A vital guide for technology professionals to help safeguard personal data and protect privacy.

In today's economy, personal information is becoming one of the world's most valuable commodities. Yet, as technological innovations provide vast opportunities to collect, process and transfer this information, the associated privacy risks grow exponentially. Now, successful technology professionals must possess the knowledge and skills to safeguard personal data and support the privacy goals of their organization.

In *An Introduction to Privacy for Technology Professionals*, leading minds in the field address how privacy and technology intersect and examine critical areas of concern in the industry. This textbook provides key concepts and techniques to use throughout the entire data life cycle, including:

- The impact of privacy on engineering
- Incorporating privacy into risk analyses
- The role of encryption and nonrepudiation in building solutions
- Concepts of identifiability and anonymity
- The impact of privacy on tracking and surveillance
- Usable and useful privacy interfaces
- Concepts of interference and other privacy harms
- The roles and management of privacy governance
- The integration of security and privacy

An official textbook of the IAPP's Certified Information Privacy Technologist (CIPT®) program, this is an essential resource for developers, system administrators, data architects, UX designers, cybersecurity professionals, key business stakeholders and those in technology acquisition.

TRAVIS D. BREAUX is an associate professor of computer science at Carnegie Mellon University. He teaches and conducts research to develop new methods and tools to build privacy-preserving, secure and trustworthy information systems. Breaux designed CMU's first privacy engineering course, which is part of the Master of Science in Information Technology-Privacy Engineering (MSIT-PE) program, and has published numerous award-winning papers on privacy and software accountability in IEEE and ACM journals and conference proceedings.

CONTRIBUTING AUTHORS

Lujo Bauer
Chris Clifton
Lorrie Faith Cranor, CIPT
Simson L. Garfinkel, CIPP/US
David Gordon
David James Marcos, CIPM, CIPT
Aaron Massey
Florian Schaub, CIPP/US, CIPT
Stuart S. Shapiro, CIPP/G, CIPP/US
Manya Sleeper
Blase Ur

$75.00
ISBN 978-1-948771-90-0
57500>
9 781948 771900

AN INTRODUCTION TO PRIVACY FOR TECHNOLOGY PROFESSIONALS

iapp

AN INTRODUCTION TO PRIVACY FOR TECHNOLOGY PROFESSIONALS

Travis D. Breaux, CIPT
Executive Editor

An iapp publication

Contents

Preface

Since the first edition of this book, *Introduction to IT Privacy*, was published in 2014, we have observed significant new advances in information technology and public policy that affect privacy. In many ways, this eight-year period tells a story where technologies that historically lived in research laboratories have seen wider commercial adoption as new forms of automation. These technologies include autonomous and semiautonomous vehicles, voice-activated assistants, smart devices and biometrics. While the conveniences afforded by some forms of automation are still being understood, the deployment is already raising new privacy challenges. Google Glasses, the eyeglasses that could snap photos and later record video, were introduced in 2012 and quickly raised questions about reasonable expectations of privacy in public spaces. While this technology did not become mainstream with the public, voice-activated smart speakers, which consumers deploy in their homes and use to check the weather and play music, are quite popular, with multiple manufacturers competing for market share, including Amazon, Apple and Google.

The privacy risks introduced by these technologies are varied, including new ways to acquire personal data, new ways to build richer personal profiles, and new challenges in discerning the truth about a person from mere fabrication. Machine learning and robotics, for example, have led to commercial drones that allow individuals to more easily acquire overhead video and sensor data, smart televisions that detect which content is being viewed and then share this information with device manufacturers, and health sensors that track real-time fitness and blood pressure. These advances in many ways integrate with and extend the smartphone revolution that led to the novel collection of real-time location by mobile apps and advertisers. Additionally, increased deployment of sensors, often to enable new consumer products and safety features, allow for the creation of richer personal profiles. In 2015, telematics devices introduced by insurance companies were capable of recording driving distances, braking patterns and speed traveled for the purpose of informing insurance rates. In 2016, a popular social media site deployed an algorithm to classify its users by their political preferences,

which contributes to other factors in behavioral profiles, such as affinities for specific racial groups. Lastly, advances in generative machine learning now allow one to create fake images and fake video, called deep fakes because they rely on deep neural networks to generate the content. This includes an app that was designed to "auto-undress" photos of women as well as an app that allows a person to speak into a camera and record audio that is transformed into the video and audio of a public personality. These technologies raise new questions about the veracity of information and the use of data to misrepresent a person's character or beliefs, potentially poisoning the public record.

Finally, in recent years, we've seen major advances in regulatory practices aimed at addressing privacy in a world where data is increasingly shared globally. In Europe, the General Data Protection Regulation (GDPR) replaces the EU Directive 95/46/EC with a major change that requires companies to obtain an individual's consent before they can build user profiles. In addition, the National Institute for Standards and Technology (NIST) conducted a series of workshops with U.S. companies, government agencies and the public to develop a framework for privacy engineering. The framework aims to guide companies in how to select actions for reducing privacy risk within their enterprise. Going forward, regulators face great challenges in ensuring that regulation keeps pace with emerging technology as it shapes how we define and promote privacy. For example, how should companies treat machine learning models trained on data of EU citizens who choose to be forgotten?

In this new edition, we enshrined advances in technology, policy and practice in updates to all the existing chapters. This includes advances in cryptographic algorithms in Chapter 2 and database reconstruction attacks and new deployments of biometric authentication services in Chapter 4. In Chapter 6, we have new material on sensor-based surveillance, due in part to the emergence of the internet of things (IoT). Chapter 7 includes new material on deep fakes as well as on fairness and bias in machine learning, and Chapter 8 has been updated to focus more on enterprise privacy for cloud computing. Finally, we added two new chapters: Chapter 5, on how to make privacy usable given that users play an increasingly large role in managing their privacy preferences; and Chapter 9, on cybersecurity and how security frameworks support protecting privacy. While these are a few highlights for the new edition, I believe you'll find this updated volume offers a single source on the topic of IT privacy that is simply unparalleled in terms of breadth and depth.

Travis D. Breaux, CIPT
Executive Editor

Introduction

A universal aspect of being a technology professional is that change is not only expected but guaranteed. Change ensures the opportunities to learn never wane—that's what keeps many of us in the profession. However, in recent years, the pace of change is both increasing dramatically and expanding to affect the broad population. People have come to expect the same quality of engagement with day-to-day technology regardless of channel or industry.

On my own journey, finding myself in the privacy industry now feels reminiscent of the early days of information security. There wasn't a roadmap on the work, just passionate, tech-savvy people who cared about making sure company assets were safe from emerging security threats.

Privacy engineering is today's equivalent. While privacy laws and guidelines have been with us for decades, to date the approach has been about terms and conditions and contractually holding suppliers and service providers accountable for company behavior. With the ever-increasing presence, dependence, and personal implications of technology on individuals, the contractual is no longer enough.

The stakes are increasing. The prevalence of internet-of-things (IoT) devices like smart watches, smart homes and smart cities is increasing both our digital footprint and its perceived value and usage. Technology has made it possible to capture and track people's movements, interests and personal information and aggregate it for marketing insights or nefarious intentions.

While technology has become a convenience for many—making it easy to order food and clothes, track our exercise or health, and keep in touch with friends and family—it has also become a necessity. Our personal and work lives frequently rely on today's technologies to simply meet day-to-day expectations. People want the convenience but are recognizing that giving up our personal data is becoming annoying, creepy or the source of lost time, data or money because of the frequency of data breaches. Additionally, incidents of malware, ransomware and identity theft are fostering distrust of technology. More and more, people are becoming fatigued by the trade-off.

Recently, however, the laws have evolved to require organizations to manage this within the technology ecosystem. Specifically, the General Data Protection Regulation (GDPR) introduced the requirement of data protection by design and by default, radically changing the paradigm from the contractual to the automatic. For technology professionals, this means a new way to design, build, test and maintain our applications, infrastructure and processes. These guidelines place the individual's needs front and center, and require protection of their rights and interests to be built in our systems, processes and infrastructure.

Today's technology professional recognizes the urgency to quickly adapt to the pace of change. The emergence of user-centric design, the wide adoption of DevOps and Agile practices, and the increased commitment to diversity and inclusion in building software today are all evidence of this recognition. In line with the now table-stakes expectations of building secure solutions, technology professionals need to adapt to the growing demand for privacy.

This book offers technology professionals a better understanding of privacy issues and their implications for today's technology solutions, processes and infrastructure. Any person in the technology solutions ecosystem will benefit from the concepts, guidelines, tools and frameworks available in this book to ensure privacy by design in their solutions. Further, the book will give tech-savvy professionals a common language with which to speak with lawyers, compliance officers, business stakeholders and others involved in the definitions needed to design, build, test and maintain solutions with privacy in mind.

Cathleen R. Scerbo
Vice President and CIO
International Association of Privacy Professionals