Communication Privacy Management and Mediated Communication

Debra L. Worthington
Auburn University, USA

Margaret Fitch-Hauser
Auburn University, USA

INTRODUCTION

Sandra Petronio (1991) introduced communication privacy management theory (CPM) to explain how individuals control and reveal private information. While it was originally developed as an organizing principle for understanding disclosure in traditional social interactions, it has since been extended to a number of contexts, most recently to evolving communication technologies and social networking sites, including online blogging (e.g., Child & Agyeman-Budu, 2010; Child, Petronio, Agyeman-Budu, & Westermann, 2011), Facebook usage (e.g., De Wolf, Willaert & Pierson, 2014; Waters & Ackerman, 2011), and Twitter and Short Message Service (SMS) (e.g., Cho & Hung, 2011; Jin, 2013; Patil & Kobsa, 2004). CPM provides a set of theoretical tools to explore the intersection of technology and individual privacy in relationship management. Below privacy is defined, components of communication privacy management theory and their application to mediated communication are outlined, and areas of future research are presented.

BACKGROUND

Both a dynamic and dialectic process, the notion of privacy suggests that individuals regulate boundaries of disclosure, personal identity, and temporality (Palen & Dourish, 2003). More specifically, it refers to our ability to manage when, how, and the extent to which our personal information is revealed to others (Westin, 1967).

When discussing the intersection of technology and privacy, people often focus on technical issues associated with technology use (see, for example, Boyles, Smith, & Madden, 2012). In reality, individuals focus significant attention on managing privacy in their online digital lives. CPM provides a means to better understand and explain how individuals use and communicate in online and mediated communication contexts (Child & Petronio, 2011).

COMMUNICATION PRIVACY MANAGEMENT THEORY

Originally developed for interpersonal contexts (Petronio, 1991), research associated with CPM initially focused on social and interpersonal interactions in areas such as family and health communication. (e.g., Petronio, 2006; Petronio & Caughlin, 2005; Petronio, Jones, Morr, 2003).

Petronio (2007) describes CPM theory as “an evidenced-based, applied theory construct to be translatable into practices” (p. 219). The CPM system rests on three elements – privacy ownership, privacy control and privacy turbulence. Eight axioms predict privacy practices (Petronio, 2013). The first two axioms are associated with privacy and the ownership of personal information. Axiom 1 proposes that individuals believe in private ownership of their personal information

DOI: 10.4018/978-1-5225-2255-3.ch605

and in their ability and right to share or protect that information from others. Axiom 2 predicts that when access to private information is granted to others, those gaining access become co-owners of the information, taking on the trust and responsibility that comes with co-ownership.

Axioms 3 – 6 are associated with privacy control. Petronio (2013) described privacy control as the regulating engine for determining the conditions of providing or denying access to private information. Thus, not only do individuals believe they are sole owners of their personal information (i.e., Axiom 1), but they also believe they alone control their personal privacy, even when that information is shared with others (Axiom 3). At the same time, how information is shared is based on the privacy rules individuals develop (Axiom 4). Core and catalyst criteria influence decisions on how and when rules are invoked. Core criteria are the most stable and predictable guidelines for privacy choices, while catalyst criteria result in privacy rule changes based on motivation and risk assessments.

Axiom 5 addresses how, once access to private information is shared with others, the original owner continues to maintain control by continued coordination and negotiation of privacy rules associated with third-party access (Petronio, 2013). However, ownership rights can be challenged when individuals manage multiple, often inter-related, privacy boundaries (e.g., can information revealed by a friend be shared with another mutual friend) (Petronio, 2002). Confidants fall into two categories – deliberate confidants purposely ask for information (e.g., bank employee and customer), while reluctant confidants receive unwanted private information (e.g., a third party present during a mobile phone exchange). Reluctant confidants may experience unwanted feelings of obligation and responsibility (Petronio & Reierson, 2009). If the parties can reach a consensus about privacy rules, and accept the means by which they became deliberate confidants, then the confidant relationship can be effectively regulated.

The complications of collective co-ownership are seen in Axioms 6 and 7. Co-ownership leads to mutually agreed upon and practiced privacy boundaries where all members of the group can engage in sharing private information (Axiom 6, Petronio, 2013, p. 10). These group held privacy boundaries are regulated by decisions about who may divulge what information to whom and when. (Axiom 7, Petronio, 2013, p. 11). Thicker boundaries suggest that the coordinated rules of those collectively holding private information are relatively closed, while thinner boundaries are more permeable, resulting in information that is more accessible and open to third parties (Petronio & Reierson, 2009). The original owner of the information and the confidant negotiate the level of access third parties may have, including the scope and extent of private information that can be shared.

The purpose of these boundaries is to govern who has control of and access to information as well as how to protect that information (Petronio, Sargent, Andea, Reganis, & Cichocki, 2004). People manage or coordinate privacy boundaries based on negotiation of privacy rules related to linkages, boundary permeability, and information ownership (Petronio, 2002). Privacy rules are both normative and situational and affected by a number of factors, including cultural expectations, individual motivations, risk-benefit assessments, gender, and the needs of the situation (Petronio, 2009). Importantly, multiple rules may be used during the boundary management process.

The final axiom, Axiom 8, addresses the area of privacy turbulence, and acknowledges that privacy regulation does, at times, fail and rules are broken. Privacy boundary turbulence often results from confidentiality breaches (i.e., privacy expectations of the original owner of information are not met by co-owners) (Petronio & Reierson, 2009). Violations of confidentiality – discrepancy breaches of privacy, privacy ownership violations, and preemptive privacy control – can negatively affect the relationship of those involved.