2017

# A comment on privacy

David Stewart
*Loyola Marymount University*, david.stewart@lmu.edu



## Recommended Citation

Stewart, D.W. A comment on privacy. J. of the Acad. Mark. Sci. 45, 156–159 (2017). DOI: 10.1007/s11747-016-0504-7

J. of the Acad. Mark. Sci. (2017) 45:156–159
DOI 10.1007/s11747-016-0504-7

COMMENTARY

# A comment on privacy

**David W. Stewart**[1]

Published online: 20 October 2016


Martin and Murphy (2017) provide a very useful and timely review of the role of data privacy in marketing. They make very clear the complexity of privacy as a construct and identify numerous rich opportunities for future research. An important theme of their paper is that privacy, and by implication, the loss of privacy, is difficult to define. The definitional problem is reminiscent of Supreme Court Justice Potter Stewart's famous conclusion about the definition of pornography: "I know it when I see it." The problem is that while each individual may know it when they see it, there may not be consensus or general agreement among individuals. So it is with privacy. Individuals know it when they see it and have clear perceptions about when they experience a loss of privacy, but they may differ in what they believe constitutes privacy and what represents a loss of privacy. This is what makes regulation, whether by a marketer or a government entity, so difficult.

Martin and Murphy offer a very comprehensive and helpful review of various approaches to the study of privacy. They note that much of the research in marketing has focused on privacy concern as a psychological construct and various ways to measure the construct. Such research focuses on an individual difference, privacy concern, rather than privacy itself. In contrast, they observe that research in information technology has tended to focus on how information may be misused. There is certainly a relationship between privacy and the misuse of information, but information can be misused in ways unrelated to privacy. Martin and Murphy also note that still another stream of research on privacy has focused on the characteristics of information or the perceptions of these characteristics. Again, there are important relationships between information characteristics and privacy, but these characteristics do not define privacy. Finally, there has been work that has identified the types of harm that may arise from breaches of privacy (see Solove 2010), but this work also skirts past a definition of the construct itself.

Indeed, what constitutes privacy, or a loss of privacy, is often determined as much by situational factors as by characteristics of the individual or the information. What people say they want in the way of privacy and how they actually behave is often quite different, especially in social media. This seeming inconsistency has been called the privacy paradox (Barnes 2006). This apparent inconsistency largely disappears when situational factors are considered. People choose to share information on specific occasions, for specific purposes, and with specific persons. These situational factors either explicitly or, more often, implicitly bound expectations about how information will and will not be used. Thus, someone may share information in a particular social medium with the expectation that the information will be available to only a limited circle of family members or close friends for their personal use and for only as long as the individual chooses to make the information available.

Such situationally determined expectations play a role in consumers' responses to marketers use of information. For example, when consumers are asked if they like to be on marketers' mailing or e-mailing lists they will often say "yes" when they perceive being on such lists as personally relevant and beneficial. On the other hand, when consumers state that they object to being on such lists they tend to cite reasons related to the nuances of irrelevant communications like junk mail and spam. In the former case, many consumers willingly share information about themselves. In the latter

✉ David W. Stewart
david.stewart@lmu.edu

[1] Department of Marketing and Business Law, College of Business Administration, Loyola Marymount University, 1 LMU Drive, Los Angeles, CA 90045, USA

case, consumers wish to maintain their privacy by not sharing information.

From a regulatory perspective a significant problem is that neither the consumer nor the marketer may have complete information about the relevant situational factors that define expectations about privacy on the part of the consumer or the ability of marketers to treat data in a particular fashion. From a research perspective, a very fruitful avenue for future work would be the development of a taxonomy of situational factors that influence expectations about privacy and the willingness of individuals to share or withhold information. For example, one reason that consumer control has been found to be related to greater consumer willingness to share information is because the consumer can customize what and how they share information. This is the flip side of marketers' ability to personalize.

A strong starting point for the development of such a taxonomy is a working definition of privacy, and Martin and Murphy review numerous definitions. However, many of the constructs they identify are constructs related to privacy, such as privacy concern, big data, and privacy failure, rather than privacy itself, and Martin and Murphy do not offer a definitive definition. Alternative definitions might suggest the same or different situational factors. Therefore, alternative definitions can be complementary and may be a particularly helpful strategy for moving research forward. Nevertheless, the development of any taxonomy must begin with a definition of the phenomenon.

## Defining privacy

Martin and Murphy observe that one of the earliest definitions of privacy is attributable to Warren and Brandeis, who defined privacy as being left alone. There is elegance in the simplicity of this definition. Implied in this definition is the concept of self or personhood. Being left alone indicates that there is a boundary between a self, which is private, and the rest of the world. At minimum, it suggests that there is a private self in addition to a public face. Without an identified "private self" there is no meaningful construct of privacy. This does not mean that there are no other transgressions related to information, e.g., defamation, but these would not be invasions of privacy. Privacy implies that there is a concealed or concealable self that an individual may or may not reveal, in whole or in part, to some others.

Defining privacy as being left alone also establishes an initial state of equilibrium; personal information is available only to the self. This is important for several reasons: (1) privacy is defined in terms of an individual's perception, being left alone; (2) the decision to share information rests with the individual; and (3) an invasion of privacy is a proactive act ("invasion" is the operative word) by another party. Of course, at the time Warren and Brandeis offered their definition, in the 1890s, it was much easier to be left alone than it is today. An individual, family, or small group could literally retreat from society. A move of 90 miles or so might have been sufficient to create a new context is which little or nothing was known about an individual or that individual's past by those with whom he or she interacted. An individual in his or her home was in a protected and private place. An invasion of privacy was literally an invasion of which the individual would often, if not always, be aware.

Technological innovations in transportation, including the automobile and airplane, in communication, including telephones and the Internet, and in information technology, including data storage and data mining, to name only a few, have made it difficult, if not impossible, for individuals to protect their privacy by withdrawal or to erase the past by making a short move. Paradoxically, the use of some of the means once used to protect privacy now require that individuals give up privacy. Moving to a remote location, if one can be found, requires travel, which may require a driver's license, a car registration, an airplane ticket, a security check, or some other requirement to provide identifying information.

Technological innovation, which is generally good for society, has increasingly placed the burden of protecting privacy on individuals, even as there are more demands for greater sharing of information as a condition of being a consumer and member of society. As the number of ways in which potential invasion of privacy can occur has grown, there has been a shift of emphasis from prohibiting and preventing invasion, where the majority of costs are imposed on the invader, to proactive protection, where the greater burden is placed on the invaded. This represents a critical dimension for the definition of privacy and any taxonomy of the factors that contribute to it and its loss.

It also suggests that the economic dimensions of privacy are complex. The burden of proactive protection includes more than financial costs. There are also cognitive, temporal, and emotional costs. Individuals are inundated with complex and idiosyncratic privacy policies that an individual may or may not agree with and may or may not accept, even if they agree. Time and effort spent processing such policies, if attention is even paid to them, is a cost. Notices of breaches of privacy are increasingly common and indiscriminate with respect to the seriousness of the breach. A result of placing the burden of defending personal privacy on the individual is desensitization; individuals become less concerned about the loss of privacy and less able to discriminate between serious breaches of privacy and minor, unintentional transgressions. Such desensitization erodes both the concept of privacy and the sense of self. It also creates greater opportunity for unscrupulous operators who can exploit the inattention and desensitization. Martin and Murphy raise a related point in their discussion of the economics of privacy where they discuss work

on the erosion of markets for privacy. However, the work they discuss makes various assumptions about how such markets might be structured. A taxonomy of situational determinants of privacy has the potential to reveal structural alternatives for privacy markets that could be explored in greater detail.

## The role of government

Among the important structural determinants of any market for privacy are government and government regulation. Martin and Murphy cast the role of government as that of benevolent and benign protector of consumer privacy. It is certainly the case that government does seek to provide some protection of consumer privacy, but it also the case that government has sought to coerce marketers into revealing private information. Government often makes information public in the interests of public interest when it is not always clear that there is any legitimate public interest. In addition, there is a long tradition of privacy defined as protection from government (Levin and Nicholson 2005).

Government is neither benevolent nor benign. Some of the largest breaches of privacy have been by government. Government has created many identifiers and identifying processes that serve as links between the private self and the external world. Having created a plethora of identifiers and identification process, the government and others admonish individuals to keep such information private or at least manage it with care. No treatment of privacy will be complete without explicit recognition of the role of government. Evaluation of alternative privacy policies among marketers needs to be placed in the context of both what government regulation permits and prohibits and the government's own privacy policies and management of information.

It is naïve assume the government is and should be the protector of privacy. Martin and Murphy briefly review research that demonstrates that third party gatekeepers often work to the detriment of consumers. It is certainly the case that the generally slow response of government to technological innovation means that regulation, especially regulation related to information technology, is dated and incomplete. Similarly, the fragmented nature of government often creates inconsistent policies and unintended consequences. For example, there is evidence that the Health Insurance Portability and Accountability Act (HIPAA) has had a detrimental impact on medical research even when there is no need for personally identifying information as a part of the research (Gomes 2009). Finally, government control of access to private information creates opportunities for the same abuses that are found in other organizations but on a much wider scale, involving the potential for far greater economic and social consequences.

The government's own problems with privacy and the well-publicized stories about breaches of government data, illegal surveillance, and misuse of personal data have produced greater awareness of the value of privacy to at least some consumers and created incentives for marketers to offer greater privacy and information security to consumers. Thus, new market solutions may develop. The development of such solutions might also be facilitated by a taxonomy of situational determinants of privacy.

## Toward a contextual framework of privacy

One conclusion that can be drawn from the Martin and Murphy paper is that there has been rather little research that focuses on privacy as a construct. Rather, the considerable research on privacy that has been published has focused on the relationship of privacy to other things: how important it is (whatever "it" is), how it might be lost, and the consequences of losing privacy. All are important topics, but they leave the construct poorly defined. Much of the research to date has focused on the loss of privacy. Much of the regulatory work among both marketers and government organizations has focused on how to prevent unwanted loss of privacy. Missing from much of this research is an effort to address the question of why privacy is important. Is privacy itself important, or is it only the consequence of losing privacy with associated negative consequences that matter?

If privacy is defined as "being left alone" it would be useful to explore the positive benefits of this state. Are these benefits associated with manifestation and/or maintenance of a sense of self, e.g., being alone with one's thoughts, collecting oneself, meditation? Are there situations in which such benefits are especially important? The European approach to privacy, with its focus on protection of individual dignity and public image, seems to embrace such positive benefits of privacy (Levin and Nicholson 2005).

It is important to separate such positive benefits and the loss of these benefits from harm that may arise from the loss of privacy that results from misuse of information and the negative consequences of such misuse. The economic consequences of identity theft are quite different from a loss of the sense of self, though both consequences may be costly.

After clearly differentiating the positive consequences of privacy from the potential negative consequences of the loss of privacy it is possible to ask about the circumstances in which an individual would give up some amount of privacy. Such a trade-off will likely be situationally determined. Development of such a taxonomy would be a significant contribution to theory, management practice, and public policy. Such a taxonomy is beyond the scope of this comment, but some of the general dimensions are clear: (1) What is the benefit of giving up information? (2) To whom will the

information be revealed? (3) At what level of detail? (4) For what purpose? (5) For what period of time? (6) How sensitive or personal is the information? (7) Is secondary use of the information expected or permitted? (8) What secondary uses of the information are possible? (9) What are the potential consequences of potential secondary uses? This is not an exhaustive list but suggests the general dimensions of a taxonomy.

Such a situational or contextual taxonomy suggests the need for a contingency theory of privacy. A contingency theory of privacy carries with it several implications. First, since only the individual providing information knows what uses of shared information are acceptable to him or her, the default for the decision to share should involve and opt-in. Second, the decision to opt-in needs to be informed by the relevant contextual factors that influence the decision to share information. The relevant information in disclosures about privacy and the use of shared information should include the relevant contingencies. Third, because contingencies can change over time individuals who opt to share information should have the ability to reverse this decision, as well as the ability to erase previously shared information to the extent possible. This perspective is far more consistent with the European view of privacy than the view in the United States (Directorate General for Internal Policies 2015). To the degree that this is the case, the European view has greater conceptual consistency, though logical consistency has never been a prerequisite for public policy.

Martin and Murphy have provided a rich source of ideas for future research by summarizing much of the extant research on privacy. Their summary offers a helpful organization of a very fuzzy literature. This commentary complements the summary by offering some thoughts about the definition of privacy as a unique construct, by differentiating research on privacy from research on factors related to privacy and its loss. Finally, this commentary suggests that the most relevant research questions are related to when and under what circumstances individuals willingly give up some privacy for some benefit. Such trade-offs are situationally determined. A taxonomy of situational dimensions that influence these trade-offs and a contingency theory of privacy would be a useful direction for future research.

## References

Barnes, S. B. (2006). A Privacy Paradox: Social Networking in the United States. *First Monday*, *11* (9), http://firstmonday.org/issues/issue11_9/barnes/index.html., accessed August 21, 2016.

Directorate General for Internal Policies. (2015). *A comparison between US and EU data protection legislation for law enforcement*. Brussels: European Parliament.

Gomes, L. (2009). The hidden cost of privacy. *Forbes*, May 21, http://www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html, accessed August 25, 2016.

Levin, A., & Nicholson, M. J. (2005). Privacy law in the United States, the EU and Canada: The allure of the middle ground. *University of Ottawa Law and Technology Journal, 2*(2), 357–395.

Martin, K., & Murphy, P. (2017). The role of data privacy in marketing, *Journal of the Academy of Marketing Science, 45*(2), doi:10.1007/s11747-016-0495-4.

Solove, D. J. (2010). *Understanding privacy*. Cambridge: Harvard University Press.