

## **Privacy and Technologies of Identity, A Cross-Disciplinary Conversation**

Edited by: Katherine Strandburg and Daniela Stan Raicu

New York, NY: Springer Science+Business Media, Inc., 2005, ISBN: 0-387-26050-1

(Price: \$129), pp. 383

Reviewed by: Sarah C. Smith

Journal of High Technology Law

Suffolk University Law School

---

As new technologies emerge, the challenge of keeping one's identity private increases. New companies continue to develop innovative methods to track merchandise, target customers, and market new products. Furthermore, in the new era after September 11<sup>th</sup>, 2001, law enforcement agencies are seeking new ways to investigate potential threats to our national security. On the other end of the spectrum is an individual worried about identity theft, junk mail, and whether these new technologies are legal. These are some of the many topics broached in a new book edited by Katherine Strandburg and Daniela Stan Raicu entitled *Privacy and Technologies of Identity, A Cross-Disciplinary Conversation*. Developed out of a symposium at the DePaul University in October 2004, Strandburg and Stan Raicu compiled abstracts of books, law review articles and other articles related to privacy and technology.<sup>1</sup> The book is divided into five main parts: an overview of the issues surrounding privacy and technology, the use of tracking devices such as radio frequency identification (RFIDs), biometrics, data-mining and other targeted marketing and some of the implications of using some of these new technologies including potential legal conflicts. Scholars from various disciplines including legal, social science, and computer science describe how technology impacts our privacy.

---

<sup>1</sup> The CIPLIT 2004 Symposium, Privacy and Identity: The Promise and Perils of a Technological Age was held at DePaul University and organized by various departments at the university.

## Part I: Introductory Issues in Privacy and Technology

The first three articles discuss the tension that exists between emerging technologies and individual privacy rights. In Daniel J. Solove's piece adapted from his book, *The Digital Person: Technology and Privacy in the Information Age*, he writes that although computers are very useful, they also enable database compilers to collect information for almost every person in the United States and then sell that information to the highest bidder. In Alessandro Acquisti and Jens Grossklags' survey, *Privacy and Rationality*, they write that while people want to protect their privacy, their actions do not always make the choices necessary to protect their privacy. Similarly, in Katherine J. Strandburg's excerpt, *Social Norms, Self Control, and Privacy in the Online World*, she argues that the desire for privacy is not always easy to achieve in the information age. Behavioral issues that are common in every day life such as self-control and temptation also exist in cyberspace.

## Part II: Privacy Implications of RFID and Location Tracking

The next three articles discuss RFIDs and other emerging location tracking devices such as GPS (global positioning systems) and some of the related privacy implications.<sup>2</sup> In Ari Juels's article *RFID Privacy*, he discusses how RFIDs are becoming a popular tool for tracking merchandise and sales. Yet, the signal controlling the RFID may not be "killed" when the merchandise leaves the store or warehouse leaving the customer vulnerable to ongoing monitoring after their purchase. In Mark Monmonier's article, *Geolocation and Locational Privacy, The "inside" story on geospatial tracking*, he writes about the dual use of RFIDs and GPS technologies and how they can be used to compliment one another. As this book suggests,

---

<sup>2</sup> A RFID chip is a tiny, wireless chip that contains a silicon microprocessor and an antenna so that it can be read by a radio-emitting scanner.

there are potential privacy implications and lawmakers have passed legislation to combat this problem. However, the underlying problems still exist. In Paul M. Schwartz's excerpt, *Privacy Inalienability and Personal Data Chips* (from his law review article entitled, *Property, Privacy and Personal Data*), he describes how privacy should be protected using his "privacy-sensitive model" that addresses five areas: "inalienabilities, defaults, a right of exit, damages and institutions."<sup>3</sup> For example, Schwartz advises using an "opt-in" as opposed to an "opt-out" default to force those who want to use the information to develop effective methods to ensure privacy.<sup>4</sup>

### Part III: Privacy Implications of Biometric Technologies

The next three articles all discuss the privacy implications of biometric technology. In Ishwar K. Sethi's article, *Biometrics*, he is concerned about the religious, informational privacy and physical privacy concerns surrounding the use of these biometric applications.<sup>5</sup> In Gang Wei and Dongge Li's article, *Biometrics: Applications, Challenges and the Future*, they discuss their concerns about the accuracy of biometrics. Furthermore, they write it is questionable as to whether people are willing to volunteer their identities in order for this technology to function effectively. Legally, Lisa S. Nelson's article, *Constructing Policy, The unsettled question of biometric technology and privacy*, argues that the current legislation is not adequate to address the privacy concerns regarding the use of biometrics. In John A. Stefani's article, *Finding Waldo, Face recognition software and concerns regarding anonymity and public*

---

<sup>3</sup> Paul M. Schwartz's excerpt, *Privacy Inalienability and Personal Data Chips* (from his law review article entitled, *Property, Privacy and Personal Data*), Privacy and Technology of Identity, A Cross-Disciplinary Conversation 93 (Katherine Strandburg & Daniela Stan Raicu, eds., Springer Science+Business Media, Inc. 2005).

<sup>4</sup> Paul M. Schwartz's excerpt, *Privacy Inalienability and Personal Data Chips* (from his law review article entitled, *Property, Privacy and Personal Data*), Privacy and Technology of Identity, A Cross-Disciplinary Conversation 99-102 (Katherine Strandburg & Daniela Stan Raicu, eds., Springer Science+Business Media, Inc. 2005).

<sup>5</sup> Biometrics is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. These include: fingerprints, eye retinas and irises, facial patterns, gait and the human voice. <http://www.wikipedia.com>.

*political speech*, he argues that due to the protections of the First and Fourth Amendments, face-recognition software should not be used in public surveillance cameras.

#### Part IV: Privacy Implications of Data Mining and Targeted Marketing

Five articles are devoted to the very controversial issue of data-mining and targeted marketing. In Christopher W. Clifton, Deirdre K. Mulligan and Raghu Ramakrishnan's article, *Data Mining and Privacy: An Overview*, they argue that the data used, not the data-mining process itself, is what is controversial. They believe that data-mining is controversial when the "nature and origin of the data, or the role played by the public sector agencies" is questionable.<sup>6</sup>

In Tal Z. Zarsky's article, *Online Privacy, Tailoring, and Persuasion*, illustrates the sheer volume of information that can be found online can lead to a debate on how best to protect individual privacy. Zarsky writes that compounding this problem of protecting privacy is the lack of a working definition of what privacy is, how and where it is being eroded and even why privacy is important.

Eric Goldman writes in his article, *Data Mining and Attention Consumption*, that data-mining in itself is not a bad technology, but that the concept of data-mining must be differentiated into data collection and data disclosure. Goldman believes that it is only when the data is *used* or *disclosed* that it can be harmful.

In Dennis D. Hirsch's article, *Is Privacy Regulation the Environmental Law of the Information Age?*, he argues that environmental laws written to correct the problems associated with pollution from the Industrial Revolution should be used to correct the problems associated with invasions of privacy from the Information Revolution. He believes that the Information

---

<sup>6</sup> Christopher W. Clifton, Deirdre K. Mulligan and Raghu Ramakrishnan, Privacy and Technology of Identity, A Cross-Disciplinary Conversation 196 (Katherine Strandburg & Daniela Stan Raicu, eds., Springer Science+Business Media, Inc. 2005).

Revolution affects our privacy in two ways: it has decreased our ability to control information about oneself and unwanted “spam” invades our “virtual space.”<sup>7</sup>

In Dilek Hakkani-Tur, Gokhan Tur, Yücel Saygin, and Min Tang’s article, *Document Sanitization in the Age of Data Mining*, they focus on finding ways in which to protect private textual information from data-miners. They argue that in order to protect our privacy we must sanitize our information to disable data-miners access to it.

#### Part V: Implications of Technology for Anonymity and Identification

The final five articles involve the implications of technology on our privacy. In Ian Kerr and Alex Cameron’s article, *Nymith, P2P & ISPs, Lessons from BMG Canada, Inc. v. John Doe*, they argue that the unintended consequences of the *BMG Canada, Inc. v. John Doe* case may lead to private-sector surveillance of online activities. The authors write that while the case itself protected privacy, the recording industry lost because it did not have adequate evidence to prove its case. They argue that this in turn will lead to invasions of privacy because the companies will first gain the necessary evidence before it initiates a lawsuit.

In Daniel J. Steinbock’s article, *Fourth Amendment Limits on National Identity Cards*, he examines the legal and privacy issues surrounding the implementation of a national identity system in the United States. Using the Fourth Amendment’s unreasonable searches and seizures analysis, Steinbock argues that although the government’s use of a national identity system would be limited, the system would be legally permissible.

In Arthur M. Keller, David Mertz, Joseph Lorenzo Hall, and Arnold Urken’s article, *Privacy Issues in an Electronic Voting Machine*, they discuss how the Open Voting Consortium (OVC) is developing a computer system that will mimic the paper ballot system while still

---

<sup>7</sup> Dennis D. Hirsch, Privacy and Technology of Identity, A Cross-Disciplinary Conversation 241 (Katherine Strandburg & Daniela Stan Raicu, eds., Springer Science+Business Media, Inc. 2005).

maintaining the privacy of the voter. The authors believe since the voter must identify him/herself before voting, it is possible to identify the specific ballot the voter used. Therefore, security and reliability are key components to any future success of the OVC model.

Yuval Elovici, Bracha Shapira and Yael Spanglet's article, *Hidden-Web Privacy Preservation Surfing (Hi-Wepps) Model*, discusses a new technology called, Hi-WePPS, may help internet surfers protect their privacy while online. While surfing the internet, a user leaves a trail that is relatively easy to track. The idea behind the Hi-WePPS is to create a false trail in order to "confuse" the tracker from discovering the real user's identity without the need for anonymity.

In Trainan Marius Truta, Farshad Fotouhi and Daniel Barth-Jones's article, *Global Disclosure Risk for Microdata with Continuous Attributes*, they argue that the more data is modified from its original form, the better it is protected. The authors tested this theory by introducing global disclosure risk measures (minimal, maximal and weighted) and found that these measures minimize disclosure of protected data. Soon the authors plan to test their theory on actual financial data.

I chose *Privacy and Technology of Identity* to learn more about RFIDs in conjunction with the Fourth Amendment of the United States Constitution. However, after reading this book I found it to be an excellent resource for numerous areas of privacy and technology issues currently facing the Information Age. Since the book compiles excerpts of books and articles, the reader is able to quickly begin research on a topic before going to the original source to learn more. Although some readers may be ignorant of some of the technical jargon, the overall idea that technology jeopardizes individual privacy is clear. Each article builds upon this idea. The number of times a person reveals information about oneself either knowingly or unknowingly

was alarming. Yet, as the book suggests, the conversation as to how to solve the problem is ongoing. The numerous authors suggests ways in which legal, political and social outlets can be used to limit the amount of data put into cyberspace. However, the reasons why the data is collected for marketing, political, social and legal reasons will not disappear any time soon. The Information Age is part of our daily lives. Computers continue to grow in size and capacity. Microchips and processors continue to shrink in size as the speed with which they collect data increases. Hopefully these authors and many more will continue to develop new ways to balance the competing interests of technology and privacy. I would recommend this book for anyone who is interested in gaining an introduction to some of the issues surrounding technology and privacy.