Computers in Human Behavior 58 (2016) 214–220

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Living in a big data world: Predicting mobile commerce activity through privacy concerns

Matthew S. Eastin, Nancy H. Brinson*, Alexandra Doorey, Gary Wilcox

The University of Texas, Austin, TX, USA

ARTICLE INFO

Article history:
Received 29 August 2015
Received in revised form
11 December 2015
Accepted 18 December 2015
Available online xxx

Keywords:
Big data
Mobile commerce
Information privacy
Communication privacy management
Personalized advertising
Location tracking

ABSTRACT

As advertisers increasingly rely on mobile-based data, consumer perceptions regarding the collection and use of such data becomes of great interest to scholars and practitioners. Recent industry data suggests advertisers seeking to leverage personal data offered via mobile devices would be wise to acknowledge and address the privacy concerns held by mobile users. Utilizing the theoretical foundation of communication privacy management (CPM), the current study investigates commonly understood privacy concerns such as collection, control, awareness, unauthorized secondary use, improper access and a newly adapted dimension of location tracking, trust in mobile advertisers, and attitudes toward mobile commerce, to predict mobile commerce engagement. Data from this study indicate that control, unauthorized access, trust in mobile advertisers, and attitude toward mobile commerce significantly predicted 43% of the variance in mobile commerce activity.

Smartphone ownership in the United States recently climbed to 75%, up from 35% in 2011 (comScore, 2015). Mobile connectivity through cell phones has made constant, continuous access to information and others a reality for the vast majority of consumers. The pervasive nature of mobile devices continues to alter the way individuals gather and communicate information at increasingly high rates. Since 2009, Internet access via mobile platforms has overtaken fixed access, with 74% of American adults reporting they regularly connect to the Internet through mobile devices like smartphones and tablets (Smith, 2015). New technologies allowing this level of connectivity and accessibility offer dual outcomes for mobile users. While they have an unprecedented ability to instantly obtain information and interact with one another from virtually any location, this constant interconnectedness also leaves them more exposed and accessible to third parties, whether this is their intention or not.

The diffusion of mobile technology and, in turn, mobile marketing has indirectly resulted in mobile devices becoming an immense storage area for personal information. Modern marketers have the capability to aggregate multiple information sources to form personal profiles about consumers, which can be used to narrowly target individuals with various forms of marketing communications (Vesanen, 2007). While asserting their ability to create experiences that reflect individual preferences, marketers have largely failed to understand the delicate balance between personalized messages that recipients welcome, and those that daze, dismay, or disturb. As reported by McCann (2013), U.S. consumer attitudes related to data sharing and advertising personalization across multiple platforms have grown increasingly negative over the past few years.

For marketing scholars and practitioners, this recent attitudinal shift indicates a critical need to better understand consumer perceptions related to personalized advertising in multiple contexts, including mobile. Exploring the relationship between consumer privacy management and the level of personalization in mobile advertising messages offers to advance research and practice in a number of ways. First, extending theory typically associated with interpersonal communication (communication privacy management) to the mobile, mass communication platform encourages scholars to consider an interdisciplinary theoretical framework that more accurately reflects the dynamics associated with computer-mediated communication (CMC). Secondly, an increased understanding of consumers' perceptions regarding personalized communication will enable mobile marketing practitioners and content publishers to better understand consumer needs and improve their campaign outcomes.

* Corresponding author.
E-mail addresses: matt.eastin@utexas.edu (M.S. Eastin), nhbrinson@utexas.edu (N.H. Brinson).

http://dx.doi.org/10.1016/j.chb.2015.12.050
0747-5632/

Previous research on mobile marketing has primarily focused on factors contributing to consumer adoption and acceptance of m-commerce (e.g.,Acquisti, 2004; Mir, 2011; Wei, 2008), as well as best practices for companies utilizing mobile advertising as part of their marketing mix (e.g., Galizia, Gee, & Landis, 2011; Rocket Fuel, 2014). Fewer studies address consumers' privacy concerns related to the availability of increasing levels of personal information in mobile contexts (e.g., Kim & Han, 2014). Using a survey approach, this study examines consumer mobile phone usage, privacy concerns, attitudes, and behaviors regarding interactions with mobile marketing using the theoretical foundation of communication privacy management (CPM).

1. Big data

The collection of personal data, once the exclusive domain of governments and state agencies, is now an inescapable part of every day life for U.S. consumers (Lyon, 2001). Half a century after computers entered mainstream society, personal data has begun to accumulate to the point where it is increasingly difficult to grasp its magnitude, much less manage the potential implications it represents to business and society Defined by Mayer-Schoenberger and Cukier (2013) as data sets so large that "the quantity being examined no longer fit into the memory that computers use for processing" (p. 6), so-called "big data" now offers the ability to "harness information in novel ways to produce useful insights or goods and services of significant value" (p. 2). According to the 2014 Global Information Technology Report, over two and a half quintillion bytes of data are created each day, and 90% of the world's total stored data was created in the last two years alone (Dutta & Bilbao-Osorio, 2014). Further, it is projected that all digital data created, replicated or consumed—known as the "digital universe"—will expand by a factor of 30 from 2005 to 2020, doubling in size each year (Gantz & Reinsel, 2012). This accelerated growth is attributed in part to the proliferation of information-sensing technologies, surveillance cameras, microphones, radio-frequency identification readers, and wireless sensor networks (IBM, 2013).

Mobile technology and the targeted, specific, and constant access to consumers that it permits is a fundamental contributor to the big data universe. While total traffic over IP networks is forecasted to triple from 2012 to 2017, mobile traffic data is projected to grow thirteen-fold, representing a more significant share of all data created and transmitted (Cisco, 2014). This enormous volume of consumer data is considered of vital economic value to business, government and society. Given that individuals surrender a measure of information privacy in exchange for economic or social benefits, underlying the collection and aggregation of this data is an implicit understanding that the individual's interests should be balanced with those of society at large. Consequently, data gleaned from personal mobile devices will continue to be a central focus of government agencies, marketers, organizations, and regulators as they seek effective ways to appropriately manage the potential benefits offered by big data while protecting individual interests in the process.

2. Information privacy and trust

Consumers' mobile information privacy concerns are largely rooted in the rapidly expanding big data ecosystem (Cleff, 2007). Conceptualized as the rights of individuals whose information is communicated to others, information privacy and the protection of personal data have long been viewed as fundamental human rights. Currently, human recognition (or "personally-identifiable information") is portrayed as the legal threshold condition for the loss of anonymity or privacy (Schwartz & Solove, 2011). However, the nature of digital communication suggests a need to rethink this definition for the modern age. An individual's digital identity encompasses a wide range of traceable offline characteristics (e.g., age, residence, income, etc.) in addition to a variety of online profiles, passwords, pin numbers, access codes, and behaviors – all of which establish concrete links between social and technological understandings of identity (Wessels, 2012). Today's digital consumer is no longer entirely anonymous since virtually every form of communication and behavior generates data that can be collected, aggregated and analyzed (Buckingham, 2008; Wessels, 2012; Zwick & Dholakia, 2004). As such, information gathered benignly for one purpose can be readily retrieved for another, and the possible linkage between mass amounts of aggregated data about an individual conceivably makes almost every point of collected data personally identifiable. Indeed, in its 2010 report, the Federal Trade Commission (FTC) recognized and addressed the "diminishing distinction between personally identifiable information … and supposedly anonymous or de-identified information" (p. 93).

Previous research in this area (i.e., Malhotra, Kim, & Agarwal, 2004; Okazaki, Li, & Hirose, 2009; Smith, Milberg, & Burke, 1996) identifies six determinants that contribute to individuals' information privacy concerns in online settings – data collection, data control, unauthorized secondary use, improper access, location tracking and awareness related to these practices. Once their personal data is collected, consumers want to exercise control over its use and distribution, particularly when a large potential exists for opportunistic behavior and breach of the social contract in an online relational exchange (Malhotra et al., 2004). Thus, awareness of privacy practices related to data collection, control, access and usage has been shown to be an active component in privacy boundary construction among online consumers (Culnan & Armstrong, 1999), and a critical intermediary to building trust in online relationships (Smith et al., 1996).

Trust and perceived risk are two other principal components shown to contribute to consumer privacy concerns (Gefen, Karahanna, & Straub, 2003), particularly in e-commerce contexts. Rotter (1980) defined trust as a generalized expectance held by an individual that the word, promise, oral or written statement of another individual or group can be relied on (p. 1). Other conceptualizations of trust include a "willingness to make oneself vulnerable to another in the presence of risk" (Kim, Ferrin, Cooper, & Dirks, 2004, p. 104), and one's belief that the other party will behave in a dependable, ethical, and socially appropriate manner (Gefen et al., 2003). Recent literature conceptually groups trust into three dimensions: ability, benevolence and integrity. "Ability," as defined by Pavlou (2003), reflects consumers' perception that an advertiser has the resources and capabilities to perform the necessary job, while "benevolence" reflects the confidence consumers have that an advertiser is positively oriented toward their interests, and "integrity" expresses the belief that an advertiser abides by a moral or professional code (p. 103). Though they may be viewed separately, these elements are most often combined as a measure for trusting beliefs.

Research related to adoption, acceptance and attitudes toward personalized online and mobile advertising suggests trust in marketing and retail practices plays a key role in determining consumers' attitudes and behaviors toward commercial activities (e.g., Karjaluoto & Alatalo, 2007; Malhotra et al., 2004; Mir, 2011). Historically, trust works in tandem with perceived risk to predict behaviors, and together the trust-risk equation is considered the most influential variable in driving behavior (Golembiewski & McConkie, 1975).