutional **"right for informational self-determination",** such requirements are concerned with the **necessity** of data collection and processing, **purpose specification**

and **purpose binding**, and **the transparency** of personal data protection. In addition, directives of the European Union and OECD also require **lawfulness and fairness**. Based on the different legal systems, there are sufficient stipulations on the legal side regarding which requirements must be legally fulfilled to store, process, and communicate personal data.

For a long time, these legal requirements were almost disregarded by the ICT community. Until very recently, there was no basic model for privacy-related requirements which implementations and usage of related information systems must fulfill. It is the specific **value of Simone Fischer-Hübner's work** (published in this book covering her habilitation thesis), that a first model is now available which permits the description of requirements derived from legal concepts.

Moreover, the author does not simply present her suggestions as a collection of principles and technical requirements. Besides developing a "privacy-friendly concept of data protection", she also presents it as a formal model, the implementation of which (when done properly) may help to prove that privacy requirements have indeed been implemented in some software. The demonstration of the model presented in this book is also embedded in contemporary concepts of IT Security, as seen by the description of its realization within LaPadula's Generalized Framework for Access Control. Consequently, implementations of her model will - if done correctly - make the related software not only adaptable to contemporary ITSEC concepts but at the same time "**conforming with law**" and "**privacy-friendly**". She also convincingly counters any argument that such models are "just theoretical and hardly to be implemented": she demonstrates that and how her model can be implemented on a relevant platform.

This book can – and hopefully will – become the foundation of a new way to model and consequently implement user requirements into ICT systems which conform better than before with human principles (starting but not ending with privacy). In this sense, it is my sincere hope that this book becomes really successful.

November 2000

Dr. Klaus Brunnstein
Professor for Application of Informatics
University of Hamburg

Preface

In the Global Information Society, the individual´s privacy is seriously endangered and is becoming more and more an international problem. An international harmonisation of privacy legislation is needed but is hardly achievable due to cultural differences. Therefore, privacy commissioners are demanding that privacy should be a design criterion and that more privacy-enhancing technologies have to be designed, implemented and used. In addition to privacy technologies for the protection of users, there is also a need for privacy enhancing technologies for protecting the data subjects, who are not necessarily system users.

In this thesis, the related areas of privacy, IT-security and privacy-enhancing technologies are presented, elaborated, analysed and discussed. The central part of this thesis is the presentation of a formal task-based privacy model, which can be used to technically enforce legal privacy requirements such as the necessity of personal data processing and purpose binding. In addition, it is specified how the privacy model policy has been implemented together with other security policies according to the Generalized Framework for Access Control (GFAC).

This thesis was submitted as a habilitation thesis at Hamburg University in Germany, where it was accepted by the habilitation committee in December 1999. Subsequently, updates have been made to reflect recent developments.

A number of persons have supported me during the time in which I wrote and completed this thesis. I would like to give my thanks to all of them:

I am especially grateful to Prof. Dr. Klaus Brunnstein, who introduced me to the field of IT security and taught me the importance of taking an holistic view. The discussions I had with him, his ideas, motivating spirit and practical support have been very valuable to me.

I also want to express my gratitude to my colleagues at the Copenhagen Business School (CBS). In particular, I thank Prof. Gert Bechlund, who invited me to be a Guest Professor at the Institute of Computer and System Sciences (DASY) at CBS from fall 1994 to spring 1995, and Prof. Lars Frank, for the interesting discussions we had while we were working together at CBS. I also thank CBS for having funded my research during the time of my guest professorship.

I also owe special thanks to my colleague Dr. Louise Yngström, who has always been a valuable discussion partner and good friend to me. I especially want to thank her for initiating my invitation as a Guest Professor at the Department of Computer and System Sciences (DSV) at Stockholm University / KTH, which was financed by the Swedish Research Council. At DSV, I also found time for completing this thesis. Therefore I also want to thank DSV for all of its support and for providing a very pleasant working atmosphere.

I also want to thank my former student and colleague Amon Ott, with whom I worked closely during the phase of specification and implementation of my privacy

policy. He was mainly responsible for RSBAC system implementation and discussed with me my system specification. I have enjoyed working with him very much.

I would also like to thank Dr. Michael Sobirey for stimulating discussions and cooperation. Furthermore, I thank my colleagues Dr. Kathrin Schier, Fredrik Björck and Kjell Näckros for discussions, support and friendship, as well as all my other colleagues from IFIP Working Group 9.6 for having been knowledgeable discussion partners.

I am also grateful to a friend of my family, William Watts, who has polished my English. Any mistakes that I might have introduced by modifying the text after he had done his corrections are entirely my own.

I also want to thank the members of the habilitation committee at Hamburg University, and also in particular the external evaluators Prof. Dr. Dr. Gerald Quirchmayr (Univ. Vienna), Prof. Dr. Waltraut Gerhardt (TU Delft) and Prof. Dr. Andreas Pfitzmann (TU Dresden) as well as Prof. Dr. Klaus Brunnstein, who acted as an internal evaluator, for all the work and time they had to spend reading and evaluating this thesis.

Last but not least, I would like to thank my family to whom I dedicate this work. I am most grateful to my beloved parents Hermann and Helga Fischer-Hübner, who have always supported and motivated me. My father as a dedicated lawyer, who was committed to his profession and clients, raised my interest in law and taught me the importance of justice. Finally, I want to express my special thanks to my dear husband Etamar, who was always there for me with love, patience and care.

September 2000 Simone Fischer-Hübner