Privacy Momentum: A New Contextually Dynamic Conceptualization of Privacy

Research-in-Progress

Caleb Bradberry
The University of North Carolina at Greensboro
czbradbe@uncg.edu

Hamid Nemati
The University of North Carolina at Greensboro
nemati@uncg.edu

Abstract
Typically, we think of privacy as something dichotomous: either you have private information, or you don't. This research explores the conceptualization of privacy as a continuum at point t and t+1, in which a piece of private information can become stale and thus change over time.

Introduction
The field of privacy research is a very diverse domain. The analysis can focus on anything from the individual to an inter-organizational context, and even beyond to the environment in which privacy itself is assessed (Smith et al. 1996, 2011). Beyond the analysis, there has also been many conceptualizations of privacy, including a view that privacy is a commodity and it is something that can be traded (Li et al. 2010). While much work has been done in this field, all of the work seems to analyze how privacy can be taken away, or how an organization can protect private information; there exists a gap in which one can view privacy as something dynamic, which changes as other factors change.

The question to look at then becomes, how is privacy dynamic? It would stand to reason that if attitude is a part of privacy concerns for an individual, and attitudes change over time, wouldn't their identified privacy responses change over time? More specifically, as attitudes, awareness, and the environmental factors change throughout an individual's life, this would also cause private information as identified in the Information Privacy Protection Responses (Son and Kim 2008), to become stale.

In order to better understand how to conceptualize privacy as a dynamic concept, it’s important to look at the individual changes in the available antecedents to privacy. Specifically, this research will identify the antecedents that can be tested, and offer proposals for testing the changes in these antecedents through a design based approach.

The structure of this research beings by offering the theoretical foundations of what factors influence privacy from the literature, and synthesize those factors into a dynamic understanding of privacy. From this synthesis, a research model will be proposed, including propositions on how the antecedents impact this conceptualization of dynamic privacy. After the proposition, a way in which to operationalize these propositions based on the research mode will be discussed. Lastly a discussion around limitations and falsifiability will be offered, and the paper will end with conclusions.

The implications of this research model will simply be to show that privacy is more than a static concept; privacy is something that changes based on its antecedents, and can be gained or lost, based on a user’s behavioral or situational privacy. Diligent work has been conducted in the privacy domain, and the goal is extend that work in such a manner as show this work in a new lens, the lens of a dynamic aspect of privacy.

Theoretical Foundations
The concept of privacy has a very dynamic and varied definition, depending upon how it is examined. This paper will show that privacy is something that changes, and to examine privacy as something an individual possesses, which is gained or lost. The most commonly accepted definition for information privacy in which this paper will examine, is defined as the individual's control of when, how, and to what extent his or her personal information is communicated to others (Review and Westin 1968; Son and Kim...
2008) From this definition, it is already evident that the control of when a person shares personal information with others is an important aspect of defining privacy. However, privacy also needs to be assessed based on individual’s behaviors, as well as situations. The following foundations will help to build a dynamic view of privacy.

![Figure 1. Proposed Theoretical Model](image-url)
Behavioral Based Privacy

This section examines privacy based on an individual’s behavioral aspects. These behaviors can be found in the literature, and include attitude, awareness, and environmental factors. These are all factors that can be defined within the scope of a user’s actions. That is to say, behavioral based privacy would be conceptualized as privacy that is gained or lost based on a user’s actions, and the following sections are identified foundations that influence a user’s behaviors and actions.

Attitude

Acquisti & Grossklags have identified several observable factors through the use of survey, user study, and analysis on an individual unit of analysis; these factors include: limited information about costs and benefits, bounded rationality, psychological distortions, ideology and personal attitudes, and market behavior (Acquisti and Grossklags n.d.). For the purposes of this research, these factors are going to be broken down as they pertain to an individual’s attitude of privacy, or an individual’s awareness of privacy. Acquisiti & Grossklags go on to explain that attitudes are formed based on ideologies and personal experiences.

Attitude is of interest because of how it is dynamic. An individual’s attitude can change, and can be measured to change. Because attitude is something that is essential to privacy (Smith et al. 2011), it is important to include in the theoretical foundations as a concept that can have measurable change.

Awareness

Another observable concept is that of awareness, in the context of privacy concerns is defined as the degree to which a person is concerned about his/her awareness of information privacy practices by websites (D’Arcy et al. 2008). The reason that awareness is important is that it functions as a concept which can be measured via an instrument in order to capture a change in how aware a user is of his or her private information. As a user becomes more aware of his or her privacy and how it is captured, they can then begin to commoditize it through the passage of time, with the understanding that companies want current and relevant information, and that their privacy is more than just dichotomous over time. Another way to view this is through the factors of rational decision making, which include: information about costs and benefits, bounded rationality, psychological distortions, ideology and personal attitudes, and market behavior (Acquisti and Grossklags n.d.).

Awareness has also been shown in privacy search be an input to an individual’s perception of privacy, as well as how awareness is manifested (Smith et al. 1996, 2011). This research proposes that this awareness factor does change depending on a user’s behavior.

Definition – Behavioral Based Privacy
The definition that can be drawn from these constructs is that privacy is dependent upon a user’s actions. A recent finding suggests that attitude influences actions in such a manner that he or she may act against what they perceive to be correct in terms of privacy controls, that by giving out this information, they are acting against their own privacy awareness, such as the case of sharing on social media (Norberg et al. 2007; Stutzman et al. 2012). From here, we can define behavioral based privacy as an action a user takes that affects his or her information privacy based on internal motivations that change over time, as predicted by attitude, awareness, and environment.

**Situation Based Privacy**

*Environment*

The environment in which the individual is in can also be variable. Laufe and Wolfe (1977) introduce the environment in which privacy is examined as consisting of three aspects of this variability: cultural, sociophysical, and life cycle. For the purposes of conceptualizing behavioral based privacy and situational based privacy, life cycle has been incorporated into situational based privacy.

The cultural element being examined assesses the mores of a community, as it is made up of language, tradition, and values within the context of consciousness around privacy (Laufer and Wolfe 1977). Other research examines cultural and social norms within the context of privacy as a contributory factor (Westin 2003), but for the purposes of a longitudinal temporal aspect, there is too much debate around if culture can change with environment. However, the next element, sociophysical, has a general consensus.

The sociophysical element is the ‘fit’ in which an individual identifies his or her self within a group of people, or in a place (Laufer & Wolfe, 1977). Laufer and Wolfe argue that this sociophysical environment can add a context of privacy, such as the socially accepted norm of being in the restroom (Laufer and Wolfe 1977). They go on to state ‘there are experiences in and with places that contribute to the development of self over time. Places have specific meanings for self: They may enhance, threaten, or simply define, and in this respect we internalize a lot of privacy settings.’ From this, it is gathered that the notion of self is changing over time, and can be evidenced through physical location.

The key take away from identifying these groups is simply that an antecedent to information privacy momentum is that there are environmental factors that contribute to a person’s privacy at any point in time. These factors are observable in a physical sense, regarding an individual’s location, and how they perceive their privacy expectations in that location; this is analogous to how an individual should expect their information privacy to be treated, depending with whom they have shared their private information. The core idea is that the environment in which they share their information will change over time.

*Life Cycle*

Laufer & Wolfe go on to incorporate a life cycle element into privacy factors. Life cycle in this context refers to an individual’s life cycle from birth to death. The example offered as to how the properties of a lifecycle are dynamic in Laufer and Wolfe’s 1977 paper includes those of periods in an individual’s life in which they go through childbearing, child raising, employment, etc, will vary depending on technology, sociocultural patterns, and historical events. They go on to identify the characteristics in the life cycle in which privacy is related, such as where an individual is in their development of life, the roles this individual can take at any point in their life, and how the sum of these individuals also modify privacy attitudes (Laufer and Wolfe 1977).

*Technological Innovation*

Another factor external to the user in terms of their privacy is technological innovation. Technological innovation has been growing at such a rapid rate, while holding Moore’s law true, that an individual may find themselves in a situation where they are unable to comprehend what the technology is doing to their privacy. This is separate from awareness, in that these factors are external to the user. For example, technology such as a backscatter machine that takes an x-ray of an individual’s skin, effectively rendering them nude in images, could very realistically not have its data encrypted and then stolen, and this individual, through no fault of their own, has had their privacy change in a very real way.

Another example of technological innovation as a situational factor in terms of a user’s privacy would be having their laptop stolen. If this laptop has a cellular enabled connection, the technological innovation behind a cellular enabled laptop would allow the user several options in terms of their information
privacy: 1. Track the laptop through the cellular connection, 2. Start an encryption routine to stop the thief from stealing their information, 3. Send a ‘kill code’ to disable the laptop so the thief couldn’t access the data. This is, again, separate from awareness, in that it is enabled by the technology, whether the user is aware of it or not.

**Definition – Situation Based Privacy**

Situation based privacy, as opposed to behavioral based privacy, can be represented by a user’s external factors that make up their situational information privacy. That is, the factors external to him or her, in any given situation. The definition offered here is that situational based privacy is the degree to which a user’s external factors as defined by their life cycle (age) and technological innovations enable their privacy in a situational context.

**Definition – Privacy Momentum**

When the definition of privacy is deconstructed into behavioral privacy and situational based privacy, it becomes evident that there is a time factor at play. Because the users actions and situations can, and will, change over time, this also means that their privacy will change over time. For example, a user who recently had their laptop stolen at time \( t = 5 \) would most likely have different perspectives concerning their data on that laptop at time \( t = 4 \) than at time \( t = 6 \). This means that user’s privacy has changed, based on a temporal factor. Because of this change in privacy, this would then influence one or more of the factors attitude, awareness, or environment. Similarly, an individual who finds themselves in a situation where their laptop is stolen will then go back and have a change in their privacy based on the technological innovation available to them, and where they are in their life cycle.

These examples lead to a definition of privacy moment. Privacy momentum, as defined herein, is a measurable change in either a user’s behavioral privacy or situational based privacy.

**Proposed Research Model – Behavioral Privacy and Situational Privacy**

Based on these theoretical foundations, and the revealed definitions of behavioral based privacy and situation based privacy, three things are made evident: 1. Information privacy actions are internalized, 2. Information privacy situations are externalized, 3. Both actions and situations influence the change in a user’s privacy. A set of propositions is thus put forward for the initial measure of Privacy Momentum.

Proposition 1: Attitude and awareness have a positive influence on behavioral based privacy.

Proposition 2: Environmental, life cycle factors, and changes in technological innovations influence situational based privacy.

Proposition 3: The changes over time on behavioral based privacy contribute to privacy momentum.

Proposition 4: The changes over time with consideration to technological innovations influence privacy momentum.

Proposition 5: Privacy momentum at time \( t \) affects attitude and awareness factors at time \( t+1 \).

From these propositions, we get a value of privacy momentum at time \( t = 0 \), or a baseline. This then allows us to hypothesize on privacy momentum, as we can observe changes in each of these relationships. The hypothesized relationships are that as privacy momentum has a higher value, there is a larger change in privacy, and as privacy momentum has a smaller value, there is a smaller change in privacy. Similarly, if the change is positive, then momentum is being gained: the user is gaining back privacy. Conversely, if the change is positive, then momentum is being lost: the user is losing privacy. This relationship can be hypothesized as follows:

Hypothesis 1: A positive change in privacy momentum will result in a user gaining privacy.

Hypothesis 2: A negative change in privacy momentum will result in a user losing privacy.

**Discussion**

**Contextualization of Privacy Momentum**

In order to better understand how an individual can view their privacy momentum, it is first important to contextualize privacy. In Greenberg’s paper, *Context as a Dynamic Construct*, he argues that context is a
dynamic construct which is viewed over a period of time, episodes of use, social interaction, internal goals, and local influences (Greenberg 2001). This paper finds several implications that must be considered when trying to operationalize a concept that is dynamic, such as the proposed privacy momentum. These implications include: 1. Determining an appropriate set of canonical contextual states may be difficult or impossible, 2. Determining what information is necessary to infer a contextual state may be difficult, and 3. Determining an appropriate action from a given context may be difficult (Greenberg, 2001). Each of these concerns can be addressed elegantly if privacy momentum is operationalized as an application on a smartphone device.

**Operationalization**

In order to operationalize the proposed research model, and assess privacy momentum, it is important to capture a baseline frame of reference from an individual. This baseline will be viewed as $t_0$, and from there, the research can check against it. In order for this to be a viable research approach, a longitudinal study is proposed. This longitudinal study can elegantly be captured using the sensors, input, and capabilities of a smart-phone type device.

In order to overcome the first concern that Greenberg has discussed, this research actually can offer an appropriate set of canonical contextual states, given that the variable of interest is information privacy, and the chosen means of measuring this privacy is a smart device. It is not without limitation though, that this is to only be measured as information privacy in terms of personal information that the device can capture.

The second concern, as mentioned by Greenberg, is determining what information is necessary to infer a contextual state may be difficult. However, given the capabilities of a smart device, and the big data analytics tools available as of writing this research, this is a trivial concern, because almost all of the information can be captured, and then the analytics can be applied to assess what data is necessary. It would seem logical then, that a pilot study first be conducted to assess how much personal information data can be captured via these devices, and then target that specific data from the user's end.

The third concern, determining an appropriate action from a given context may be difficult, can also be controlled with thoughtful mobile application design. With thoughtful design, the application can capture the essence of this concern: is the user's change in privacy based on internal or external factors?

With these concerns out of the way, it is revealed that a mobile application on a smart device would be an ideal solution to longitudinally assess changes in privacy. This mobile application would capture a baseline frame of reference, $t = 0$, when it is installed, based on the permissions granted to it. From there, it could passively capture information data of the user at any point $t = n$, given the user's consent at the initial application installation. The data that the device could capture could be a range of sensitive information, from location data to personal contacts, to the information within the text messages that the user is sending. All of this information would then be anonymized into a report at each point $t = n$, and big data analytics could then be applied to not only measure a change in privacy over time, but also what factors are most statistically significantly changing over time.

**Limitations**

The proposed model is a variance model. As such, it is built around looking at certain concepts that have been identified in the literature as having a temporal aspect, and suggesting that these concepts have a variation over time. While privacy momentum is the dependent variable, the independent variables are still subject to externalities beyond variance in time.

The proposed operationalization is a longitudinal study, and requires the development of a new artifact. This artifact, while its intention is meant to benefit our understanding of privacy, would only be employed if the user was entirely aware of the information that it would capture, to pose no less than minimal harm to the users involved.

**Conclusions and Recommendations**

This research has examined privacy as something an individual can possess, gain, or lose, depending on any point in time. It has examined how temporal aspects can influence the antecedents towards privacy concerns, and offers a theoretical model in order to test the change in privacy over time using a latent
growth model. While privacy is a vast domain, this research has sought to offer a new lens from which standing research could benefit.

References


