Chapter 1

Introduction and Overview

**Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski,
Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano**

Abstract This chapter introduces the book *Modern Socio-Technical Perspectives on Privacy*. The book informs academic researchers and industry professionals about the socio-technical privacy challenges related to modern networked technologies. This chapter provides a working definition of privacy, describes the envisioned audiences of this book, and summarizes the key aspects covered in each chapter. The chapter concludes with an invitation to join our community of privacy researchers and practitioners at modern-privacy.org.

B. P. Knijnenburg (✉)
School of Computing, Clemson University, Clemson, SC, USA
e-mail: bartk@clemson.edu

X. Page
Brigham Young University, Provo, UT, USA
e-mail: xinru@cs.byu.edu

P. Wisniewski
College of Engineering and Computer Science, University of Central Florida, Orlando, FL, USA
e-mail: pamela.wisniewski@ucf.edu

H. R. Lipford
College of Computing and Informatics, UNC Charlotte, Charlotte, NC, USA
e-mail: richter@uncc.edu

N. Proferes
School of Social and Behavioral Sciences, Arizona State University, Tempe, AZ, USA
e-mail: nicholas.proferes@asu.edu

J. Romano
Google, New York City, NY, USA
e-mail: jennifer@romanocog.com

© The Author(s) 2022

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_1

1.1 Introduction

Privacy issues are intricately tied to real-world implementations of modern online systems, with many users lamenting a lack of understanding about and control over the personal data collected by online entities [1]. Academics and industry professionals who wish to address these issues must familiarize themselves with the various socio-technical aspects of privacy that affect the user experience of modern networked technologies. This book gives researchers and professionals a foundational understanding of online privacy as well as insight into the issues that are most pertinent to modern information systems, covering several modern topics (e.g., privacy in social media, IoT) and underexplored areas (e.g., privacy accessibility, privacy for vulnerable populations, cross-cultural privacy). It draws upon the latest works by authors in the networked privacy research community (c.f., [2–7]), which is growing quickly as the discourse about and around privacy is becoming increasingly prominent in academia and in the public.

The consensus among this research community is that the term “privacy” is complex, misunderstood, and often misused in empirical human-computer interaction (HCI) research as well as in public discourse [8]. Thus, this introductory chapter starts by exploring the question of “What is Privacy?” With a baseline definition of privacy in place, this chapter then provides a description of the structure of the book, highlighting the key takeaways of each chapter in the context of this volume as a whole. We conclude this chapter with an invitation to join our growing community of researchers and professionals seeking to address the privacy challenges that lie ahead.

Who should read this book? While we purposefully present this book as an academic text, with arguments backed up by a vast and carefully cited body of academic literature, it was written and compiled with the explicit aim of bridging the divide between academia and practice. As such, our primary goal is to inform IT students, researchers, and professionals about both the fundamentals of online privacy and the issues that are most pertinent to modern information systems. It consists of short chapters that provide an overview on each topic and gives concrete advice for researchers and practitioners. Particularly, we envision the following audiences:

- **Teachers of undergraduate IT students** can assign (parts of) this book for a “professional issues” course or assign specific chapters in the “domains” section as part of a course on said domains (e.g., IoT, social media, healthcare, or personalization). We particularly recommend the “Privacy Frameworks” (Chap. 2), as it introduces the various lenses through which privacy can be discussed.
- **IT professionals** are encouraged to select chapters covering domains and audiences relevant to their field of work, as well as the “Moving Forward” chapters that cover ethical and legal aspects. Each chapter contains a number of bullet-point lists that serve as a shortcut to the content presented in the preceding or subsequent section.

- **User researchers in the IT industry** are advised to start with the “Privacy Frameworks” (Chap. 2) and should subsequently focus on those chapters in the “audiences” section that fit their target user profiles. The “Moving Forward” section will help them provide an ethical and legal context to their work, and the final “Bridging Privacy to Practice” (Chap. 19) will help them understand the main privacy-related issues that are currently being discussed in the industry.
- **Academics outside the field of privacy** who are interested in studying privacy or privacy-related topics will likely be most interested in the chapters in the “theory and methods” section of this book, as these chapters cover the most prominent academic approaches to the study of privacy. Their selection of subsequent chapters will depend on their particular area of research.

1.2 What Is Privacy?

There is a wide range of privacy theories and frameworks that approach the topic in different ways. Some classify information types by sensitivity [9, 10], others focus on privacy as awareness and control of information [11], and still others approach it from a state-based perspective where there are different privacy states that affect how we engage with others (e.g., anonymity, intimacy) [12]. Underlying these various approaches are some fundamental differences in how privacy is conceptualized. For instance, much of European law frames privacy as a fundamental human right that must be protected [11]. However, American society often treats privacy as a commodity that can be bought and sold and that can be weighed against other benefits and drawbacks [11]. In terms of benefits, privacy is not only an important right for individuals but also crucial to freedom of speech and democracy [13]. Hand in hand with this debate is whether privacy is a means toward other goals (e.g., creativity, democracy, character development) or whether privacy is a desirable end-state in itself, as assumed in some frameworks where the goal is a state of privacy (e.g., solitude) [14]. There are also more technical definitions of privacy, such as those used for differential privacy, which treats privacy as the level of obfuscation of algorithmically generated noise in data [15]. As one can see, defining privacy is not a simple matter.

Another debate about privacy is whether it is an individual good or a societal good [11]. For instance, interface designers may treat privacy as an individual-level decision, where a user defines what is the right level of privacy by customizing a setting or choosing a permission default [10, 16]. However, recent research recognizes that privacy also serves a societal goal, and more collective conceptualizations of privacy (see Chap. 6) should be used in the design of systems [17, 18]. This leads to tensions between satisfying the desires of an individual versus the needs of groups, or even societies as a whole.

While we have left the authors of each chapter to select their own specific definition of privacy and theoretical lens through which it is studied, we acknowledge that most existing works on socio-technical aspects of privacy employ one of the

frameworks that is covered in the “Privacy Frameworks” (Chap. 2) in this book. Fundamentally, we want to make the readers of this book aware of the ephemeral nature of the concept of privacy, specifically the following:

- **Privacy is a complex, multifaceted concept** that has been defined in numerous ways—from legal to normative definitions—that uncover important and differing aspects of networked privacy. Whereas technical definitions of privacy tend to be precise but narrow, the broad and complex nature of privacy is a defining characteristic of the concept as a socio-technical phenomenon.
- **Being aware of different privacy theories and frameworks** is the first step toward advancing modern privacy. Since no single definition can adequately capture every facet of privacy, we have asked the authors of individual chapters to emphasize the theoretical lens through which they view their work. Readers are advised to study the relevant theoretical lenses so as to gain a more fundamental understanding of the presented material.
- **Privacy is contextual**—this is a shared element of all existing privacy theories and frameworks (cf. [19]). Hence, the second step toward advancing modern privacy is to avail oneself of the key concerns in different contexts and the privacy norms and needs for different populations.
- **Being aware of diverse privacy perspectives** can help researchers, practitioners, and policy-makers ensure that they are considering privacy holistically and not unintentionally missing key components.

The remainder of this chapter briefly discusses the broad spectrum of privacy perspectives covered in the rest of this book.

1.3 Privacy Theory and Methods

There is no single theory that covers the concept of privacy as it shapes—and is shaped by—our everyday experiences. The “theory and methods” section of this book therefore covers a range of theoretical lenses through which one can view the concept of privacy. The chapters in this section relate to “modern” privacy phenomena, thus emphasizing its relevance to our digital, networked lives, but they can equally be applied to “real-world” situations (which, of course, rarely escape the influence of the digital world anyway).

“Privacy Frameworks” (Chap. 2) is an overview chapter that demonstrates how research frameworks developed in academia can support privacy research, design, and product development. It covers definitional perspectives on privacy as information disclosure, as interpersonal boundary regulation processes, and as prescriptive reflections on information flows. Furthermore, it explains how privacy can be construed as a design objective or a target for personalization. This chapter is foundational and will help the reader deepen their understanding of subsequent chapters.

“Revisiting APCO” (which stands for Antecedents, Privacy Concerns, and Outcomes) introduces the most prominent perspective on privacy from the field of Information Systems. This model was first developed in a foundational literature review by Smith et al. [20] and later updated by Dinev et al. [21]. The model was specifically developed to theorize how root causes of users’ privacy concerns connect to specific behavioral outcomes and actions. The chapter focuses on the model’s use in research and its applicability to design processes while simultaneously highlighting the limits of the model in explaining user behavior.

“Privacy and Behavioral Economics” (Chap. 4) examines the different streams of research in the area of judgment and decision-making that attempt to study complex privacy behaviors in different scenarios. It focuses on three themes in this research: (1) individuals’ uncertainty about their own preferences and desires in terms of privacy, as well as the uncertainty and difficulty they face in predicting the consequences of particular information disclosures, (2) the context dependence of individuals’ privacy concern, and (3) the degree to which privacy concerns are malleable and prone to manipulations by different actors.

“The Development of Privacy Norms” (Chap. 5) presents a social-theoretical perspective on privacy. This chapter examines how what we consider appropriate information flows in any given situation is shaped by particular norms. Privacy norms are socially constructed and evolve over time, particularly as new networked and persistently listening technologies have been introduced into society. The chapter details how we develop, revisit, and negotiate norms around privacy when faced with new technologies.

The final chapter in this section covers “Privacy Beyond the Individual Level” (Chap. 6). Acknowledging that privacy increasingly revolves around the actions of multiple actors, this chapter discusses several contemporary situations where “group privacy” is relevant, such as tagging on social networks, privacy in workplace teams, life logging, and AI-based inference technologies. The chapter details the dynamics of the multi-stakeholder privacy decisions that occur in these situations, examining potential tensions that exist between the rights and preferences of individual group members or between individuals and the group as a whole. Finally, the chapter outlines tools and other mechanisms that can support collaborative privacy management and group privacy protection.

1.4 Domains

While privacy permeates all aspects of modern life, there are a number of domains in which privacy concerns and implications are particularly salient. The “domains” section of this book covers a number of these domains—some of which are well established, while others are emergent. We want to emphasize that these domains (and their privacy implications) are continually evolving and that the emergence of novel socio-technical domains is a regular occasion. Hence, we advise readers to

treat these chapters as introductions to their respective topic areas and encourage them to conduct a subsequent investigation into the state of the art.

“Social Media Privacy” (Chap. 7) describes various types of social privacy concerns, covering public versus private information disclosure, imagined audiences and context collapse, self-presentation and impression management, and issues of availability and physical access. Furthermore, the chapter explains how social media users regulate different interpersonal boundaries on social media: relationship (regulating appropriate interactions with others based on relationship type), network (who is in my network), territorial (where content can be posted), disclosure (what information is shared), and interactional boundaries (what social interactions are acceptable). The chapter emphasizes the importance of designing social media with individual differences between users in mind and ends by pointing out the negative consequences of not addressing social media users’ privacy concerns.

The chapter on “Privacy Enhancing Technologies” (Chap. 8) covers technological solutions that can prevent or limit privacy violations. It covers protocols that can be used to secure communication channels (secure messaging, email, and HTTPS), authenticate data access (two-factor authentication), and anonymize our interactions on the Internet (Tor). It presents existing work from the usable security community describing users’ issues with these technologies and outlines research directions to help improve their usability and support their adoption.

“Tracking and Personalization” (Chap. 9) are at the heart of many modern mobile and online experiences. This chapter covers the various uses of personalization—ranging from recommender systems and intelligent user interfaces to user-tailored and context-aware advertisements—and discusses how user tracking powers these use cases. It then covers the downsides of user tracking and the various ways in which companies can misuse tracking to infer private information about users and/or engage in price discrimination or invasive advertising practices. The chapter concludes with a discussion of recent and potential future work to improve the balance between personalization benefits and concerns about tracking. This includes practical considerations around state-of-the-art privacy-preserving personalization practices for system developers willing to strike this balance.

The chapter on “Healthcare Privacy” (Chap. 10) describes sources of privacy threats that have accompanied digitization of healthcare. It emphasizes the complex environment in which health information is shared, involving practitioners, labs, clinics, hospitals, medical organizations, health insurance companies, as well as the patients themselves and their family members. It also notes how health information is often dispersed, not only in official health records repositories but on mobile devices, as it is transferred to different stakeholders and even shared on personal or public social media and online forums. The chapter describes a range of applicable policies and legal regulations, including HIPAA, and the type and location of data that is regulated under these various policies. It acknowledges an important deficiency of existing policies: they regulate neither the data collected by health monitoring and fitness sensors nor the data that is shared via social media, online communities, and mobile apps. The chapter highlights genetic data as a novel area that is not well regulated, especially given that it is difficult to anticipate the privacy

issues that may arise from such data. Throughout the chapter, the reader will find practical recommendations, tailored to different stakeholders, touching on how to share information appropriately using adequate technical protections.

The “domains” section ends with a chapter on “Privacy and the Internet of Things (IoT)” (Chap. 11). It covers household IoT (smarthomes), public IoT (smart cities, smart buildings, and self-driving cars), and wearable IoT (fitness trackers, smartwatches). It covers how these technologies are used for security and safety, remote access and automation, resource management, wellness monitoring, and entertainment. It subsequently covers the main problems that particularly apply to (or are particularly prominent in) the IoT domain. Particularly, it discusses the fact that many IoT systems operate outside the user’s awareness, making privacy issues less salient. Moreover, most IoT devices give those who are being observed by them little (household/wearable IoT) or no (public IoT) control over their privacy settings. Even when such settings are available, interacting with them is particularly difficult due to the lack of a visible interface. Aside from this, the active presence of IoT devices intrudes upon our daily lives and may alter our behavior, and their always-on nature means that they accumulate a lot of data that can be used to make far-reaching inferences about the user and/or be vulnerable to hackers. Finally, the chapter acknowledges that IoT systems may reveal personal information to its multiple users (e.g., households) and that they may face difficulties in reconciling the privacy preferences of their multiple users.

1.5 Audiences

Recurring privacy surveys that started in the early 1980s have consistently found a substantial diversity in privacy concerns and behaviors across the population [12]. Taking this diversity of concerns and practices into account is a major challenge for corporations that wish to respect the privacy preferences of the audiences that use their platforms or services. The “audiences” section of this book highlights audiences that have traditionally been ignored when creating privacy-preserving experiences: people from other (non-Western) cultures, people with accessibility needs, adolescents, and people who are underrepresented in terms of their race, class, gender or sexual identity, religion, or some combination.

The first chapter in this section covers “Cross-Cultural Privacy Differences” (Chap. 12). The increasingly global nature of social networking sites as well as the broader information economy has revealed an urgent need to study how users in different cultures manage their privacy differently. This chapter offers practical tips that can inform the privacy design for technologies that are used globally. The chapter highlights important differences in privacy decision-making between people in individualistic cultures and collectivistic cultures and makes recommendations for global social networks and global e-commerce companies based on these differences. Regarding social networks, the chapter recommends investing more effort to support collective privacy management in collectivistic countries, differentiating

mechanisms for audience control in different cultures, providing users more privacy support to protect others' privacy in collectivistic countries, and emphasizing mechanisms to support individual privacy in individualistic countries. Regarding e-commerce, the chapter recommends customizing data collection strategies and enabling different options to control personal data flow in different countries, as well as differentiating relationships between privacy perceptions and privacy decisions.

The chapter on "Accessible Privacy" (Chap. 13) focuses on the intersection of accessibility and privacy, paying particular attention to the privacy needs and challenges of people with disabilities. The chapter opens by acknowledging that people with disabilities face heightened challenges in managing their privacy. For example, people with visual impairments are more vulnerable to shoulder surfing and aural eavesdropping. Moreover, their use of assistive technologies and their need to ask others for help (in person or virtually) open them up to additional vulnerabilities. The chapter further covers how existing end-user privacy tools (e.g., CAPTCHA, authentication tools) are often inaccessible to people with disabilities, making them more vulnerable to privacy threats. In response, the chapter calls for design guidelines that support the creation of more accessible privacy tools and addresses how such guidelines should incorporate the variances among users with disabilities.

The chapter on "Privacy in Adolescence" (Chap. 14) covers the unique developmental life stage where teens transition between childhood and emerging adulthood, distancing themselves from their parents. It acknowledges that teenage years are characterized by increased sociality and peer pressure, the need for more autonomy and privacy, as well as heightened risk-seeking behaviors. The chapter addresses how existing tools for monitoring teens online are heavily focused on parental control, using authoritarian restriction and privacy-invasive monitoring that negate the developmental needs of teens. It emphasizes that the fallacy of these tools is that they assume that teens do not care about privacy. The chapter subsequently outlines how, instead, teens' strategies are often just different from adults' privacy management strategies, requiring a different set of tools that support teen self-regulation. In particular, such tools should emphasize collaborative practices and open communication within families and give teens some leeway to make mistakes, learn from them, and be able to recover.

The final chapter in the "audiences" section covers "Privacy and Vulnerable Populations" (Chap. 15), which are defined as groups of individuals who are more susceptible to privacy violations because of their race, class, gender or sexual identity, religion, or other intersectional characteristics or circumstances. This chapter explores the role that social norms play in shaping privacy theory and how this can disadvantage members of vulnerable populations. It also covers how technologies exacerbate existing inequalities, including in terms of privacy. The chapter outlines what the specific privacy concerns and needs of certain vulnerable populations might encompass and proposes intersectional approaches to some of the biggest challenges for vulnerable communities. Finally, it explains how technologists can identify and incorporate vulnerable populations into requirements-gathering, testing, and policy-making, including a thought experiment to help guide readers as they consider how to incorporate vulnerable users into their design process.

1.6 Moving Forward

In the “Moving Forward” section of this book, we take a higher-level, systemic perspective on the field of privacy. The chapters in this section outline approaches to privacy that move beyond one-size-fits-all solutions, explore ethical considerations, and describe the regulatory landscape that governs privacy through laws and policies. Perhaps even more so than the other chapters in this book, the chapters in this section are forward-looking, in that they use current personalized, ethical, and legal approaches as a starting point for potentially groundbreaking reconceptualizations of privacy to serve the modern technological landscape. The section ends with a chapter that is the product of a series of interviews with industry professionals who were asked to comment upon the topics covered in this book.

The chapter on “User-Tailored Privacy” (Chap. 16) describes an approach to privacy that provides adaptive privacy decision support that fits the preferences and concerns of each individual user. This chapter outlines the measure-model-adapt framework that underlies user-tailored privacy. The chapter acknowledges that the plurality and multidimensionality of people’s privacy decision-making practices can only be captured via direct observation of their behaviors or via inference from their attitudes. It outlines how, depending on the situation, a user-tailored privacy system can automate people’s existing privacy practices, recommend complementary practices, or aim to move people beyond their current practices. It highlights opportunities for personalization that exist in adapting the privacy settings of an application, the means of justifying certain information requests, the interface for setting one’s privacy settings, or the tracking and personalization practices that the application employs.

The second chapter in this section is titled “The Ethics of Privacy in Research and Design: Principles, Practices, and Potential” (Chap. 17). The chapter starts with a retrospective on the past 50 years of privacy research, in which privacy contexts expanded from the individual to Internet, interdependence, intelligences, and artificiality. It discusses how each expansion has broadened the field of ethical concerns. The chapter then introduces a principlist framework to guide ethical decision-making and uses this framework to assess the challenges posed by several emerging technologies from the perspective of five ethical principles: autonomy, justice, nonmaleficence, beneficence, and explicability. The chapter ends by identifying a number of resources that codify the reasoning outcomes of ethics, including technical standards, codes of conduct, curricular programs, and statements of principles.

The next chapter complements this perspective with a policy analysis. Titled “EU GDPR: Towards a Regulatory Initiative for Deploying a Private Digital Era” (Chap. 18), it examines the global privacy policy landscape, with a particular focus on Europe’s General Data Protection Regulation (GDPR). The chapter both explains the GDPR, its evolution from previous EU privacy policies and standards, what the law requires of companies, and how it is becoming a “gold standard” globally for privacy regulation. The chapter concludes by examining other national policies which are modeled on some of the key requirements of the GDPR.

Our book concludes with a chapter titled “Reflections: Bringing Privacy to Practice” (Chap. 19). This chapter reflects on the topics covered in this book from the perspective of a number of industry professionals who were interviewed on these topics. The chapter indicates how industry researchers can benefit from academic research—specifically its longer-term perspective and its opportunity to study a broader population. Conversely, it highlights how academic researchers can look toward industry researchers to find potential areas of impact and to verify theories with a large sample in an ecologically valid setting. At the same time, the chapter acknowledges that the timelines of academic and industry research often do not match and that there are several legal and ethical barriers that preclude the sharing of industry data with academic partners. The chapter ends on a call to action, encouraging academic and industry researchers to engage in collaborative events and projects to share research ideas, outcomes, and best practices.

1.7 Conclusion

In line with the final chapter’s call to action, we end the current chapter with an invitation to join the community of editors, authors, and readers of this book at modern-privacy.org. On this Web site, we track research publications related to the topics of this book, maintain useful resources related to privacy-enhancing design, and announce upcoming events that connect privacy researchers across industry and academia. Through this site, we aim to connect you to the growing community of researchers and professionals seeking to address the privacy challenges that lie ahead. We hope that you enjoy this book and look forward to your participation!

References

1. Auxier, Brooke, Rainie Lee, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center.
2. Ayalon, Oshrat, and Eran Toch. 2017. Not even past: Information aging and temporal privacy in online social networks. *Human Computer Interaction* 32 (2): 73–102.
3. Lampinen, Airi, Fred Stutzman, and Markus Bylund. 2011. Privacy for a networked world: Bridging theory and design. In *CHI’11 Extended Abstracts on Human Factors in Computing Systems*, ACM, 2441–2444.
4. Lipford, Heather Richter, Pamela J. Wisniewski, Cliff Lampe, Lorraine Kisselburgh, and Kelly Caine. 2012. Reconciling privacy with social media. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion*, ACM, 19–20.
5. Stark, Luke, Jen King, Xinru Page, et al. 2016. Bridging the gap between privacy by design and privacy in practice. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ACM, 3415–3422.
6. Vitak, Jessica, Pamela Wisniewski, Xinru Page, et al. 2015. The future of networked privacy: Challenges and opportunities. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*, ACM, 267–272.

7. Wilkinson, Daricia, Moses Namara, Karla Badillo-Urquiola, et al. 2018. Moving beyond a “One-size Fits All”: Exploring individual differences in privacy. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, W16:1–W16:8.
8. Barkhuus, Louise. 2012. The mismeasurement of privacy: Using contextual integrity to reconsider privacy in HCI. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, ACM, 367–376.
9. Ackerman, Mark S., Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-commerce: Examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on electronic commerce*, ACM Press, 1–8.
10. Pamela Wisniewski, A. K. M., Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give social network users the privacy they want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, ACM, 1427–1441.
11. Solove, Daniel J. 2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.
12. Westin, Alan F. 1967. *Privacy and Freedom*. New York, NY: Atheneum.
13. Solove, Daniel J. 2007. “I’ve Got Nothing to Hide” and other misunderstandings of privacy. *San Diego Law Review* 44: 745.
14. ———. 2006. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (3): 477–564.
15. Dwork, Cynthia, and Aaron Roth. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science* 9 (3–4): 211–407.
16. Wisniewski, Pamela J., Bart P. Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies* 98: 95–108.
17. Dourish, Paul, and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human Computer Interaction* 21 (3): 319–342.
18. Jia, Haiyan, and Xu. Heng. 2016. Measuring individuals’ concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10: 1.
19. Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.
20. Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. Information privacy: Measuring individuals’ concerns about organizational practices. *MIS Quarterly* 20 (2): 167–196.
21. Dinev, Tamara, Allen R. McConnell, and H. Jeff Smith. 2015. Research Commentary—Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the “APCO” box. *Information Systems Research* 26 (4): 639–655.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.