

# **Socially-Informed Privacy-Enhancing Solutions Economic Privacy and the Negotiated Privacy Boundary**

Charis A. Kaskiris<sup>1</sup>  
kaskiris@sims.berkeley.edu  
School of Information Management and Systems  
UC Berkeley

Workshop on Socially Informed Design of Privacy-enhancing Solutions in Ubiquitous Computing

UBICOMP 2003  
Seattle, WA

October 2003

## **Abstract**

Recent literature in ubiquitous computing proposes the use of conceptual models from the social sciences to inform the design of privacy-preserving technologies. The social sciences on the other hand provide a variety of normative and positive models of human behavior based partly on empirical observation and predominately on modeling cultures of the different disciplines. Designers of privacy-related ubiquitous technologies ought to first understand the nature of privacy and how it affects the behavior of the users of such technologies and then utilize the models of behavior which are closer to actual behavior. We discuss in particular the characteristics of economic privacy and how applying behavioral economic modeling may produce qualitatively different results than rational modeling. We propose that humanly usable systems need to incorporate qualitatively valid social thinking into them and offer some cautionary remarks on issues relating to identification problems in the social sciences.

## **1. Introduction**

Socially-informed design of privacy-enhancing solutions in ubiquitous computing incorporates social science insights and models in assessing the way users will interact with such systems and how their concerns for privacy can or should be accommodated. Viewing privacy as the right to control the release of private information or information created by a private party, then privacy concerns arise once such release of information leads to decreasing the party's well-being<sup>2</sup>. Ubiquitous computing technologies at a rudimentary level are surveillance mechanisms as their main purpose is the collection of personalized information, and as such, require differentiated levels of information disclosure from users. These technologies include a variety of information collection and use applications and may vary in the way they store, process, and interconnect information. Personal digital assistants which store local user information for local use, passive sensors which collect topical information regardless of users, reactive sensors that act on disclosure of particular forms of information, interconnected data sharing personalization services. Certain technologies may be interactive in nature and hence may require active disclosure of information for participation. Hence, informed design of such solutions requires an understanding of human behavior in assessments of privacy when they interact in ubiquitous computing environments.

### *Properties of Privacy-Related Information*

---

<sup>1</sup> I want to thank Jose Signoret and Vanessa Arce for useful conversations and Yale Braunstein and Maarten Sierhuis for useful comments and suggestions.

<sup>2</sup> This interpretation may include utilitarian approaches as well as well-being metrics as described in Hedonic Psychology (Kahnemann, Diener & Schwartz, 1999). Langheinrich (2002) provides different definitions of privacy. Our definition is closer to the one provided in Westin as described in Langeheinrich.

Privacy possesses the characteristics of public goods, that is, non-rivalry and non-excludability. Non-rivalry is the property of information of not diminishing through its consumption. Non-excludability is the property of information that allows multiple users to concurrently make use of it.<sup>3</sup> Another important property of privacy-related information, however, is its recombinant growth property, that is the creation of additional information by recombining information through patterns in the information. At an abstract level, this property relates to two main aggregation mechanisms which render seemingly equal information transactions to create more information than the information disclosed or possessed at the time of its release.

Firstly, a user may possess static private information regarding her individual preferences but may also engage in the generation of new information through transactions with her environment or other users within these environments. Certain transactions may be revealing identification information in order to be able to acquire access to certain goods or information or groups within a particular context. If the same user reveals the same information in another context, then it renders the two contexts conditionally dependent, even though they are independent. Hence, by revealing the same information in different contexts the user has created more information. Secondly, a different aggregation mechanism may also reveal additional information about the user from the same level of information revelation. Information aggregation points gain categorical knowledge of distributional characteristics of a user (e.g. she is an average user as she does what the average user does) by collecting information over many users. Then even though the user has the perception of only revealing static information, she has effectively created more dynamic information about herself, some of it which was unknown to her at the time of disclosure. Ubiquitous computing environments enhance the effect of the recombinant growth property through their ability to make both revealed preferences and behavioral information, persistent (Palen & Dourish, 2003) and most importantly structured. Acquisti (2002) argues that ubiquitous computing environments increase the uncertainties of the use of information over time and across transactions. We relate this insight into behavioral models of judgment under uncertainty.

Following our definition of privacy and its properties, we can identify the main threat to a user's economic privacy as being the use of persistent structured information and technologies to classify users into willingness-to-pay groupings, which leads to effective price discrimination against them. Oldzyko (2003) argues that the continuing tension between sellers who want to provide individual-based pricing and buyers who resist such surplus extraction out of them, will dictate which technologies will be adopted widely<sup>4</sup>. The boundary of this tension depends crucially on user judgment and assessment of such possible violations and the willingness to participate, a boundary that needs to be negotiated.

The purpose of socially-informed design of privacy-preserving technologies is to enable user effective participation by meeting both the participation constraints of a user and also provide incentives for users to take advantage of differential services in such environments. Acquisti (2002) provides a discussion of how economic theory of incentives may provide insights into the design of such systems and privacy enhancing technologies. We argue that there are more concerns beyond incentives which relate to systematic biases in the way humans make assessments of the value of their own privacy.

In the next sections we discuss social-science approaches discussed in the ubiquitous computing and privacy literature. In particular, we make use of rational economic modeling as an approach to understanding how this privacy boundary is defined. We highlight important limitations of such an approach and show that alternative behavioral economic models may provide different insights which are important in the design of such systems.

---

<sup>3</sup> Varian (1998) provides a discussion of markets for information goods.

<sup>4</sup> There are obviously further non-economic concerns regarding release of private information and private patterns of transactions relating to security, prosecution, and surveillance, which we are not explicitly dealing with here.

In section 2 we provide a short discussion of recent literature on privacy and ubiquitous computing. In section 3 we discuss judgment under uncertainty from economic theory and how alternative interpretations using behavioral models may provide different insights into privacy assessments. In section 4 we present the issue of self-serving biases and how perceptions of fairness may make users refuse to participate in ubiquitous computing environments where the privacy policies may be deemed unfair. Finally we conclude with the belief that the proper form of social science models which will help in better ubiquitous computing solutions are ones that are empirically grounded.

## **2. Social Models of Privacy**

Recent literature on privacy and ubiquitous computing has focused on bringing social science insights into the design of ubiquitous systems. Palen and Dourish (2003) propose the application of Irwin Altman's theory of privacy which views it as a dynamic dialectic process. The authors identify three main boundaries that need to be negotiated, namely (1) the disclosure boundary, (2) the identity boundary, and (3) the temporal boundary. In the identity boundary discussion the authors mention the problem with the persistence of information that is something that ubiquitous computing provides are outside the control of the user. The authors also claim that the institutional setting of the environment in which this technology will be implemented needs to be taken into consideration. This argument follows incentive engineering approaches which are the realm of implementation theory in economics<sup>5</sup>. In the identity boundary there is the problem of providing enough information to be an effective participant versus nonparticipation due to privacy concerns. In such a boundary, there is the possibility of non-truthful revelation of preferences. Rational economic models provide strategy-proof approaches to this, where no user has any benefit from misrepresenting her preferences<sup>6</sup>. Finally, in the temporal boundary specific instances of information disclosure are not isolated from each other; they occur as the outcome of a sequence of historical actions, and as the first of many expected actions stretching out into the future.

Langheinrich (2002) proposes that privacy violations are border crossings (citing Gary T. Marx). These borders are physical, social, spatial and temporal, and transitory. These borders are negotiated through the interaction of the system with the user or the expectations of a group of users. This is similar to the proposed boundary negotiation proposed by Palen and Dourish (2003), where aligning the incentives of the users for disclosure of information is as crucial as building the system to accommodate such functionality. This of course would work if the actual users of the system behave rationally<sup>7</sup>. Acquisti (2002) and Varian (as cited in Acquisti 2002) discusses areas in which economic theory may help in the design of mechanisms which are privacy enhancing. The notion is that a user, faced with an uncertain future use of her information, makes an assessment knowing the set of future states and the probability distribution over that set and assesses the expected utility of participating or not. If the expected utility, calculated as the sum of the value of possible future states, then the user can make an informed decision on whether to participate with a technology or not and to what extent to do so. These models assume that the users know the set of possible states of the world, that the users know the probability distribution over this set, that these users are self-interested and finally that these users can perform assessments using a formal and extensive algorithmic processing.

Attempting to validate predictions of the rational economic models, research in the psychology of decisions and judgment has explored and identified systematic behaviors that counter the assumptions and predictions of the rational economic models. Some of the results extend rational

---

<sup>5</sup> See Chapter 10 of Rubinstein and Osborne for a technical introduction; Acquisti (2002) provides a less technical discussion and references.

<sup>6</sup> A proposal for strategyproof systems is described in (Ng, Parkes & Seltzer, 2003).

<sup>7</sup> Alfie Kohn argues that such incentives schemes only provide compliance temporarily and in the long run they cause more harm than good (Kohn, 1999).

theory and some have different results under certain conditions. These models objective is to strive for closer empirical validity. We look at specific areas of behavioral economics which may provide insight into how humans behave in environments where they have to negotiate over their right to privacy and the provision of services (Kahneman & Tversky, 2000)(Gilovich, Griffin, Kahneman 2003). Rabin (2000) provides a rather non-technical introduction to behavioral economics. Even though this research was not specific to privacy, its insights may prove useful in out understanding of privacy assessments as they deal with the more universal concept of judgment. In the case of privacy judgment under uncertainty is critical.

### **3. Judgment under Uncertainty and Time**

In negotiating the different boundaries of privacy, a user may have to deal with different levels of assessment. If a protocol of negotiating the extend of private information release exists, then the user needs to make an assessment what are the potential payoffs/costs of her action today and its impact on future benefits/costs before making an decision to participate and at what level to do so.

The classical model of rational choice assumes that a rational user will choose what action to pursuit by assessing the probability of each possible outcome, discerning the utility of each outcome, and calculate the expected utility of each outcome. The option followed will be the optimal level of utility and uncertainty. Systems that incorporate such models need to incorporate such assumptions.

There are three areas were such assumptions have systematic empirical validity deviations: (1) the recombinant growth nature of privacy-related information and the structured persistence of captured information makes the set of possible privacy-related outcomes a dynamic rather than a static one (hence, a rational user needs to make assessments of the future possible outcomes from future recombination of information) increasing the complexity of the problem; (2) user's assessments of likelihood and risk do not conform to the laws of probability but rather through heuristics; (3) calculations of probability and multi-attribute utility are formidable tasks even for doctoral students in statistics. (Introduction in Gilovich, Griffin, Kahneman 2003).

Kahneman and Tversky (2000) have provided a heuristic approach which is categorically different from rational models. They propose three general heuristics – availability, representativeness, and anchoring and adjustment – that underlie human intuitive judgments. In the case of privacy assessments, the availability heuristic may piggyback on knowledge of similar situations and effects of loss of privacy. In making an assessment of the computing environment and the likelihood of these negative effects taking place, the user assess the similarity between these cases (piggyback on automatic pattern recognition) and finally the user may have a default expectation of these losses and the probability of these losses which then uses to adjust his valuation (based on an anchor value, i.e. 50% of getting spammed). Hence, given that we expect users to be behaving in such a way then maybe systems need to provide enough information for the users to be able to make better quick assessments of the privacy threats of the system. Kahneman and Tversky also observe that users are in general overconfident regarding the possibility of something bad happening to them and they will more probably engage in risky privacy practices where such risk is not warranted.

Furthermore, in choice over time, humans exhibit present-biased preferences (O'Donahue & Rabin, 2000) as evidenced by procrastination, gym-participation, and addiction (e.g. smoking). Present-biased preferences use hyperbolic discounting versus the exponential discounting offered by rational models. It is important to note that the exponential model of discounting has been one proposed by Savage and accepted as the norm within the rational choice community. It is not an empirically driven formulation but rather a mathematical. In making assessments about present a future utility users are modeled to perform dynamic programming. Obviously, such a calculation is not in the realm of a user who needs to assess the future utility of accepting to reveal a certain

degree of information. Herbert Simon (1957) provided a different model of reasoning using simple heuristics to make such assessments, that is, the users are bounded rational.

Finally, even the institutional (incentive) setting in which the judgment is made, may promote temporal compliance but no long run well being<sup>8</sup>. Alfie Kohn (1999) would argue that incentive schemes to promote information sharing are ways of taking advantage of the present-biasedness of users in assessing future costs versus current rewards. A large reward now blurs the future possible losses from future abuse of privacy-related information. Most of the problems with information disclosure are of this sort, that is, at the time of a basic transaction the user fails to foresee that the current reward is dwarfed by endless spam deleting in the future.

#### **4. Bargaining over Boundaries**

Another problem with engaging in an information-sharing transaction with such a system comes from problems with self-serving biases in assessments of fairness and the retaliatory nature of the response in bilateral bargaining situations. These arise in many contexts in social sciences where the two parties involved in a negotiation have a common interest in transacting since they can both become better off thru agreement to trade. Examples arise in the context of international affairs, marriage counseling, labor disputes, civil litigation, and credit attribution. Many of these negotiations unfold over long periods of time and provide many opportunities for parties to interact and decide on the terms of the trade, that is, how the surplus produced will be divided. Nevertheless, in many occasions, negotiations reach no conclusion over the terms of the trade and lead to impasses. An impasse describes a state where both parties agree to disagree. The topic of this paper is an investigation of behavioral aspects of negotiators that lead them to negotiate in a manner that leads to impasses.

Traditional bargaining theory has evolved through two strands of research: the traditional axiomatic Nash Bargaining Solution (Nash, 1950, 1953) and the game theoretic, non-cooperative or sequential models starting with the perfect equilibrium concept (Rubinstein, 1982)<sup>9</sup>. In the game-theoretic setting impasses is attributed typically to incomplete information. Each party possesses private information about factors such as their alternatives to negotiated agreements, costs of delay and reservation values, causing them to be mutually uncertain about the other side's reservation value. Uncertainty produces impasse because parties use costly delays to signal to the other party information about their own reservation value (Kennan and Wilson, 1989; Crampton, 1992).

In their article "Explaining Bargaining Impasse: The Role of Self-Serving Biases" (Babcock and Loewenstein, 1997), Babcock and Loewenstein invoke the notion of self-serving biases to account for behavior in a rich variety of settings, for instance, the failure to reach an agreement in laboratory bargaining games, the behavior of job searchers, and the discrepancy between plaintiffs' and defendant's assessments of tort cases. They propose that self-serving bias may be a causal factor of the impasse in the negotiation thru the following effects:

- (a) If the two parties perceive the values of their alternatives to negotiated settlements in self-serving ways which lead to the elimination of the contract zone;
- (b) If each party believes that their notion of fairness is impartial and shared by both sides, then they will interpret aggressive bargaining by the other side as an unfair practice which may cause the former party to retaliate<sup>10</sup>;
- (c) Negotiators are strictly averse to bargaining below their perceived fairness level and given the self-serving bias fail to accept a deal that makes them better off.

---

<sup>8</sup> Alfie Kohn (1999) provides arguments against the behaviorist approach to psychology and discusses that incentive schemes only provide temporal compliance but not aggregate well-being. Revelation of privacy information seems to follow the same vein of temporal reward for future cost.

<sup>9</sup> For a modern treatment of bargaining theory Muthoo (1999) offers a discussion of models and applications.

<sup>10</sup> For a thorough discussion of social preferences and the notion of fairness Rabin (1993) offers a literature review and a model that deals with actors being willing to harm themselves to punish an unfair counterparty.

Furthermore, research in psychology and economics has shown that parties care not only about what the offer is but also care about the fairness of the proposal reflecting on her party's motivations (Rabin 1993). Following Rabin, we also propose that there is a fourth effect that is in effect that Babcock and Loewenstein have not investigated:

- (d) When negotiators perceive an unfair proposal they become vindictive and may harm themselves through an impasse rather than giving any gain to the other party.

The importance of these findings is that if a user of an ubiquitous computing solution or environment, perceives that the system is setup in way that it unfairly treats the user's concerns over the disclosure of information, then the user may choose to not participate at all, even though in doing so both the system and the user will benefit. This means that the system has to be able to make better assessments of what a fair level of information sharing is and what a fair level of information protection guarantees are needed so as to be perceived that it is a fair state of affairs.

## **5. Designing for Privacy**

What we have seen in our discussion is that models from the social sciences may vary in their predictions of the behavior of humans in different environments. Given the properties of privacy-related information and the exacerbation of their effects by ubiquitous computing technologies, it is important for designers of ubiquitous computing solutions to try to better understand the intentions, limitations, and the difficulty of assessment of users when it comes to privacy and how ubiquitous computing environments affect that. Behavioral models in privacy may need further experimental investigation as proposed by Acquisti & Grossklags (2003).

Social psychologists<sup>11</sup> have investigated human behavior empirically. What they have uncovered about understanding and predicting behavior is that the single best predictor of whether a person will or will not engage in a given behavior is that person's intention to perform that behavior and that there are relatively few variables that serve as the immediate determinants of intention (and behavior). Furthermore, the relative importance of attitudes and norms as determinants of intentions (and behaviors), depends upon both the behavior under consideration and upon the population considered. In a ubiquitous computing environment users may behave in particular ways with regards to their privacy attitudes following a few determinants of intention – which might be fairness assessments, or prior experience.

Finally, social sciences are not exact sciences. Different models may dictate different data collection requirements and user interfaces. Building mechanisms in systems that assess the behavior of users may also be prone to data analysis problems which are pervasive across all social sciences, such as the identification problem Manski (1995). Identification problem deals disambiguating cause and effect when data is collected from simultaneous behaviors. As Manski proposes, designers who incorporate computational logic based on behaviorally collected data need to tolerate ambiguity.

## **6. Conclusion**

We have looked at the nature of privacy-related information and how the impact of ubiquitous computing may exacerbate privacy assessment calculations. Different social theories of negotiating over boundaries and the difficulty in assessing privacy related risks and utilities were further explored. Rational choice models from economics would have different expectations on how users will interact with such systems. We propose the use of models of human behavior towards privacy which are empirically validated. Social science models may also suffer from empirical validation problems which might affect the way systems use that information. Such models will help in the design of more human-centric ubiquitous computing solutions.

---

<sup>11</sup> See Martin Fishbein's work.

## References

- Acquisti, Alessandro and Jens Grossklags (2003) "An Experimental Approach to Information Security Attitudes and Behavior," in: *Proceedings of the Second Annual Workshop Economics and Information Security (WEIS 2003)*, College Park, Maryland, US, May 29-30, 2003.
- Acquisti, Alessandro (2002) "Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments," *Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02)*, Goteborg, Sweden.
- Babcock, Linda and George Loewenstein (1997), "Explaining Bargaining Impasse: The Role of Self-Serving Biases," *JEP*, 11, 1: 109-126.
- Babcock, Linda, Xianghong Wang and George Loewenstein (1996), "Choosing the Wrong Pond: Social Comparisons in Negotiations that Reflect a Self-Serving Bias." *QJE*, 111, 1: 1-19.
- Chatterjee, Kalyan (1982), "Incentive Compatibility in Bargaining Under Uncertainty," *QJE*, 97, 4: 717-726.
- Crampton, Peter (1992), "Strategic Delay in Bargaining with Two-sided Uncertainty," *RES*, 59: 205-225.
- Gilovich, Thomas; Griffin, Dale W. and Kahneman, Daniel. *Heuristics and Biases: The Psychology of Intuitive Judgment*. Cambridge, U.K.; New York: Cambridge University Press, 2002.
- Kahneman, Daniel; Diener, Ed and Schwarz, Norbert. *Well-Being : The Foundations of Hedonic Psychology*. New York: Russell Sage Foundation, 1999.
- Kahneman, Daniel and Tversky, Amos. (2000) *Choices, Values, and Frames*. New York Cambridge, UK: Russell sage Foundation; Cambridge University Press, 2000.
- Kennan, John and Robert Wilson (1989), "Strategic Bargaining Models and Interpretation of Strike Data," *Journal of Applied Econometrics*, 4: 87-130.
- Kohn, Alfie. (1999) *Punished by Rewards : The Trouble with Gold Stars, Incentive Plans, A's, Praise, and Other Bribes*. Boston: Houghton Mifflin Co., 1999.
- Lederer, Scott Anind K. Dey, Jennifer Mankoff. (2002). "Everyday Privacy in Ubiquitous Computing Environment," *Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02)*, Goteborg, Sweden.
- Langheinrich Marc (2002), "Privacy Invasions in Ubiquitous Computing," *Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02)*, Goteborg, Sweden.
- Manski, Charles F.(1995) *Identification Problems in the Social Sciences*. Cambridge, Mass.: Harvard University Press.
- Muthoo, Abhinay (1999), *Bargaining Theory and Applications*: Cambridge: Cambridge.

- Nash, John (1950), "The Bargaining Problem," *Econometrica*, 18:155-162.
- Nash, John (1953), "Two Person Cooperative Games," *Econometrica*, 21: 128-140.
- Ng, Chaki, David C Parkes, Margo Seltzer (2003) "Strategyproof Computing Systems: Infrastructures for Self-Interested Parties". *Workshop on Economics of Peer-to-Peer Systems, SIMS, Berkeley*.
- O'Donoghue, Ted and Matthew Rabin (2000), "The Economics of Immediate Gradification," *JBDM*, 13: 233-250.
- Oldzyko, Andrew (2003). *Privacy, Economics, and Price Discrimination on the Internet*. Mimeo Digital Technology Center, University of Minnesota.
- Osborne, Martin J. and Rubinstein, Ariel. *A Course in Game Theory*. Cambridge, Mass.: MIT Press, 1994.
- Palen, Leysia and Paul Dourish. (2003). Unpacking "Privacy" for a Networked World. In *Proceedings of the ACM Conference on Human Factors in Computing Systems CHI 2003* (Fort Lauderdale, FL). New York: ACM.
- Rabin, Matthew (1993) "Incorporating Fairness into Game Theory and Economics," *AER*, 83, 5: 1281-1302.
- Rabin, Matthew (2002) "A Perspective on Psychology and Economics," *European Economic Review*, 46, 657-685.
- Roth, Alvin E. (1995), "Bargaining Experiments" In Kagel, John and Alvin Roth, eds. *Handbook of Experimental Economics*. Princeton: Princeton UP: 253-348.
- Rubinstein, Ariel (1982), "Perfect Equilibrium in a Bargaining Model," *Econometrica*, 50: 97-109.
- Simon, Herbert Alexander (1957). *Models of Man: Social and Rational; Mathematical Essays on Rational Human Behavior in a Social Setting*. New York,: Wiley
- Varian, Hal. (1998). *Markets for Information Goods*,  
<http://www.sims.berkeley.edu/~hal/Papers/japan/>.