Privacy Laws, Technological Developments, and Their Impact on You
Review of: *Understanding Privacy and Data Protection: What You Need to Know*

Timothy J. Toohey
Thomson Reuters/ Aspatore, United States, 2014
ISBN: 978-0-314-29194-3
Price: $28.99, pp. 178

Reviewed By: Anthony Gatto
Journal of High Technology Law
Suffolk University Law School

"*Data privacy and security issues that once were the province of geeks and a small cadre of cybersecurity lawyers now feature almost daily in the news."*[1]

Data privacy impacts millions of people across the globe yet how many people have tried to navigate through the maze of laws and regulations which govern this field? In *Understanding Privacy and Data Protection*: *What You Need to Know*, author Timothy J. Toohey explores the legal framework and ongoing trends affecting privacy and data security.[2] Toohey suggests that despite the complexities of the field, it is more than ever important for businesses and consumers alike to understand this legal framework and his book provides invaluable guidance about privacy laws and technological developments that impact privacy.

The book could not have been written by a more qualified individual. Mr. Toohey received his JD from Boalt Hall School of Law and holds a PhD in history from Harvard University. In addition, Mr. Toohey has attended Stanford University and Oxford University as a Rhodes Scholar. Currently, Mr. Toohey is a partner with the Los Angeles law firm Morris Polich & Purdy LLP where he is the head of the firm's Cyber, Privacy, and Data Security team. He holds the titles of United States Certified Information Privacy Professional (CIPP/US) and European Union Certified Information Privacy Professional (CIPP/E). Mr. Toohey has spoken

---

[1] TIMOTHY J. TOOHEY, UNDERSTANDING PRIVACY AND DATA PROTECTION: WHAT YOU NEED TO KNOW 12 (Thomson Reuters/ Aspatore 2014).
[2] *See* Toohey, *supra* note 1, at 10.

and written widely on privacy, data security, and technology with his recent publications including: *The Balance Between Data Flow and Privacy: A United States Perspective* and *Piracy, Privacy, and Internet Openness: The Changing Face of Cyberspace Law*. In addition to these professional accomplishments, Mr. Toohey teaches courses in United States Constitutional History and Legal History.

Mr. Toohey's book begins by introducing the reader to certain hypotheticals which demonstrate how millions people every day can be affected by data privacy. These hypotheticals include: a social media account being hacked, a telemarketer getting ahold of your cellphone number, and a password encryption problem at work.[3] Toohey then informs the reader that all of these hypotheticals are based on real world events of which most ended in lawsuits.[4] The tone he uses forces the reader to take this information as a warning that everyone is vulnerable to such unfortunate events.

After the introduction full of real world hypotheticals, chapter one introduces to the reader the various legal and social definitions of the word "privacy." Toohey lists certain information that people consider "private" and goes on to provide a working definition of the term "data privacy" which he communicates as "claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] Chapter Two focuses on U. S. Federal Privacy and Data Protection Laws while chapter three focuses on U.S. State Privacy laws. These chapters highlight the various state and federal laws in the U.S. that cover data privacy. In particular, these chapters educate the reader on the country's lack of a comprehensive federal data privacy law and the freedom of the individual states act where the federal government has not. Mr. Toohmey warns

[3] *See* Toohey, *supra* note 1, at 8.
[4] *See* Toohey, *supra* note 1, at 8.
[5] *See* Toohey, *supra* note 1, at 19 (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Bodley Head Ltd, 1967)).

businesses and consumers of the complexity involved in trying to determine what data laws apply to different jurisdictions.[6]

The book continues to educate the reader on data privacy laws but shifts its focus in chapter 4 to International data privacy and protection laws. With a globalized world connected through technology, this chapter reminds the audience that it is important to be aware of data privacy laws anywhere they conduct business or have employees.[7] The chapter briefly traces the history of the European privacy laws and goes on to explain the important parts of the framework that governs data protection in the European Union known as "The European Data Protection Directive."[8] The reader is then introduced to the idea of "cross-border" frameworks such as the EU/U.S. Safe Harbor Principles, which will ensure customers that a company adhering to these principles is deemed to have "adequate: privacy protection.[9] The chapter concludes by briefly explaining the privacy laws in Mexico, Australia, and various Asian countries.

Up to this point, the book educates readers on the various state, national, and international privacy laws. Chapter five adds to the list of privacy laws by exploring privacy issues in the workplace. One of the more interesting topics of this chapter is the section designated to companies who have implemented a "Bring Your Own Device" (BYOD) approach. Under this approach, companies allow employees to bring their own electronic devices to work such as laptops, tablets, iPads, and cell phones and utilize these devices for work purposes.[10] As Toohey explains, this approach causes a "blurring" of the terms "private" and

[6] *See* Toohey, *supra* note 1, at 53.
[7] *See* Toohey, *supra* note 1, at 64.
[8] *See* Toohey, *supra* note 1, at 65.
[9] *See* Toohey, *supra* note 1, at 68.
[10] *See* Toohey, *supra* note 1, at 86.

"personal" and causes much confusion when employees are compelled to turn over "personal" devices to corporate officials in the event of a lawsuit.[11]

Chapter six demonstrates how crucial data privacy and protection is by examining the topic of data security and breaches. The chapter describes some of the financial consequences a corporation suffers as a result of a breach, informing the reader that the average total organizational cost of a data breach in the United States is $5,403,644.[12] It then goes on to discusses the corporate liability for breaches imposed by state law, federal law, data breach notification laws, and other self-governing codes and regulations. The topics of this chapter create a smooth transition into chapter seven which describes the role of the Federal Trade Commission (FTC) as the nation's privacy and data security "watchdog."[13] The chapter describes the range of the FTC's powers and enforcement priorities. In particular, the chapter explains enforcement actions the FTC has taken against such corporate giants as Google, Facebook, Twitter, Myspace, and Wyndham Hotels.[14]

Chapter eight appropriately follows chapter seven by expanding on the topic of enforcement actions, but this chapter covers a different kind of enforcement action- namely, the litigation of lawsuits by private parties against businesses. Most notably are AOL's agreement to settle a class action suit for $5 million, Google settling a suit for $8.5 million, and Facebook settling a suit for $9.5 million for the use of what was then known as its "Beacon" program.[15]

Chapter nine again shifts focus and introduces a discussion on government surveillance and privacy. The chapter begins by explaining surveillance under U.S. Law and describes some of the effective and efficient ways government agencies such as the FBI use surveillance

[11] *See* Toohey, *supra* note 1, at 86.
[12] *See* Toohey, *supra* note 1, at 91.
[13] *See* Toohey, *supra* note 1, at 105.
[14] *See* Toohey, *supra* note 1, at 108-111.
[15] *See* Toohey, *supra* note 1, at 120-23.

technology in areas including counterterrorism and homeland security. The chapter then discusses the more controversial issues of surveillance by examining the constitutionality of U.S. government surveillance programs. The chapter concludes by giving a brief, yet highly informative analysis of the recent events of the NSA and "whistleblower" Eric Snowden.[16]

The remaining two chapters of the book covers the recent trends in data privacy protection and suggestions on the proper infrastructure for data privacy protection in a home or business since there is no "one size fits all" infrastructure.[17] The book concludes with a "Frequently Asked Questions" section which includes the questions and answers to forty seven questions.

Overall, the book is a very informative read. The author does an outstanding job of writing to an audience with a wide range of data technology familiarity. If you're new to the data technology field, the author writes in a way that you will not be highly confused. If you're a seasoned veteran to the field, this book is also written in a way not to bore you to death. However, if you are looking for analysis, this book is not for you. There is little analysis by the author and the book almost reads like a study guide for a Law School Exam. It is very informative and could be valuable for an audience that needs to learn about various areas of data privacy and protection in a short time. Contrastingly, if you are looking for a book that includes new theories, or a fresh prospective, this is not it. But providing new theories or a detailed analysis of data privacy was not the overall goal Mr. Toohmey was trying to accomplish by writing this book. Toohmey sought to write a book that could help businesses and consumers alike to understand the legal framework, privacy laws, and technological developments in the field of data privacy and protection. He achieved his goal by writing this book.

[16] *See* Toohey, *supra* note 1, at 130-134.
[17] *See* Toohey, *supra* note 1, at 150.