A Privacy Control Theory for Online Environments

Maria Moloney
Trinity College Dublin
Maria.Moloney@cs.tcd.ie

Frank Bannister
Trinity College Dublin
fbnnistr@tcd.ie

Abstract

Extant literature in Information Systems often reports a significant level of unease among the Internet community with regard to threats to online privacy but fails to identify a comprehensive set of specific online privacy concerns. Moreover, out of the concerns that have been identified by a number of surveys, it is unclear whether any have adequate theoretical foundations. This paper uses the existing privacy literature and in particular the work of two prominent privacy theorists, Westin and Altman, to devise an online privacy model which outlines the components of the online privacy concept and their interdependencies. A theory for online privacy is then derived from this model.

1. Introduction

In the last twelve months, there have been a number of high profile breaches of privacy reported in the media. One such breach occurred in late August 2008 when the British government began an investigation into how a computer containing highly sensitive bank information of over a million people was sold via online auction site eBay [1].

In 2005 the American nonprofit consumer education and advocacy project, Privacy Rights Clearinghouse, started keeping a record of all breaches of sensitive data. To date, over 236 million records containing personal information have been involved in security breaches [2]. Given the frequency and magnitude of these breaches, it is little wonder that concern is growing among the public for the safety of their personal information in an age where, if not correctly managed, technology allows for an individual's personal information to reach the public domain quite easily.

In this paper, it is argued that an interdisciplinary approach is required to resolve the ethical questions surrounding the protection of an individual's private space. Consequently, the paper draws on the disciplines of law, social studies and information systems to examine specifically the concept of privacy in online environments. The paper is organised as follows. The next section examines some theories and definitions of privacy from within these disciplines. Section three presents a model of online privacy and section four outlines a theory of online privacy and a possible application. This is followed by a short discussion of future work and some final remarks and conclusions.

2. Review of Relevant Literature

According to Westin [3], whenever a privacy claim is recognised in law or social convention, people speak of "privacy rights". Privacy has been declared a fundamental right of every human in many enduring bodies of law, the principle ones being Article 12 of the Universal Declaration of Human Rights [4], article 8 of the European Convention on Human Rights [5], and articles 7 and 8 of The Charter of Fundamental Rights of the European Union [6].

This paper uses privacy definitions from two domains that have contributed greatly towards the formulation of the privacy concept to which our modern society adheres. These domains are the ethical and legal domains.

A challenge, and an opportunity, in this research is that there is no universally agreed definition of what constitutes privacy. This may be because attitudes to privacy are in part culturally determined [7]. However, it is also a complex concept. To give a flavour of the complexity of the problem, consider the following approaches to the subject. The theorist Charles Fried [8] believes that privacy is not simply an absence of information about a person in the minds of others, rather it is the control that a person has over information about themselves. This view is somewhat incomplete in that privacy can be interpreted as the control that a person has over information about themselves *that they wish to keep from others*. In reaction to Fried's 'control theory' of privacy Moor [9] proposes a 'restricted access' view of privacy. Rather than regarding privacy as an all or nothing

978-0-7695-3450-3/09 $25.00 © 2009 IEEE

proposition, Moor regards it as a complex of situations in which information is authorized to flow to specific people, at specific times. He argues that in a highly computerized culture, it is simply not possible to control all personal information that resides on computer systems around the world. Therefore, the best way to protect privacy is to make sure that the right people have access to relevant information at the right time. Moor calls this view of privacy, the restricted access view, which has the added advantage of Fried's control centred theory in that it gives individuals as much control over personal data as realistically possible. For this reason he labels his theory the "control/restricted access" theory of privacy [9].

An advocate of Moor's control/restricted access theory is Herman Taviani. Taviani [10] also points out that modern privacy theorists tend to analyse the notion of privacy in terms of controlling the flow of personal information and have coined the phrase "informational privacy" to express this new concept. The term, informational privacy, is often used when referring to an individual's online privacy (although it should be noted that, even though protecting an individual's personal information once submitted online is a key area for concern, submitting personal information is not an individual's sole reason for spending time online. Both social and non-social activities make up for a large portion of an individual's time spent online [11]).

The variety of views can be further illustrated by looking at the work of arguably the two key figures in the privacy domain of the last thirty years, namely Alan Westin and Irwin Altman. Both put forth their own theories of privacy in the 1970's and have since enjoyed considerable recognition from their peers [10, 12-20]. Westin [21] defines privacy as:

"*the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*"

He delineates four states of privacy:

- Solitude is the state of being free from the observation of others;
- Intimacy relates to the seclusion experienced by individuals when they are a member of a small group. This type of seclusion promotes the development of close relationships;
- Anonymity is concerned with freedom from identification and from surveillance in public places;
- Reserve is based on limiting disclosure to others and requires others to recognise and respect that desire.

He also outlines four functions or reasons for privacy:

- Personal autonomy is the desire to avoid being manipulated, dominated, or exposed by others;
- Emotional release is the release of tensions under social restrictions like role demands, emotional states or minor deviances;
- Self-evaluation deals with extracting meaning from personal experiences and exerting individuality on events;
- Limited communication sets interpersonal boundaries and protected communication allows for sharing personal information with trusted others [3].

In contrast, Altman [22] defined privacy simply as:

"*the selective control of access to the self*".

He sees 'selective control' as intrinsic to privacy because people try to control their openness or distance to others by being open and available or closed and unavailable at different times and for different reasons [22]. Altman argues that, privacy is a dynamic process whereby people vary in the degree to which they make themselves accessible to others. He describes the crucial idea of his framework as being that privacy is a central concept that provides a bridge between personal space, territory and other realms of social behaviour. He describes privacy as "*a dialectic and dynamic interpersonal boundary regulation process by which a person or group regulates interaction with others*" [22].

According to Altman, the word "dialectic" in this definition refers to the openness or distance of self to others. For example, whether the individual seeks or avoids social interaction. The meaning of "dynamic" indicates that the desired privacy level, which varies due to individual and cultural differences, continuously moves along a continuum of openness and distance in response to changes in circumstance over time.

This research uses a combination of Westin and Altman's privacy theories as the basis for developing an *online* privacy theory.

The next section outlines how the online privacy theory was formulated by firstly developing an online privacy model which explains the various concepts involved in online privacy and their interdependencies. This allowed for the whole schema of online privacy to be represented more clearly and thus more easily interpreted for a theory.

3. Formulation of the Theory

The first step in arriving at the online privacy theory was to represent the findings in the form of a model, where both the theoretical foundations of

privacy could be explored by examining in depth Westin and Altman's theories of privacy and the modern concept of online privacy could be analysed through examination of several recent academic studies.

The first step in devising the model was to derive individual sets of potential privacy concerns from both privacy theories. This was done through close examination of both theories and inferring privacy concerns from them.

The second step was to explore the concept of privacy in a modern setting and to examine whether the theoretical foundations from the privacy theories, developed over thirty years ago, still apply today. The modern setting was the "online environment" and the concerns individuals had about their privacy were in this case examined by looking at evidence from the empirical literature [7, 23-33]. These first two steps are described in more detail in [34].

From the information gathered through examination of both privacy theories and the empirical literature, a remarkable difference between theory and practice regarding privacy concerns emerges. While the concept of trust in relation to privacy features heavily among the online privacy concerns, Westin and Altman fail to mention it directly. Westin [21] touches upon it when he describes the need for privacy to achieve personal autonomy. He describes individuals as having different layers of protection around themselves; only a few close individuals are allowed to enter into the innermost layers closest to the true self. Similarly, Altman and Taylor [22] use an onion metaphor in their social penetration theory to explain the same phenomenon. An individual's personality has multiple layers, like an onion. As people get to know one another they penetrate each layer to come closer to the core of the individual. However, neither theorist incorporates the concept of trust into their privacy theories.

The concern about relinquishing control over personal space is evident in both theory and practice. Such concern indicates that individuals need to feel in control of their privacy at all times both on and offline. Furthermore, it is clear that individuals' privacy concerns are based on both real risks (such as identity theft) and a personal desire for privacy, even where no real risks exist. Trust enables the individual to feel more in control of a situation when the risks of the situation are unknown. Essentially, the degree of trust that individuals have in a third party affects their perception of the level of risk involved in any transaction with that third party.

The next two sub-sections review the existing literature on online trust and Rotter's concept of the locus of control [35]. Section four derives the final online privacy theory.

3.1. An Exploration of Online Trust

Liu et al. [36] believe that trust is a complex social phenomenon that reflects technological, behavioural, social, psychological and organisational aspects.

A body of research suggests that in order to facilitate individuals making trusting decisions online which may include imparting personal information online, the counterparty must engender a perception of trustworthiness. The literature suggests a number of characteristics that collectively create a perception of trustworthiness [37-39]. Most researchers differ when identifying the exact characteristics. Nevertheless, a set of common characteristics have been derived. Table 4, taken from [40] summarises these.

Table 1. Perceived characteristics of trustworthiness.

Perceptions of trustworthiness	Researcher
Competence Integrity Benevolence	[41]
Ability Integrity Benevolence	[42]
Competence Benevolence Integrity	[43]
Ability Integrity Benevolence	[39]
Knowledge and expertise Openness and honesty Concern and care	[44]
Competence Concern Openness Reliability.	[45]
Competence Benevolence Values	[46]
Ability Integrity Benevolence	[47]
Knowledge and expertise Openness and honesty Concern and care	[37] [38]
Competence Integrity	[48]

If imparting personal information online involves making a trusting decision, this literature could be interpreted as implying that online trust is a prerequisite for imparting personal information.

There is sufficient evidence to suggest that individuals differ greatly in their tendency to trust [39, 49-51] and an individual's propensity to trust is frequently proposed as one of several key determinants of online trust [39, 50-53]. Nevertheless, it must be noted at this point that because of the subjective nature of online trust, it is not possible to measure exactly how much trust is needed in a given scenario to ensure online privacy concerns do not arise.

3.2. The Locus of Control

The second concept that is part of online privacy is that of an individual's locus of control. The concept of locus of control was formulated by Julian Rotter in [35] and it refers to an individual's generalized expectations concerning where control over future events in their life resides. "Internal control" is the term used to describe the belief that control of future outcomes resides primarily in oneself while "external control" refers to the expectancy that control is outside of the individual, either in the hands of powerful others or due to fate or chance.

Individuals with an internal locus of control believe that they control their own destiny. They also believe that their own experiences are controlled by their own skill or efforts [54]. People who have an external locus of control tend to attribute their experiences to fate, chance, or luck. The situation is out of their control. These individuals generally do not learn from previous experience. Since they attribute both their successes and failures to luck or chance, they tend to lack persistence and not have high levels of expectation [54].

Generally, the formulation of locus of control stems from family, culture, and experience. Most so called internals have been shown to come from

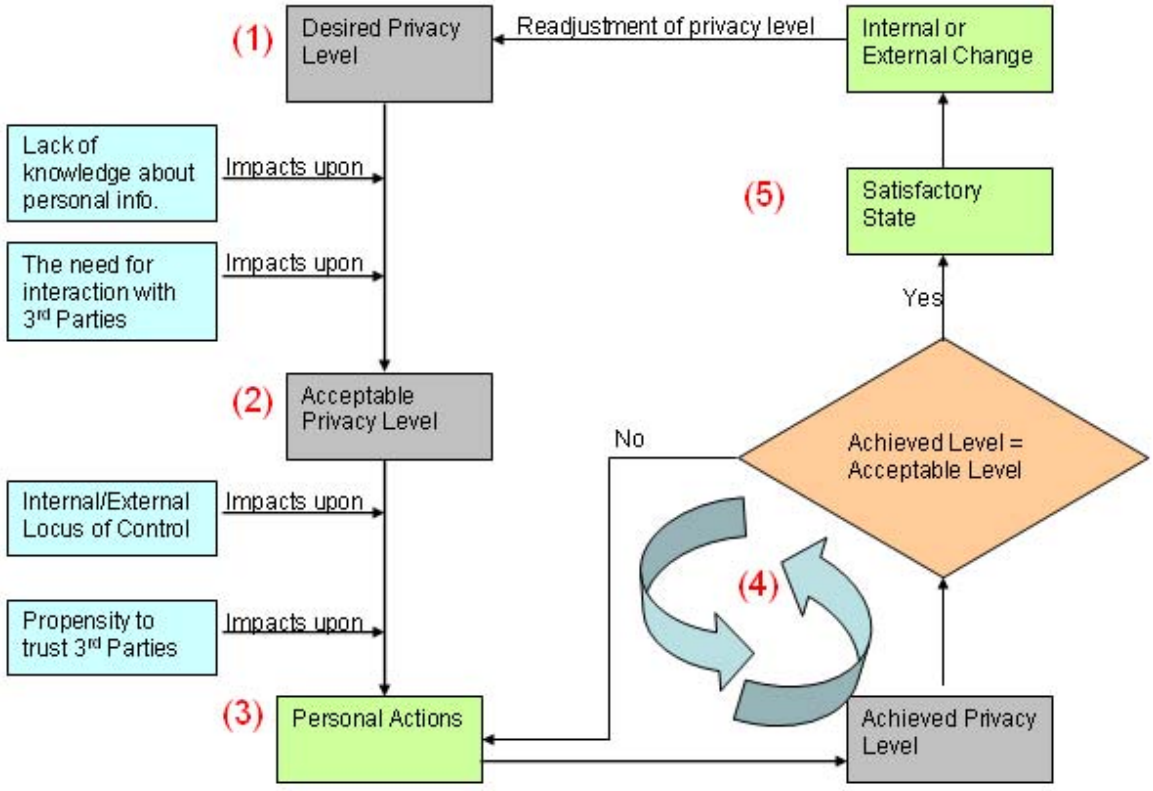

Figure 1 A model for online privacy

families that focused on effort, education, and responsibility. On the other hand, most externals come from families with a low socioeconomic status where there is a perceived lack of control over their lives [55].

3.3 The Model Explained

In light of these facts, that each individual typically experiences varying levels of trusting behaviour and has varying expectations regarding the sources of control, figure 1 shows an interpretation of online privacy by way of a model. This model aims to highlight areas where privacy concerns arise so that measures can be taken to reduce them. The model represents:

- The process by which an individual strives to achieve their desired level of privacy.
- The influencing factors that impact upon the possibility of achieving the desired level of privacy, namely:
  - Online privacy concerns;
  - Trust in the behaviour of external bodies;
  - The need to feel in control;
  - Other needs, for example, the need to buy items online requires the individual to submit credit card details to a third party online.

The 5 step process outlined in figure 1 can be explained as follows:

- Individuals move between the four dimensions and functions of privacy, outlined by Westin, until they achieve their desired level of privacy (1).
- They then encounter external factors from their environment, which impact on an individual's ability to achieve their desired level of privacy, such as privacy concerns and the need to interact with 3rd parties. As a result, they settle on an acceptable level of privacy (2).
- They take action to implement the acceptable level of privacy. The actions they take are heavily influenced by their propensity to trust and whether they have an internal or external locus of control. As a result, the personal actions differ from individual to individual (3).
- They continue to take action until the achieved level of privacy equals the acceptable level of privacy (4).
- They maintain that level of privacy until a new level is required due to internal and/or external changes and the process starts again (5).

Drawing together these ideas, the following statements regarding the concept of online privacy must be outlined before the online privacy theory can be presented:

1. Some degree of trust is a prerequisite for individuals to impart personal information online.
2. Individuals need to feel in control of their personal space while online.
3. A privacy theory should incorporate both concepts of trust and control in some manner if it is to describe accurately privacy in an online environment.

The next section outlines the privacy theory formulated by this research based on these statements.

4. A Theory of Online Privacy

This section proposes a definition of online privacy based on the literature and then goes on to develop this definition into a theory of online privacy. Online privacy, from the perspective of the individual, is defined as follows:

"*Online Privacy is the continuous process of negotiating, with relevant third parties, an optimum or acceptable level of disclosure of personal information in an online environment*."

This process involves a form of trusting behaviour on the part of the individual and encompasses both access to and use of their personal information.

In light of this definition, the concept of online privacy can be seen as a subjective decision-making process which necessitates negotiation with third parties for the continuous protection of personal information. Additionally, the optimum or acceptable level of online privacy for a given individual is greatly influenced by the individual's personal characteristics and pressures from their external environment. The principal pressures upon an individual from their external environment are:

- The quantity and reliability of the information that is available to the individual about the security of any personal information that they may have imparted online and the use to which that information may be put.
- The strength of the desire of the individual to obtain the goods, services or information provided by a third party.

The dominating personal characteristics influencing an individual's optimal level of online privacy are:

- Whether the individual has an internal or external locus of control. Individuals with an internal locus of control would have more of a need for the provision of online privacy guarantees such as privacy seals and privacy policies. Such individuals need to feel they are in control before they feel comfortable with imparting their personal information online. Individuals with an external locus of control would have less of a need for such provisions.

- An individual's propensity to trust online third parties. Individuals with a high propensity to trust have a lesser need for privacy guarantees. Inversely, individuals with a low propensity to trust have a greater need for privacy guarantees and for provision of information regarding the use of their personal information.

4.1. Conceptualising Online Privacy

The need for online privacy arises when individuals decide upon a level of social or commercial interaction that they desire from an online experience. They then take measures to reach this level. As seen from Westin's theory, there are four states of privacy within which an individual moves. These states of privacy are applicable not only in a physical space, but also in a virtual space.

Solitude, in an online context, translates into the desire of the individual to ensure that their actions and movements are not monitored while online. Goodwin in [13] argues that individuals often seek such solitude, when purchasing items either online or offline for three main reasons. The first reason is to enhance the quality of the consumption experience. The second is to avoid interference from disapproving reference groups and the third is to avoid the discomfort associated with self-discrepancy. She argues that while it is widely accepted that public displays of possessions communicate information about oneself, concealment can also help an individual achieve self-presentational goals. By achieving consumer solitude, the individual can maintain his or her presented self to specific audiences while experimenting with consumption behaviours to express a variety of possible selves.

The state of intimacy over the Internet means that being secluded in small online groups allows for the fostering of close relationships within those groups. These small online groups can exist in various guises over the Internet. For example, social networking sites, blogs and newsgroups allow for users to experience intimacy while online by being a member of a small group or community.

The state of Internet anonymity means freedom from identification and from surveillance or observation of any kind [56]. This is the state of privacy that allows individuals to be able to browse the Internet with a considerable amount of identity protection. Internet anonymity is not absolute. That is, the degree of anonymity one enjoys may vary. However, through a combination of public-key encryption and special anonymous remailer computers, messages can be sent over the Internet with a high degree of certainty that they cannot be traced to their originator [57]. Additionally, individuals can use cyber cafes as well as a variety of more sophisticated (and some illegal) techniques to remain anonymous online.

Reserve over the Internet encompasses actions such as an individual restricting the circulation of their email address to close friends in order to avoid unwanted advertising emails and spam. Additionally, individuals are entitled to expect that propagation of their sensitive information, such as their financial or health information is limited and controlled. However, not only information that is deemed private by society should be protected. Individuals have the right to determine what they consider their private information to be.

Even though an individual has a desired privacy state, they will sometimes need to accept a less than desirable state of privacy in order to interact in that environment. This is due to the influences of factors in the external environment which are outside of the individual's control. This less than desirable state of privacy is defined as the *optimal* or acceptable level of privacy that is achievable in a given external environment.

Once the optimal level of privacy has been decided upon by the individual, they can then carry out a series of actions to ensure it is achieved. For example, an individual may wish to remain anonymous while on the Internet, but over time the desire to buy an item online becomes stronger than remaining anonymous. Therefore, the individual carries out a series of preliminary actions to assess the risks involved in submitting their personal information (such as credit card details) online. Examples of such actions could be asking friends how safe it is to buy online, or checking the privacy policies of the vendor website to ensure the site safeguards personal information. Once individuals have assessed the online environment and the perceived risks involved, there are two choices available to them. They can decide that the need to buy online outweighs the perception of the risk of submitting their personal information, or they can decide to remain anonymous and forego the purchase. Individual choose the actions that bring them closest to their optimal level of privacy.

It is important to mention at this point that the desired level of online privacy is a non-monotonic function similar to Altman's description of the traditional concept of privacy. That is to say that complete online privacy is not necessarily the optimal solution. It is possible for an individual to experience too much or too little online privacy. When there is too much online privacy (actual > desired level), a person may be deprived of the opportunity to interact online. On the other hand, when there is too little privacy (desired > actual level), a person may feel the need for

more online solitude. The goal of this research is to obtain the optimal level of privacy for every individual at all times. The next subsection gives examples of how this research can be used to achieve that goal.

4.2. Application of the Theory

As stated in the previous section, the ultimate aim of this research is to obtain the optimal level of privacy for every individual at all times. In order to achieve this goal, this research suggests giving control of an individual's privacy back to the individual. In doing so, the individual's personal privacy preferences will determine the level of online privacy they experience.

One possibility which would give control back to the user would be to build a privacy slider application into web browsers which would allow the individual to specify their desired level of online privacy *before* going online. The slider could contain four privacy levels. These levels correspond to the states of privacy outlined in Westin's theory.

Choosing the solitude level on the privacy slider, the first of Westin's privacy states, would translate into the desire of the individual to prevent people they know offline from finding out their actions and movements online. By selecting online solitude, the individual maintains his or her offline self to offline audiences while experimenting with various online behaviours.

The level of intimacy on the privacy slider, corresponding to the second of Westin's privacy states, allows a select number of other users to see when the user is online. Being secluded in small online groups allows for the fostering of close relationships within those groups, while being invisible to the outside online world by blocking tracking applications and cookies.

If the user chooses the anonymous level, the third of Westin's states, they will be able to browse the Internet with a considerable amount of identity protection as the user's IP address will be withheld. Additionally, the privacy slider, when set to this level, will block any attempts by websites to track the user's online movements or to download any cookies onto the user's machine.

The reserve level of the privacy slider, the fourth of Westin's privacy states, restricts the possibility of identifying the user to a specified list of 'trusted' websites. If an unknown website seeks the user's identification, a warning message will appear reminding the user that the website is not a trusted site. Additionally, cookies and tracking applications will be blocked for all but trusted sites. This allows an individual to restrict the circulation of their personal information to trusted third parties.

Individuals can specify, from a list within the slider application, what they consider their private information to be and therefore what information to protect.

In order to ensure a user's desired state of privacy is achievable while interacting online, users must continuously assess the online environment and take necessary action. The privacy slider could aid the user in achieving their desired level of privacy by continually monitoring the online situation and the user's actions. It could use dynamic privacy policies and privacy policy agents to adjust and readjust a user's privacy needs for the duration of their time online. If the user's desired level of privacy is not possible as a result of the need to interact with online third parties, the privacy agents negotiate an 'optimal' level of privacy (see figure 1) for the user by prompting the user for the best course of action to take in the form of privacy messages and warnings. This allows the user to set their privacy according to their propensity to trust and the level of control they need in order to feel comfortable about their online privacy.

The World Wide Web Consortium (W3C) [58] has set up a project called the Platform for Privacy Preferences (P3P) which has defined a specification that allows the encoding of human-readable privacy policies into machine-readable XML. This specification could be used to develop the privacy slider application.

The privacy slider could have two main functions. Primarily, it could activate privacy policy agents which compare the user's desired level of privacy (solitude, intimacy, reserve or anonymity) with a website's XML privacy policy, (however, a limitation of this is that not all websites have XML privacy policies).

Secondly, the privacy application has functionality that acts in much the same way as a reputation system. The user has the ability to independently rate their experiences, by answering a series of questions with regard to how trustworthy they perceive the website to be and how they feel their private information is handled by the website.

A type of collaborative filtering algorithm could then determine ratings for the website in question. These privacy reputation ratings could be stored in an independent database. However, a limitation of this scenario is that it would take time for websites to build up their privacy reputations and also it is not clear where the independent database could be stored.

Whenever the user re-visits the website in question, their privacy slider application would check not only the websites XML privacy policy but also this reputation rating and verify it was equal to or above the privacy requirements of the user. If the privacy reputation rating was below the user's privacy requirements then a conflict would occur and the user

would be notified immediately. In this situation, the user could decide to ignore the privacy warning and continue interacting with the website or they could choose to disengage from the privacy negotiations and move onto another website. Such a system might also avail of independent agent information such as reliability ratings (cf. eBay). It should be possible to design such machine interfaces in a way that minimalizes the requirement for user intervention and, in a similar manner to current spam filters, such a system could learn over time to 'know' its user's preferences.

The conclusion discusses the contributions and the future work of this research.

5. Conclusions and Future Work

The next step in this research is to validate the privacy control theory. This will be achieved by carrying out a series of non-participant observation sessions over a six month period. The sessions will be carried out by observing computer literate individuals while they spend time online. Each session will last for one hour and each participant will be observed for a minimum of 10 hours over the six month period. The participants will be a representative mix of male and female Irish adults of various ages.

The overall objectives of this research are twofold. Firstly, it seeks to develop, through the use of an online privacy model, a theory of online privacy that reflects adequate privacy needs in all online experiences. Secondly, once a theory of privacy has been satisfactorily defined and validated, it can be used to form the basis for the design of an interface between the user and the Internet

The importance of this research lies, firstly in defining the concepts of online privacy which in turn contributes towards determining an individual's privacy needs in the digital world. Secondly, it lies in contributing towards preventing privacy abuses to that individual once they have divulged private information online. If the latter is achieved, this research will have contributed towards regaining control of the online privacy of not only adults but also of the most cherished and most vulnerable in society, children.

References

[1] CBS News, "Laptop with bank details of over a million Britons sold on eBay," vol. 2008: CBS News, 2008, pp. http://www.cbc.ca/consumer/story/2008/08/26/ebay-britain.html.

[2] Privacy Rights Clearinghouse, "A Chronology of Data Breaches," vol. 2008. San Diego: Retrieved on 23rd January 2008 from: Privacy Rights Clearinghouse: http://www.privacyrights.org/ar/ChronDataBreaches.htm, 2005.

[3] A. F. Westin, "Social and Political Dimensions of Privacy," *The Journal of Social Issues*, vol. 59, pp. 431-453, 2003.

[4] United Nations, "Universal Declaration of Human Rights," in *General Assembly resolution*, vol. 217, *United Nations*, 1948, pp. A (III).

[5] The Council of Europe, "The European Convention on Human Rights," in *C364*, *European Union*, 1950.

[6] The Council of Europe, "The Charter of Fundamental Rights of the European Union," in *C364*, *European Union*, 2000.

[7] S. J. Milberg, S. J. Burke, H. J. Smith, and E. A. Kallman, "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM*, vol. 38, pp. 65-74, 1995.

[8] C. Fried, "Privacy [a moral analysis]," in *Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press, 1968, pp. 333-345.

[9] J. H. Moor, "Towards a theory of privacy in the information age," *ACM SIGCAS Computers and Society* vol. 27, pp. 27-32, 1997.

[10] H. T. Taviani, "Philosophical Theories of Privacy: Implications for An Adequate Online Privacy Policy," *Metaphysics*, vol. 38, 2007.

[11] S. Zhao, "Do Internet Users have more Social Ties? A Call for Differentiated Analyses of Internet " *Journal of Computer-Mediated Communication*, vol. 11, 2006.

[12] E. Boritz, W. G. No, and R. P. Sundarraj, "Internet Privacy: Framework, Review and Opportunities for Future Research," *Available at SSRN: http://ssrn.com/abstract=908647* 2006.

[13] C. Goodwin, "A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption," *Journal of Consumer Psychology*, vol. 1, pp. 261-284, 1992.

[14] S. T. Margulis, "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *The Journal of Social Issues*, vol. 59, pp. 411-429, 2003.

[15] S. T. Margulis, "Privacy as a Social Issue and Behavioral Concept," *The Journal of Social Issues*, vol. 59, pp. 243-262, 2003.

[16] S. T. Margulis, J. A. Pope, and A. Lowen, "The Harris-Westin's Index of General Concern About Privacy: An Attempted Conceptual Replication," vol. 2007: Seidman College of Business, Grand Valley State University, Grand Rapids, Michigan, U.S.A.
Notes, 2006.

[17] N. Marshall, "Dimensions of Privacy Preferences," *Multivariate Behavioral. Research*, vol. 9, pp. 255-271, 1974.

[18] H. Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy*, vol. 17, pp. 559-596, 1998.

[19] W. A. Parent, "A New definition of Privacy for the Law," *Law and Philosophy*, vol. 2, pp. 305-338, 1983.

[20] M. Rotenburg, "What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy," *Stanford Technology Law Review*, 2000.

[21] A. F. Westin, *Privacy and Freedom*. London: The Bodley Head Ltd, 1970.
[22] I. Altman, *The Environment and Social Behavior*. Monteray, California: Brooks/Cole, 1975.
[23] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences," presented at The 1st ACM conference on Electronic commerce Denver, Colorado, United States 1999.
[24] J. A. Castañeda and F. J. Montoro, "The effect of Internet general privacy concern on customer behavior," *Electronic Commerce Research*, vol. 7, pp. 117-141, 2007.
[25] G. S. Dhillon and T. T. Moores, "Internet Privacy: Interpreting Key Issues," *Information Resources Management Journal*, vol. 14, pp. 33-37, 2001.
[26] T. Dinev and P. Hart, "Internet Privacy Concerns and their Antecedents - Measurement Validity and a Regression Model," *Behaviour and Iinformation Technology*, vol. 23, pp. 413-422, 2004.
[27] J. F. George, "The Theory of Planned Behavior and Internet Purchasing " *Internet Research: Electronic Networking Applications and Policy*, vol. 14, pp. 198-212, 2004.
[28] Harris.Interactive, "Privacy On and Off the Internet: What Consumers Want," Privacy & American Business, Hackensack, New Jersey 22 May 2007 2002.
[29] K.-L. Hui, H. H. Teo, and S.-Y. T. Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, vol. 31, pp. 19-33, 2007.
[30] G. R. Milne and M. E. Boza, "Trust and concern in consumers' perceptions of marketing information management practices.," *Journal of Interactive Marketing*, vol. 13, pp. 5-24, 1999.
[31] J. Phelps, G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information.," *Journal of Public Policy & Marketing*, vol. 19, pp. 27-42, 2000.
[32] J. E. Phelps, G. D'Souza, and G. J. Nowak, "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation.," *Journal of Interactive Marketing*, vol. 15, pp. 2-17, 2001.
[33] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, vol. 20, pp. 167-196, 1996.
[34] M. Moloney and F. Bannister, "Online Privacy: Measuring Individuals' Concerns," in *EC Web 2008*, G. Psaila and R. Wagner, Eds.: Springer-Verlag Berlin Heidelberg, 2008, pp. pp. 21 – 30.
[35] J. B. Rotter, "Generalized expectancies for internal versus external control of reinforcements.," *Psychological Monographs*, vol. 80, pp. 1-28, 1966.
[36] H. Li, Z. Chen, X. Qin, C. Li, and H. Tan, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks," 2002.
[37] B. Barber, *The Logic and Limits of Trust*. New Brunswick, New Jersey: Rutgers University Press, 1983.
[38] V. T. Covello, "Trust and Credibility in Risk Communication," *Health Environment Digest*, vol. 6, pp. 1-4, 1992.
[39] M. k. O. Lee and E. Turban, "A Trust Model for Consumer Internet Shopping," *International Journal of Electronic Commerce*, vol. 6, pp. 75-91, 2001.
[40] R. Connolly and F. Bannister, "Consumer Trust in Internet Shopping in Ireland: Towards the Development of a more Effective Measurement Instrument," *Journal of Information Technology* vol. 22, pp. 102-118, 2007.
[41] S. C. Chen and G. S. Dhillon, "Interpreting Dimensions of Consumer Trust in E-Commerce," *Information Technology and Management*, vol. 4, pp. 303 - 318 2003.
[42] A. Bhattacherjee, "Individual Trust in Online Firms: Scale Development and Initial Test," *Journal of Management Information Systems* vol. 19, pp. 211 - 242 2002.
[43] D. H. McKnight, V. Choudhury, and I. S. R. C. Kacmar(2002) Developing and Validating Trust Measures for E-Commerce: An Integrative Typology, 13(3) pp. 334-359., "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research*, vol. 13, pp. 334-359, 2002.
[44] R. G. Peters, V. T. Covello, and D. B. McCallum, "The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study," *Risk Analysis*, vol. 17, pp. 43-54, 1997.
[45] A. K. Mishra, "Organizational Responses to Crisis: The Centrality of Trust," in *Trust In Organizations*, Kramer, M. Roderick, and T. Tyler, Eds. Newbury Park: Sage, 1996, pp. 261-287.
[46] S. B. Sitkin, "On the Positive Effect of Legalization on Trust," in *Research on Negotiation in Organizations*, vol. 5, R. J. Bies, R. J. Lewicki, and B. J. Sheppard, Eds. Greenwich: CT: JAI Press, 1995, pp. 185-217.
[47] R. C. Mayer, J. D. Davis, and F. D. Schoorman, "An Integrative Model of Organisational Trust," *Academy of Management Review* vol. 20, pp. 709 – 734, 1995.
[48] J. K. Lieberman, *The Litigious Society*. New York: Basic Books, 1981.
[49] P. J. Ambrose and G. L. Johnson, "A Trust Model of Buying Behavior in Electronic Retailing," presented at The Association for Information Systems, Baltimore, MD, 1998.
[50] D. Gefen, "E-Commerce: The role of familiarity and trust. ," *The International Journal of Management Science*, vol. 28, pp. 725–737, 2000.
[51] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* vol. 15, pp. 336-355, 2004.
[52] D. H. McKnight and N. L. Chervany, "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology.," *International Journal of Electronic Commerce*, vol. 6, pp. 35-59, 2001.
[53] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Initial Trust Formation in New Organisational Relationships," *Academy of Management Review*, vol. 23, pp. 473-490, 1998.
[54] D. Gershaw, "Line on Life: AIDS and Teenagers," vol. 2008. Retrieved from: http://virgil.azwestern.edu/~dag/lol/AIDSTeens.html, 1989.

[55] H. Levenson, "Multidimensional Locus of Control in Psychiatric Patients," *Journal of Consulting and Clinical Psychology*, vol. 41, pp. 397-404, 1973.
[56] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology¬ ▯ [57] M. A. Froomkin, "Anonymity and Its Enmities " *Journal of Online Law*, vol. Article 4, 1995.
[58] "Platform for Privacy Preferences (P3P) Project: Enabling smarter Privacy Tools for the Web," vol. 2006: World Wide Web Consortium, 1994.