Sabine Trepte
Leonard Reinecke *Editors*

# Privacy Online

## Perspectives on Privacy and Self-Disclosure in the Social Web

Springer

# Privacy Online

Sabine Trepte • Leonard Reinecke
Editors

# Privacy Online

## Perspectives on Privacy and Self-Disclosure in the Social Web

Springer

*Editors*

Sabine Trepte
University of Hamburg
Department of Psychology
Von-Melle-Park 5
20146 Hamburg
Germany
sabine.trepte@uni-hamburg.de

Leonard Reinecke
University of Hamburg
Department of Psychology
Von-Melle-Park 5
20146 Hamburg
Germany
leonard.reinecke@uni-hamburg.de

ACM Codes: K.4, K.5, K.6.5, H.4, H.5
ISBN 978-3-642-21520-9 e-ISBN 978-3-642-21521-6
DOI 10.1007/978-3-642-21521-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011932726

*Cover design:* deblik

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

Privacy is a basic human need, and losing privacy is perceived as an extremely threatening experience. Privacy embraces solitude, personal space, or intimacy with family and friends and as such, it is a ubiquitous and trans-cultural phenomenon. Privacy leverages well-being; without privacy we are at risk of becoming physically or mentally ill.

Our fundamental need for privacy is contrasted by a second powerful mechanism of social interaction: self-disclosure to others is similarly important for social functioning and psychological well-being. We need to self-disclose to bond with others, form meaningful relationships, and receive social support. A lack of ability to self-disclose causes clinical symptoms such as loneliness and depression.

Striking the right balance between creating private spaces and self-disclosure is a complex task, if not the most challenging one in interacting with others. Today, in times of online communication and the Social Web, this task is further complicated by two confusing facts:

Firstly, our online communication is usually accessible to a vast number of people. On social network sites, it is very common for several hundred online friends to have access to the personal information, status updates, and private pictures of a profile owner. In addition to these online friends as a "known audience," there are other "unknown audiences," such as advertisers who purchase the users' aggregated profile information from social media companies to address their target audiences.

Secondly, many users appear not to feel threatened in terms of their need for and experiences of privacy when communicating online. On social network sites, micro-blogs, or in forums, they publish a vast amount of information that is considered private or even intimate in other contexts. Although they are aware of their data's publicity on an abstract level, many feel free to speak and to open up to others.

Consequently, we are facing a new situation that demands answers to a variety of pressing questions: Does online self-disclosure change our need for and experiences of privacy? What are the benefits of self-disclosure online? How does the loss of informational privacy influence our online communication?

These and many more questions will be addressed in the following chapters. We are extremely grateful to the authors who contributed to this volume. All of the chapters offer new theoretical approaches to online privacy. The work presented here goes far beyond a summary of existing research: it offers new theoretical models on the psychological functioning of online privacy, novel ideas on the hows and whys of online privacy, and intriguing solutions for some of the most pressing issues and problems in the field of online privacy.

We would like to thank the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) for supporting the work and the meetings of the "Young Scholar's Network on Privacy and Web 2.0" – a group of scientists from five different countries dealing with online privacy – that have generated fruitful discussions and helped develop many of the ideas expressed in this volume. We hope that these ideas will stimulate future research and contribute to our understanding of the complex challenges to privacy in an online world.

The volume *Privacy Online* is dedicated to those that inspire us and allow for creativity, change, and new perspectives: our families, solitude, and personal space.

Hamburg, August 2011

*Sabine Trepte*
*Leonard Reinecke*

# Contents

Part I Approaches

**Part II Applications**

**Part III Audiences**

# Contributors

**Bernhard Debatin** Ohio University, Athens, OH, USA
debatin@ohio.edu

**Nicole B. Ellison** Michigan State University, East Lansing, MI, USA
nellison@msu.edu

**Paige L. Gibson** University of Illinois at Chicago, Chicago, IL, USA
plg2uic@gmail.com

**Rebecca Gray** Michigan State University, East Lansing, MI, USA
grayreb2@msu.edu

**Nina Haferkamp** Technical University of Dresden, Dresden, Germany
nina.haferkamp@tu-dresden.de

**Maren Hartmann** Berlin University of Arts, Berlin, Germany
hartmann@udk-berlin.de

**David J. Houghton** University of Bath, Bath, UK
d.j.houghton@bath.ac.uk

**Cornelia Jers** University of Hohenheim, Stuttgart, Germany
cornelia.jers@uni-hohenheim.de

**Adam Joinson** University of Bath, Bath, UK
A.Joinson@bath.ac.uk

**Nicole C. Krämer** University of Duisburg-Essen, Duisburg, Germany
nicole.kraemer@uni-due.de

**Cliff Lampe** Michigan State University, East Lansing, MI, USA
lampecli@msu.edu

**Kevin Lewis** Harvard University, Cambridge, MA, USA
kmlewis@fas.harvard.edu

**Wiebke Loosen** Hans-Bredow-Institute for Media Research at the University of Hamburg, Hamburg, Germany
w.loosen@hans-bredow-institut.de

**Wiebke Maaß** Hamburg Media School, Hamburg, Germany
w.maass@hamburgmediaschool.com

**Ben L. Marder** University of Bath, Bath, UK
b.l.marder@bath.ac.uk

**Stephen Margulis** Grand Valley State University, Grand Rapids, MI, USA
margulis@gvsu.edu

**Zizi Papacharissi** University of Illinois at Chicago, Chicago, IL, USA
zizi@uic.edu

**Jochen Peter** University of Amsterdam, Amsterdam, The Netherlands
j.peter@uva.nl

**Oliver Quiring** University of Mainz, Mainz, Germany
quiring@uni-mainz.de

**Leonard Reinecke** University of Hamburg, Hamburg, Germany
leonard.reinecke@uni-hamburg.de

**Jan-Hinrik Schmidt** Hans-Bredow-Institute for Media Research, Hamburg, Germany
j.schmidt@hans-bredow-institut.de

**Charles Steinfield** Michigan State University, East Lansing, MI, USA
steinfie@msu.edu

**Monika Taddicken** University of Hamburg, Hamburg, Germany
monika.taddicken@uni-hamburg.de

**Mike Thelwall** School of Technology, University of Wolverhampton, Wolverhampton, UK
M.Thelwall@wlv.ac.uk

**Sabine Trepte** University of Hamburg, Hamburg, Germany
sabine.trepte@uni-hamburg.de

**Patti Valkenburg** University of Amsterdam, Amsterdam, The Netherlands
p.m.valkenburg@uva.nl

**Asimina Vasalou** University of Bath, Bath, UK
minav@luminainteractive.com

**Jessica Vitak** Michigan State University, East Lansing, MI, USA
vitakjes@msu.edu

**Joseph B. Walther** Michigan State University, East Lansing, MI, USA
jwalther@msu.edu

**Mike Z. Yao** City University of Hong Kong, Hong Kong, PR China
mike.yao@cityu.edu.hk

**Marc Ziegele** University of Mainz, Mainz, Germany
ziegele@uni-mainz.de

# Part I
# Approaches

# Chapter 1
# Introduction to Privacy Online

**Joseph B. Walther**

Even before the various networks supporting online communication converged as the Internet, tensions existed between users' desires to communicate online in very personal ways and their assumptions that their disclosures would or should be treated as privileged and private. These tensions have not abated with the advent of social media. Just as it was with the most bare-bones, text-based online communities of the past, it is with contemporary media: The more users disclose of themselves, the more they may enjoy the benefits these systems have to offer. At the same time, the more they disclose, the more they risk what they themselves consider breaches of their privacy. In light of this ongoing issue, this volume is not only timely in the manner in which it addresses these tensions as they are manifest in contemporary social media platforms, it also contributes to a tradition of research on the dualism of privacy, privilege, and social interaction that online communication has incurred as far back as (or farther than) the advent of the Internet itself.

Three complicating factors that have and continue to confront users of online systems include (1) a misplaced presumption that online behavior is private, (2) that the nature of the Internet at a mechanical level is quite incommensurate with privacy, and (3) that one's expectation of privacy does not constitute privileged communication by definition.

Perhaps it is due to the analogous offline activities which online communication resembles or replaces, that many Internet users notoriously post information online which they do not anticipate will be seen by others than the specific group they imagined when posting. A personal face-to-face conversation is fleeting. A phone call is most likely to be confined to the dyad that conducts it. A social party on held private property is presumably self-contained. These settings allow participants to maintain their sense of privacy consistent with the definitions reflected in Stephen Margulis's Chap. 2, that focus on individuals determining for themselves when,

J.B. Walther (✉)
Michigan State University, East Lansing, MI, USA
e-mail: jwalther@msu.edu

S. Trepte and L. Reinecke (eds.), *Privacy Online*,
DOI 10.1007/978-3-642-21521-6_1, © Springer-Verlag Berlin Heidelberg 2011

how, and to what extent their communications are transmitted to others (except of course by hearsay rather than by duplication and transmission). The presumptions accompanying these precedent settings may be hard to dispel, and it may be difficult for Internet users (at least those who are not digital natives) to recognize that online exchanges are neither fleeting nor confined. This divergence has led to many surprises and disappointments. These include the notorious anecdotal reports of students or employees being terminated or punished as a result of posting depictions of or statements reflecting illegal, insulting, or foolish behavior on their social network profiles.

These disparities between traditional communication settings and new media may be due in large part to the mechanical infrastructure of the Internet. The *psychological* privacy afforded by communication channels may lull users into a false assumption of *informational* privacy, a central distinction that informs the thesis of Sabine Trepte and Leonard Reinecke's Chap. 6. This may be true of the phone call and the conventional letter (which can also be intercepted), as well as the Internet. But the Internet is, at its root, a store-and-forward technology. That is, in order for the Internet to work as it does it must be able to capture, retain, and transmit the information which users enter into it (see Walther 2002). This differs from face-to-face, telephonic, and written exchanges. Yet many Internet users fail to realize that something once put online more or less stays online and may be retrieved by others and replicated, despite the subsequent inclination or efforts of the original poster to protect or remove it. Moreover, the nature of systems' architectures facilitate, if not determine, the propagation of social information, an argument articulated in contemporary terms in Zizi Papacharissi and Paige Gibson's work in Chap. 7 that includes "sharability" among the characteristics defining social media's very makeup.

Users also frequently believe that the expectation of privacy that they had when conversing or posting online constitutes some legal protection against that information being shared. Although the expectation of privacy does indeed privilege certain forms of communication under US law, the domains to which these legal restrictions apply are far more narrow than many Internet privacy advocates suggest. That is, the law privileges only conversations between patients and their doctors or therapists, and attorney-client conversations. Yet the myth prevails that any conversation is privileged that took place with an expectation of privacy, however misplaced that expectation may have been, contributing to what Bernhard Debatin refers to in Chap. 5 as "ignorance and a false sense of security (that) play an important role" in users' approach to the privacy of their online postings.

This position has been propagated by numerous researchers who have argued that if Internet users believe that they communicate privately online, then it is unethical and may be illegal to analyze their messages for research purposes and that human subjects review boards should almost never allow it (Frankel and Sang 1999; see also Hudson and Bruckman 2004; McArthur 2001). Counterarguments have been raised along the lines that, again according to US legal doctrines, messages that have been captured and stored in a publically-accessible space have no privilege whatsoever (Walther 2002) aside from copyright protection (Jacobson 1999), and that the analysis of such messages requires no more human subjects protections than analyzing newspaper content. It is clear that journalists who wish to quote from publically-available online communities and other social media do so quite regularly and without seeking permission, as discussed by Wiebke Loosen in Chap. 15, and as Jan-Hinrik Schmidt discusses in Chap. 12, Twitter users "retweet" others' messages without reservation to audiences unintended by the original source. By definition and in practice, it appears, if anyone in the Internet-using public can see one's messages, the messages are in the public domain.

In light of this, educating users about their online footprints seems to be a more promising objective than to change laws or admonish researchers and other viewers to behave differently with respect to online information. As Mike Yao points out in Chap. 9, despite norms and customs affecting "privacy issues offline, to which a set of well-established cultural, social, and legal norms may be applied, the burden of online privacy protection is primarily shouldered by an individual's own conscious effort." More effective efforts should be devoted to helping users to understand the nature of the Internet in order to develop, according again to Debatin (Chap. 5), "an enlightened understanding of technology and its unintended consequences" in terms of a "*privacy literacy* that enables them to. . .make educated choices." Yao (Chap. 9) depicts what may be required in terms of shaping those choices in terms of attitudes and subjective norms, while Kevin Lewis's Chap. 8 shows how the normative behavior of one's Facebook friend network influences the behavior of privacy setting adoptions over time.

Just as history shows that controversies over online privacy are not new, it also shows that technological efforts for the protection of privacy have a long line of succession, especially in realms in which the Internet provides unique benefits to its users. In Chap. 16, Jochen Peter and Patti Valkenburg describe the unique affordances that Instant Messaging and social media offer adolescents for communication that is vital to their development. Online communication, especially that which may be done anonymously, pseudonymously, or confidentially, allows for the exploration of identity generally and for the examination of sexual identity as well.

Whereas Peter and Valkenburg limit their focus to adolescents, the use of the Internet for identity exploration and sexual exploration by adults has also been a focus of research and speculation for some time. In an adult context, similar behaviors are described in exploratory or therapeutic rather than developmental terms (Cooper et al. 1999; Turkle 1995, resp.). Such exchanges were frequently noted on Multi-User Discussions (MUDs), where the pseudonymity provided by these systems has been described as a critical enabling feature of such virtual spaces for identity exploration (Stone 1995). Yet controversy arose even within these text-only pseudonymous venues, when users who had developed strong relationships with others through their pseudonymous selves felt betrayed at the outside publication of doubly-pseudonymized quotations (see Bruckman 2002), foreshadowing quite precisely what boyd (2007, p. 2) has since characterized as the privacy-threatening aspects of social network sites ("persistence, searchability, exact copyability, and invisible audiences"). Moreover, just as MUD users developed intimacy with one another by divulging their secrets as well as their real-life names and email addresses (Jacobson 1996; Parks and Roberts 1998). Like the text-based virtual reality use of the past, "social Web use offers advantages and gratifications that increase in direct proportion to the degree of self-disclosure," according to Monika Taddicken and Cornelia Jers in Chap. 11 of this volume. Yet then as now such intimacy comes at jeopardy of privacy, just as Debatin (Chap. 5) points out that for contemporary users of social media, "their level of privacy protection is relative to the number of friends, their criteria for accepting friends, and the amount and quality of personal data provided" online. These risks can be mitigated somewhat, according to Nicole Ellison and colleagues in Chap. 3, by limitations in friending behaviors, privacy settings, and disclosures.

Another form of Internet-enabled therapeutic exchange came as users asked for and received advice on deeply personal issues on discussion systems such as Usenet News. It appears that such personally-revealing and advice-oriented exchanges remain valued activities among older Internet users today, according to Wiebke Maaß in Chap. 17. When Usenet was at its peak, individuals who posted to some of its discussions shielded their identities through the use of *anonymous remailers*. They often did so when addressing stigmatizing issues such as certain illnesses, sexual dysfunctions, or psychological problems. Anonymous remailers posted messages to Usenet without the user's identifying address (see Bacard 2010). By appending a pseudonym to the message instead, users could track which replies subsequently developed that addressed their own original posting. They could post follow-up messages using the same pseudonym via such systems. *Traceable remailers* kept a record of the original sender's address, so that other users could respond by email to the pseudonymous address, whereupon the remailer sent replies back to the original sender. Indeed, anonymity was one of the major attractions for the use of online versus offline social support (Walther and boyd 2002), where, unlike offline social support, both men and women communicated similarly (cf. Mike Thelwall in Chap. 18). Despite growing technological sophistication of anonymous remailers, their use for slander, copyright violations, or potentially subversive political whistle-blowing (much as WikiLeaks provides today) made them susceptible to international subpoenas calling on their operators to reveal the identity of users and thereby abridge the privacy such systems offered. This led the most famous of these systems, anon.penet.fi, to be shut down by its operator rather than be opened to police (see http://w2.eff.org/Privacy/Anonymity/960830_penet_closure.announce). The rise of alternative and easier-to-use web applications has displaced both MUDs and Usenet discussions to a great extent, yet as Peter and Valkenburg make clear, newer systems still benefit users' psychosocial development by providing apparently private communication opportunities.

Yet even in contemporary social media, with full view of one's name and a plethora of identifying features, users actively manage their online self-presentations, as Nicole Krämer and Nina Haferkamp detail in Chap. 10. Indeed, social network sites enable individuals the "*mass management* of real world ties," as Marc Ziegele and Oliver Quiring suggest in Chap. 13. These tendencies sit rather uncomfortably alongside Joinson and colleagues' assertion in Chap. 4 that social network sites provide to at least those whom individuals have granted certain privileges a "radical transparency" about a profile owner's self and behaviors, that may even include, as Maren Hartmann's Chap. 14 points out, the disclosure of individuals' geographic locations by their location-aware mobile phones. It is somewhat paradoxical that, on the one hand, "social network sites...are thriving on users' willingness to disclose and consume personal information," as Joinson et al. reflect, plus the fact most of one's Facebook "friends" are known to a profile owner offline to at least some extent (Ellison et al. 2007), but that, on the other hand, impression management activity remains fertile within these sites.

The paradox may be resolved to some extent by noting that impression management has limited and unintended effects. Facebook users can readily identify elements on their own profiles (including their online photos) and in those of their friends that are distorted and not quite true offline (DeAndrea and Walther in press). Although they excuse themselves and their close friends for such exaggerations, they attribute greater hypocrisy and blame for such distortions to those of their friends who they know less well. It is unclear whom individuals are trying to mislead with these inaccurate self-presentations, given the radical transparency of which Joinson and colleagues write. Perhaps it is themselves, as another part of the psychosocial development that Peter and Valkenburg describe of adolescents.

In sum, the chapters in this book offer readers much more than a thorough and contemporary treatment of online privacy and the social web. They offer a sophisticated collection of installments on topics that are quite traditional in their concern and quite under development as Internet communication technologies continue to evolve. They offer a glimpse of the future as well, not only by exploring emergent issues that are arising with new technological applications. They do so by suggesting theory-based research agendas that can guide inquiry beyon the current incarnation of social technologies, just as the privacy issues that arose with the development of earlier Internet communication technologies have morphed but remain with us today.

## References

Bacard A (2010) Anonymous remailer F.A.Q. http://www.andrebacard.com/remail.html. Accessed Mar 2011

boyd d (2007) Why youth (heart) social network sites: the role of networked publics in teenage social life. http://www.danah.org/papers/WhyYouthHeart.pdf. Accessed Dec 2010

Bruckman A (2002) Studying the amateur artist: a perspective on disguising data collected in human subjects research on the Internet. Ethics Info Technol 4:217–231

Cooper A, Scherer CR, Boies SC, Gordon BL (1999) Sexuality on the Internet: from sexual exploration to pathological expression. Prof Psychol Res Pract 30:154–164

DeAndrea DC, Walther JB (in press) Attributions for inconsistencies between online and offline self-presentations. Commun Res

Ellison N, Steinfield C, Lampe C (2007) The benefits of Facebook "friends": social capital and college students' use of online social network sites. J Comput Mediat Commun 12:1143–1168; Article 1. http://jcmc.indiana.edu/vol12/issue4/ellison.html

Frankel MS, Sang S (1999) Ethical and legal aspects of human subjects research on the Internet: a report of a workshop June 10–11, 1999. http://www.aaas.org/spp/dspp/sfrl/projects/intres/report.pdf. Accessed 15 May 2002

Hudson JM, Bruckman A (2004) "Go away": participant objections to being studied and the ethics of chatroom research. Info Soc 20:127–139

Jacobson D (1996) Contexts and cues in cyberspace: the pragmatics of naming in text-based virtual realities. J Anthropol Res 52:461–479

Jacobson D (1999) Doing research in cyberspace. Field Methods 11:127–145

McArthur RL (2001) Reasonable expectations of privacy. Ethics Info Technol 3:123–128

Parks MR, Roberts LD (1998) "Making MOOsic": the development of personal relationships on line and a comparison to their off-line counterparts. J Soc Pers Relat 15:517–537

Stone AR (1995) The war of desire and technology at the close of the mechanical age. MIT Press, Cambridge

Turkle S (1995) Life on the screen: identity in the age of the Internet. Simon & Schuster, New York

Walther JB (2002) Research ethics in Internet-enabled research: human subjects issues and methodological myopia. Ethics Info Technol 4:205–216; Rpt. http://www.nyu.edu/projects/nissenbaum/ethics_wal_full.html

Walther JB, boyd s (2002) Attraction to computer-mediated social support. In: Lin CA, Atkin D (eds) Communication technology and society: audience adoption and uses. Hampton Press, Cresskill NJ, pp 153–188

# Chapter 2
# Three Theories of Privacy: An Overview

**Stephen T. Margulis**

## 2.1 Introduction

This chapter reviews the current most important theories of privacy.[1] The review is addressed to those unfamiliar with theories of privacy. It is my goal to provide those readers with a foundation on which to build. To this end, the chapter summarizes the two best articulated and best supported theories of privacy (Altman 1975; Westin 1967) as well as Petronio's (2002) communication privacy management (CPM) theory, an important extension of Altman's theory that is particularly suited for the study of social networking. Additionally, this chapter considers two larger issues about what privacy is: issues in defining privacy and lessons to be learned from Altman's and Westin's theories. I begin with the three theories of privacy.

Irwin Altman's and Alan Westin's theories were selected because they have stood the test of time. Both figure prominently in major reviews of privacy in the 1970s (Margulis 1977), 1980s (Sundstrom 1986, Chap. 13), and 1990s (Newell 1995). Moreover, they have paved the way for others, particularly Petronio's CPM theory.

[1] This chapter draws heavily on two articles by the author in the *Journal of Social Issues* (Margulis 2003a, b). The author wishes to thank Wiley-Blackwell for allowing the use of this material. I wish to thank Sandra Petronio for her very helpful review of her theory and for providing published and unpublished material.

S.T. Margulis (✉)
Grand Valley State University, Grand Rapids, MI
e-mail: margulis@gvsu.edu

S. Trepte and L. Reinecke (eds.), *Privacy Online*,
DOI 10.1007/978-3-642-21521-6_2, © Springer-Verlag Berlin Heidelberg 2011

## 2.2 Westin's Theory

Westin's (1967) theory of privacy addresses how people protect themselves by temporarily limiting access of others to themselves. For Westin (1967, p. 7)

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [Moreover] … privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means. . ..

Westin (1967) proposes that people need privacy. Privacy, in concert with other needs, helps us to adjust emotionally to day-to-day interpersonal interactions. For Westin, privacy is both a dynamic process (i.e., over time, we regulate privacy so it is sufficient for serving momentary needs and role requirements) and a non-monotonic function (i.e., people can have too little, sufficient, or too much privacy). Westin specifically limits his theory to Western democracies because privacy is consistent with the sociopolitical values of these democracies. For Westin, privacy is neither self-sufficient nor an end in itself, but a means for achieving the overall end of self-realization.

Westin postulates four states of privacy. *Solitude* is being free from observation by others. *Intimacy* refers to small group seclusion for members to achieve a close, relaxed, frank relationship. *Anonymity* refers to freedom from identification and from surveillance in public places and for public acts. *Reserve* is based on a desire to limit disclosures to others; it requires others to recognize and respect that desire. The states are the means by which the functions (purposes or ends) of privacy are achieved. The states are, in effect, the "hows" of privacy.

Westin also posits four functions (purposes) of privacy. They are, in effect, the "whys" of privacy. *Personal autonomy* refers to the desire to avoid being manipulated, dominated, or exposed by others. *Emotional release* refers to release from the tensions of social life such as role demands, emotional states, minor deviances, and the management of losses and of bodily functions. Privacy, whether alone or with supportive others, provides the "time out" from social demands, hence opportunities for emotional release. *Self-evaluation* refers to integrating experience into meaningful patterns and exerting individuality on events. It includes processing information, supporting the planning process (e.g., the timing of disclosures), integrating experiences, and allowing moral and religious contemplation. The final function, *Limited and protected communication*, has two facets: limited communication sets interpersonal boundaries; protected communication provides for sharing personal information with trusted others (Westin 1967).

For Westin (1967), privacy operates at the individual, group, and organizational/institutional levels. This is an early statement of the multiple levels often associated with privacy (cf. Petronio 2002). Although Westin's definition of privacy is often cited, it is his privacy states and functions that have occasioned research. The research supports (to varying degrees) and extends the states and functions; it examines the relationships between the states and functions; it applies the states and functions to specific contexts (see Margulis 2003b, pp. 413–415, for a summary of this research).

Nevertheless, possibly because Westin is a political scientist and lawyer, and not a behavioral scientist, questions remain. Do Westin's four functions flow into one another? Do they co-occur or overlap in time or do they occur independently? Do specific dimensions of privacy underlie Westin's states? Are privacy factors organized hierarchically? Can the functions be understood as traits? Finally, Westin's endorsement of organizational-level privacy is problematic because he models the organization on an individual who acts alone rather than as a collective. (See Margulis 2003b, p. 418, for supporting information and citations.)

## 2.3 Altman's Theory

Altman, like Westin, has influenced how we understand privacy. Altman's analysis of privacy focuses on individual and group privacy and behavior (i.e., privacy-regulating mechanisms) operating as a coherent system. He takes a dynamic and a dialectical perspective on privacy regulation (i.e., it is a process that paces and regulates interaction with others; we change how open or closed we are in response to changes in our internal states and external conditions) (Altman 1990; Margulis 1977). Because Altman is a social and an environmental psychologist, social interaction is at the heart of his theory and Altman uses the environment to provide mechanisms for regulating privacy.

Privacy, for Altman, is "the selective control of access to the self" (1975, p. 24). Privacy has five properties. Firstly, privacy involves a dynamic process of interpersonal boundary control. Secondly, Altman differentiates desired and actual levels of privacy. Thirdly, privacy is a non-monotonic function, with an optimal level of privacy (desired = actual level) and possibilities of too much privacy (actual > desired level) (e.g., crowding) and too little (desired > actual level) (e.g., social isolation). Fourthly, privacy is bi-directional, involving inputs from others (e.g., noise) and outputs to others (e.g., oral communication). Fifthly, privacy operates at the individual and group level (Altman 1975; Margulis 1977).

For Altman, there are multiple behavioral mechanisms for regulating privacy (e.g., territorial behavior, cultural norms) that operate as a coherent system. Consequently, one mechanism can substitute for another (e.g., a nod of approval for the word "yes"), can amplify another (e.g., shout "no" and slam a door shut), or can modulate another (e.g., offer an apology for locking one's door). Moreover, Altman posits a hierarchy of privacy functions, the most central of which is creating self-identity.

In Altman's approach, three features of privacy are particularly important. Firstly, privacy is inherently a social process. Secondly, a proper understanding of psychological aspects of privacy must include the interplay of people, their social world, the physical environment, and the temporal nature of social phenomena (Altman 1990). Thirdly, privacy has a cultural context; specifically, privacy is a cultural universal but psychological manifestations are culturally-specific (Altman 1975, 1977).

Altman's theory has received impressive empirical support (see Margulis 2003b, p. 419, for a summary). It also has stimulated theory development by others (see Margulis 2003b, pp. 419, 421, 422). Lastly, Altman's theory of privacy is sufficiently comprehensive to be a general theory about the regulation of social interaction (Margulis 1977).

The central issue with Altman's theory is whether his boundary concept is a metaphor or a theoretical construct. In this regard, Petronio (2002), whose theory builds on Altman's ideas, regards it as a metaphor.

## 2.4 Petronio's CPM (Communication Privacy Management) Theory

The most valuable privacy theory for understanding interpersonal computer-mediated communication, such as blogging and social networking, was stimulated by Altman's dialectical conception of privacy as a tension between opening and closing a personal boundary to others (see Child et al. 2009). That theory is Petronio's (2002) CPM (communication privacy management) theory.

In CPM theory, privacy boundaries can range from complete openness to complete closedness or secrecy. An open boundary reflects willingness to grant access to private information through disclosure or giving permission to view that information, thus representing a process of revealing. On the other hand, a closed boundary represents information that is private and not necessarily accessible, thus characterizing a process of concealing and protecting. The relationship between the boundaries is dialectical, consistent with Altman's thesis, because we continuously adapt our level of privacy and disclosure to internal and external states because we simultaneously need to be open and social as well as private and preserve our autonomy. Moreover, we achieve desired levels of privacy and disclosure through the use of privacy rules. That is, when we make a decision to disclose private information, we use a rule-based privacy management system that regulates the degree of boundary permeability (how much is told) and that manages linkages (who we want to know the information) and the level of shared ownership with others. Using this rule-based management system allows CPM theory to consider *how* decisions are made about revealing and concealing private information (Petronio 2002).

Five propositions underpin CPM theory (Petronio and Durham 2008). The first proposition is that private information is defined in terms of ownership in that when people believe the information belongs to them, they count it as private. The second is that because they define private information as something they own, they therefore believe they have the right to control the distribution of that information (Petronio and Reierson 2009). The third is that people develop and use privacy rules, based on personally important criteria, to control the flow of private information. These rules impact the management of individual and collective (i.e., dyadic and group) privacy boundaries. Individual privacy rules are based on cultural values, gendered orientations, motivational needs, contextual impact, and risk-benefit ratio criteria. The fourth is that once private information becomes shared, a collective privacy boundary is formed and others receiving private information become co-owners of that information. From the perspective of the original owner, co-owners have fiduciary responsibilities to manage and therefore jointly control this private information in a way that is consistent with the original owner's rule. Privacy rule coordination between the original owner and co-owner is negotiated and revolves around decisions about permeability, co-ownership responsibilities, and linkage rules. *Linkage rules* determine who else can know (become a co-owner of) the information. *Permeability rules* determine how much others can know about the information. *Ownership rules* determine how much control co-owners have over co-owned information. (For an instrument to measure these three factors, see Child et al. 2009.) These rules might be implicit (e.g., based on a person's assumption that the other person has learned the requisite rules/norms) or explicit because of a need to clarify or modify an existing rule or to introduce/negotiate a new rule (Child et al 2009; Petronio 2002). These privacy rules are dynamic: they change, grow, or remain stable for periods (Petronio 2002).

Privacy rules also have several attributes (Petronio 2002). Firstly, privacy rules may become so routine that they form the basis for privacy orientations. Routinization can be aided by the use of sanctions to control the use of privacy rules. Nevertheless, these rules are often subject to change. Secondly, we must manage our individual and collective boundaries. Collective boundaries require interpersonal coordination (see Petronio 2002, p. 32f, for a discussion of collective coordination patterns). Thirdly, effective boundary management might fail. For example, there can be boundary turbulence because a co-owner feels no obligation to protect the discloser's private information. Whatever the reason, ineffective boundary management means that co-owners need to take corrective action to ensure effective boundary management (Petronio 2002).

The fifth proposition of Petronio's CPM theory, as noted, is that when privacy rules are not coordinated between the original owner and co-owner, there is a possibility of *boundary turbulence* because people do not consistently, effectively, or actively negotiate collective privacy rules. Boundary turbulence occurs when co-owners fail to effectively control (manage) the flow of private information to third parties.

In sum, CPM theory extends Altman's original proposal of privacy regulation, as Altman has noted, by articulating "[a] most complicated set of dynamics" and by articulating the operation of communication privacy management at the individual, dyadic, and group levels (Petronio 2002, p. xvi). And like Westin, Petronio also focuses on the management of private information.

For applications of CPM theory to interpersonal computer-mediated communication and blogging, see Child and Petronio (2011), Child et al. (2009), Child and Agyeman-Badu (2010).

## 2.5 What Privacy Is: Issues in Defining Privacy

Privacy is an elusive concept because it is an elastic concept (Allen 1988). The psychological concept subsumes a wide variety of philosophical, legal, behavioral, and everyday definitions. Moreover, the relationships between privacy and cognate concepts (e.g., deception, secrecy, anonymity) are debatable because of disagreements about the boundaries of privacy as a concept (see, e.g., Margulis 2003a, 2009). Also, in the moral domain, there is disagreement about whether privacy is best understood as protecting "behavior which is either morally neutral or valued by society" (Warren and Laslett 1977, p. 44), a common perspective, or whether privacy also can support illegitimate activities, such as misuse of a public office (Westin 1967), vandalism (Altman 1975), and morally dubious behavior like lying (Derlega and Chaikin 1977). Lastly, there is no agreement on the proper philosophical frame within which to define privacy. In this regard, the theories of Altman, Petronio, and Westin are consistent with the limited-access perspective (Allen 1988) but there are other perspectives. (See Tavani 2007, for four perspectives, including limited access.)

I examined the variability in definitions of privacy, primarily in psychological analyses of privacy but also in studies of how people defined privacy (cf. Newell 1998). Based on my examination, I inductively derived "an abstract skeleton" of the means and ends of privacy: "Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (Margulis 1977, p. 10). This "skeletal" definition, so to speak, failed to note that, in the privacy literature, control over transactions usually entailed limits on or regulation of access to self (Allen 1988), sometimes to groups (e.g., Altman 1975), and presumably to larger collectives such as organizations (e.g., Westin 1967). Because I inductively derived the definition from a wide range of examples, it follows that the variation in specific definitions reflects how the terms and the relationships among terms, in the abstract skeleton, were interpreted within those definitions. In individual cases, it also reflected the additional concepts and/or relationships that were included in a definition. For example, the concept of control, in the abstract skeleton, has been interpreted as social power (Kelvin 1973) and as personal control (Johnson 1974). Johnson's (1974) distinction between primary (direct) and secondary (indirect) personal control over the attainment of privacy-related outcomes illustrates the use of an additional concept.

Although I concluded that the psychological concept emphasizes privacy as control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access (Margulis 1977), there have been (e.g., Pennock and Chapman 1971) and continue to be legal and philosophical analyses of the meaning of privacy, some of which, as noted (e.g., Tavani 2007), would have us go beyond the limited-access perspective (Allen 1988) or raise questions about the boundaries of privacy (e.g., Davis 2009). In the final analysis, privacy remains an elastic concept. Therefore, if you intend to use a behavioral theory of privacy, you should determine whether its definition of privacy meets your requirements.

## 2.6 What Privacy Is: Lessons from Two Theories of Privacy

One way to examine the core of privacy is to compare the commonalities and differences in the two best supported theories of privacy: the theories of Altman (1975) and Westin (1967).

Both theories discuss how individuals and groups control or regulate access to themselves (i.e., both illustrate the limited-access approach). Both theories describe our need for privacy as a continuing dynamic of changing internal and external conditions, to which we respond by regulating privacy in order to achieve a desired level of privacy. In turn, achieved privacy can affect internal states and external conditions. Both agree that attempts to regulate privacy may be unsuccessful: we may achieve more or less privacy than we desired. Both agree that privacy can take many forms. Both agree that privacy has universal characteristics and that the nature of the forms that privacy can take is probably culturally-specific. Both agree that privacy can support illegitimate goals. Both differentiate the forms (or the hows) from the functions (or the whys) of privacy. Both agree that the functions of privacy include opportunities for self-evaluation and that privacy contributes to self-identity and individuality. The principal difference is that Altman's theory is relatively inclusive of privacy phenomena because it emphasizes social interaction but Westin's is less so, often focusing on information privacy, a subset of social interaction. (In this regard, CPM theory also focuses on information privacy.) That two independent, well-supported theories share so much in common suggests that they provide a reasonable foundation for understanding the fundamentals of privacy as a psychological concept.

Westin (2003) also has described three distinct empirically-derived (not theoretically-derived) positions on privacy that the public holds. The High-Privacy position assigns a high(er) value to privacy claims and seeks comprehensive governmental interventions to protect privacy. (See Bennett 1995, for an overview, and Lyon and Zuriek 1996, for examples of the High-Privacy position.) The Balanced-Privacy position values privacy claims but advocates tailored (e.g., sectoral) governmental interventions to address demonstrated abuses as well as voluntary organizational initiatives to promote individual privacy. (See Etzioni 1999, and Westin 1967, for different approaches to Balanced Privacy.) The Limited-Privacy position usually assigns a lower value to privacy claims than to business efficiency and societal-protection interests and it opposes governmental intervention as unnecessary and costly. (For an example, see Singleton 1998.) I would add a variant on the Limited-Privacy position, based on the claim that openness ought to trump privacy. This position has its roots in humanistic psychology (e.g., Jourard 1971). Interestingly, a contemporary advocate of this position is Mark Zuckerberg, the founder and CEO of Facebook, currently the largest social networking site (Vargas