Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited

Christian Flender and Günter Müller

Institute of Computer Science and Social Studies
University of Freiburg
Freiburg, Germany
{flender, mueller}@iig.uni-freiburg.de

Abstract. The paper at hand aims to provide a rational explanation of why people generously give away personal data while at the same time being highly concerned about their privacy. For many years, research has come up with attempts to untangle the privacy paradox. We provide a thorough literature review on privacy decisions in socio-economic scenarios and identify explanatory gaps. To explain paradoxical behavior in privacy decision making we illuminate (1) generous data disclosure and (2) high valuation of privacy as two non-commuting observations of incompatible preferences (types). Abstract risk awareness of privacy threats and concrete privacy decisions are not interchangeable, i.e. disclosing personal data prior to becoming aware of privacy risks does not equal the raising of risk awareness before revealing personal information. Privacy decisions do not commute as subjects may alter their preferences indeterminately, i.e. at the time an actual decision is made, in response to discomfort arising from conflicting preferences.

Keywords: Privacy, Indeterminacy, Noncommutativity.

1 Introduction

The unprecedented success of recent internet services dealing with personal data fulfills the need of many companies to know their customers. As companies progress in transforming their business by incorporating the collection, storage, and analysis of vast amounts of consumer data, opportunities for addressing the right target groups with their individual preferences rises. However, consumers becoming increasingly transparent with regard to their preferences also raise concerns over the erosion of their privacy. Many surveys witness serious privacy concerns of consumers[1]. This appears paradoxical as they easily forget about their fears provided the right circumstances like entertainment, attention, or comfort are given, i.e. the benefits received in return for data disclosure. Moreover, the disparity between stated preferences and actual behavior, i.e. the privacy paradox, may not only turn out to be disadvantageous for consumers.

[1] cf. https://www.cdt.org/privacy/guide/surveyinfo.php

J.R. Busemeyer et al. (Eds.): QI 2012, LNCS 7620, pp. 148–159, 2012.

Also for service providers this may have negative consequences. Consumers confronted with their paradoxical behavior, e.g. when finding out about their personal data being used without consent, may react with resentment, which may cause damage to customer relationships[1].

Economically, the privacy paradox is of high relevance. Discrepancies between attitudes and actual decisions may affect economic welfare[2,3]. A potential threat to welfare stems from consumers becoming increasingly aware of such discrepancies. As a consequence an erosion of trust may threaten markets for services based on the collection and dissemination of personal data. For instance, trust is likely to erode once consumers find out that provided contact information will be used for unwanted marketing phone calls or past purchase orders will serve as input for price discrimination. Accordingly, for many years research in economics, psychology, and social studies, has been addressing privacy decision making as its object of investigation. However, it occurred only recently that attempts to describe human decision making with the tools borrowed from quantum theory emerged, e.g. [4,5], thereby offering a new perspective of phenomena like the privacy paradox.

From this perspective, we provide a rational explanation of why people generously give away personal data while at the same time being highly concerned about their privacy. We argue that observations of abstract risk awareness of privacy threats and concrete privacy decisions are not interchangeable, i.e. they do not commute. Prior to that we come up with a thorough literature review on privacy decisions in socio-economic scenarios and identify explanatory gaps. The paper is structured as follows.

In the next section we review empirical studies and explanatory attempts related to the privacy paradox. Literature stems from several fields like privacy economics, cognitive psychology, and information systems, and its review is structured along three descriptive dimensions (1) incomplete information, (2) bounded rationality, (3) and decision biases. Then, in section 3, we come up with a formalization of the privacy paradox. By means of a numerical example representative for conflicting privacy observations, we show that stated preferences and actual behavior interfere, i.e. abstract risk awareness and concrete privacy decisions do not commute. Finally, in section 4, we speculate about how our results may contribute to transparency and trust on markets of recent internet services and give an outlook towards future work.

2 Explanatory Gap: The Privacy Paradox

According to Westin (1967) privacy refers to each individual's right to control, edit, manage, and delete information about them and decide when, how, and to what extent information is communicated to others[6]. There are several studies showing that individuals are quite clear about their valuation and desired level of privacy. However, when observed in practical situations people's willingness to disclose personal data stands in stark contrast to their own privacy claims.

2.1 Empirical Observations

In the US several polls and surveys support the claim that people care about their privacy[2]. Given the success of companies like Google and Facebook as well as the amount and sensitivity of data disclosed in exchange for using their services, the privacy paradox appears intuitively evident. Beyond intuition, there are quite a few behavioral studies witnessing the privacy paradox. As one of the main schools of privacy research, behavioral economics studies how individual, social, cognitive and emotional biases influence privacy decision making.

Spiekermann et al. (2001) conducted an experiment with data from 171 participants and compared their self-reported privacy preferences with actual data disclosure[7]. The authors analyzed questionnaire answers to discern privacy preferences and log files to analyze behavior and found that participants did not live up their self-reported privacy attitudes when it comes to interactions with an anthropomorphic shopping bot. Risk awareness was determined by clustering users according to their level of concern. 76% of participants care about their privacy. 30% are privacy fundamentalists, 26% profiling averse (avoidance of disclosure of hobbies, interests, health data, etc.), and 20% identity concerned (avoidance of disclosure of name, address, and email). Only 24% are marginally concerned.

Norberg et al. (2007) demonstrate the existence of the privacy paradox within two experimental studies[8]. Their hypothesis draws from individuals' consideration of risks and trust. The authors are interested in the degree to which privacy attitudes or intentions might influence actual disclosure behavior. As opposed to risks, they assume that trust directly influences privacy behavior. Risk considerations have an influence on stated preferences but influence is not strong enough to have an effect on actual behavior. As environmental factor trust has stronger effects on actual behavior and outweighs privacy concerns. In contrast, when asked about intentions to provide personal information it is the other way round and risk outweighs trust. Privacy intentions or attitudes and actual data disclosure are paradox as risk awareness dominates in abstract decision situations and reliance upon trustworthiness dominates in concrete decision making processes. In their studies the authors found support of risks significantly influencing privacy intentions. However, they didn't find trust having an effect on actual behavior as expected. Nonetheless, Dwyer et al. (2007) showed that trust and usage goals affect people's willingness to disclose personal information in online social networks[9]. They found that Facebook users expressed greater trust in Facebook than MySpace users did in MySpace. According to this higher level of trust Facebook users were more willing to disclose data on the site.

Sheehan and Hoy (1999) conducted a study to investigate linkages between E-mail users' privacy concerns and their change of behavior[10]. The authors found that with an increase in privacy concern actual behavior changed. In particular, respondents with increased privacy awareness were more likely to provide incomplete information to web sites, or to request removal from mailing lists. Although they do not claim to have found a causal relationship between stated

[2] cf. `https://www.cdt.org/privacy/guide/surveyinfo.php`

concerns and actual privacy decisions, the authors revealed a clear correlation between the two observations.

With regard to trade-offs between costs and benefits Sayre and Horne (2000) examined privacy decision making in an offline context[11]. They found that people are willing to give away their personal information in exchange for small discounts in a grocery store. Here the assumption is that consumers trade benefits (small discounts) for the costs (risks associated with personal data disclosure). A trade-off is calculated according to an individual's utility function which takes as input costs and benefits.

Awad and Krishnan (2006) deduce benefits from the degree a service is personalized and fits consumer needs[12]. In contrast, costs are driven by perceived privacy risks. Personalized product recommendations of online shops are beneficial to consumers in the sense of reduced search efforts. On the other hand, consumers often don't know about the way their data is used and protected. This lack of knowledge incurs costs due to the risks that have to be taken into account. In privacy decisions users are constantly balancing the costs and benefits of data disclosure and concealment according to their primary goal of maximizing utility.

In line with trading costs and benefits three major attempts have been put forth to explain paradoxical behavior in privacy decision making[13,14]. In the following incomplete information, bounded rationality, and decision biases such as immediate gratification affecting users' perception will be discussed with regard to their explanatory shortcomings.

2.2 Incomplete Information

According to homo oeconomicus, the prototype of an economic man, consumers maximize their utility with rational decisions based on available information. Consumers under- or overestimate the value of their privacy due to incomplete information about the costs and benefits of data disclosure. For instance, since consumers often are not even aware about their data being collected at all, they do have incomplete information about the market value of their personal data. Also users do not know about consequences of their data being used for profiling or linkage with other data sources. From the background of complete information about the value of their data (benefits) and potential risks (costs) consumers would be able to calculate the right balance between costs and benefits and maximize utility. Incomplete information prevents users from acting rationally and maximizing utility. Nevertheless, from their subjective point of view and within their limited boundaries of reasoning, data disclosure may appear rational for users themselves. From an objective third person's point of view, i.e. having complete information, privacy behavior may appear contradictory, cost-neglecting, and irrational.

Others have argued against the assumption of complete information. Acquisti and Grossklags (2009) share the view that incomplete information complicates privacy decision making[15]. Subjects have to consider multiple layers of outcomes and associated probabilities and not just deterministic outcomes. This leads to highly imprecise estimates of the likelihood and consequences of adverse

events. Eventually, privacy threats and protection modes are ignored altogether. The authors favor the view that in most privacy decision making situations it is unrealistic to assume the existence of known or unknown probabilities or subjective beliefs for probabilities over outcomes. Besides acting on incomplete information people posses no consistent preferences between alternatives, they do not chose the utility maximizing option, they do not discount future events consistently, and they do not know the probability distributions over outcomes. Instead, individuals' rationality is bounded, heuristics are applied for privacy decisions and biases affect consumers' behavior whenever they compare alternatives, perceive risks, and discount values. In contrast to risk-awareness where probabilities of possible random outcomes are objectively known, uncertain and ambiguous decision outcomes are not pre-determined and thus probabilities cannot be objectively known.

2.3 Bounded Rationality

Bounded rationality states that human decision making is bounded by nature and so decisions often result in wrong or biased conclusions[16]. Consumers under- or overestimate the risk of data disclosure. Underestimating risks due to limited cognitive abilities explains paradoxical behavior in privacy decision making. Like the possibility of having complete information, bounded rationality assumes the possibility of unbounded rationality leading to objectively right and unbiased conclusions. Privacy decisions resulting in wrong or biased conclusions are essentially irrational as outcomes are not Pareto-optimal and thus inefficient. Again, from a subjective point of view, disclosing personal data despite privacy concerns may appear quite rational to the subjects themselves. This confusion of ontological and epistemological categories, i.e. subjective and objective rationality, however, is problematic. There are no truly rational decisions based on all facts for or against all possible courses of action. Cumulative aggregations of facts about the world, by themselves, are meaningless[17]. To capture significance or involvement, they must be assigned relevance. However, such an assignment of relevance just adds more meaningless facts, a problem that very quickly leads to infinite regress. Facts are essentially meaningless because they are indeterminate up to the point in time an actual decision is made. Nevertheless, uncertain and ambiguous outcomes may have an effect on privacy decision making. As put forth by Tversky and Kahnemann (1981), the way a problem or question is framed affects how subjects respond[18]. For instance, Acquisti and Grossklags (2005) showed impacts on willingness to accept or reject a privacy-related offer when consequences of the offer are re-framed in uncertain or ambiguous terms[19].

2.4 Decision Biases

Other attempts to explain the privacy paradox refer to decision biases. For instance, the time frame costs and benefits are perceived lead to decision biases. In observations of hyperbolic discounting subjects prefer rewards that arrive sooner[20], e.g. benefits derived from using a search engine, compared to

long-term risks such as potential data breaches. Such immediate gratification is stronger than future privacy concerns. For instance, the chance to socialize with peer group members immediately beyond restrictions of analogous communication overweighs potential privacy threats.

Besides biases related to time frames the tangibility of decision factors plays a role in privacy decision making. Privacy, i.e. the right to informational self-determination, is less tangible than risks associated with physical harm such as becoming ill or having an accident. Acquisti (2004) presents a model on privacy behavior grounded in the tendency to trade-off privacy costs and benefits in a way that may be inconsistent with privacy intentions leading to damages in the future[21]. Users draw less attention to privacy risks which require their active intervention, or prevention, than to risks they are exposed to more passively but which they can imagine more illustratively.

In [15] several other biases are suggested to drive privacy decision making. For instance, the valence effect refers to the tendency to overestimate the likelihood of favorable events. People tend to think privacy harms to other users is more likely than to themselves. Rational ignorance is another effect that occurs when costs of learning are higher than potential benefits gained from a decision. For example, consumers may consider costs for reading privacy policies too high compared to the expected benefit of using a service.

As technical mean to influence biases in privacy decision making privacy statements are meant to foster consumers to act in accordance with their privacy preferences. However, studies show that simply stating privacy guidelines does not avoid the privacy paradox[22]. To reduce discrepancies between stated preferences and actual behavior privacy statements do not have an impact on most users' behavior. Rather simplified social interaction appears to influence privacy decision biases. Drawing from[7] Berendt et al. (2005) argue that simplifying communication plays a role for opinion change in privacy decision making. They refer to ELIZA, an electronic psychotherapist developed by Joseph Weizenbaum in the 1960s, who, in the course of interaction, became a trusted interaction partner. This appears to be in accordance with one of the basic drivers in human communication and language acquisition, i.e. cooperative behavior in terms of sharing attitudes and informing others helpfully[23].

From a sociological point of view, peer group pressure plays an important role in privacy decision making. People disclose information to conform and in conforming they pose threats to their privacy. Opting out becomes hardly possible if exclusion from the group is undesirable. For instance, members of social groups using social networks as their primary communication medium put pressure on their peer group members to do likewise, i.e. share information and conform to social norms. Peer group members not conforming to communication and information sharing rituals are sanctioned with attention deprivation and exclusion from the social group. Opting out and privacy protection becomes increasingly difficult the more group members agree on information sharing as a basic principle constituting their affiliation. Social desirability biases may contaminate

intentions to disclose personal information in such a way that stated preferences are not predictive for actual disclosure behavior anymore[24].

In summary, there are several fruitful attempts to explain the privacy paradox. Incomplete information measures privacy decision outcomes from the background of complete knowledge of all relevant facts. Bounded rationality measures decision outcomes from the background of decisions made without cognitive limitations. Eventually, decision biases consider social, cognitive and emotional factors influencing privacy decision making. Several explanatory gaps can be derived from the forgoing discussion.

Explanatory attempts discussed so far consider uncertainty to be inherent in privacy decision making. However, preferences guiding privacy decisions often are not merely revealed but realized only when the decision is made. In such cases uncertainty is not due to lack of information where costs and benefits are assumed to be out there readily determined though not yet known. Rather uncertain events are indeterminate[25]. Thus distinctions between complete and incomplete information as well as bounded and unbounded rationality become obsolete. Privacy decisions based on preferences which are not due to lack of information and cognitive limitations are inherently context-dependent. Explanatory attempts taking decision biases into account point to the right direction by explaining paradoxical behavior with dependence upon contextual factors. The disparity between stated preferences and actual behavior is not a contradiction but depends on the psychological and sociological context. Thus from the background of a high valuation of privacy personal data disclosure is not necessarily irrational. In the next section, we describe stated preferences and actual behavior as two non-commuting observations of incompatible preferences (types).

3 Indeterminacy and Noncommutativity

More recently several attempts to describe human decision making with the tools borrowed from quantum theory emerged[4,5] thereby offering a new perspective of phenomena like the privacy paradox. This new perspective allows incorporating effects like indeterminacy, i.e. the outcome of a decision making process is determined at the time the decision is made but not prior to it, and noncommutativity, i.e. two decisions A and B are not interchangeable, in descriptions of privacy decision making. These effects are common in daily situations[26] but hardly considered in behavioral studies of privacy. To our best knowledge quantum effects haven't been considered in a privacy context yet.

In the context of information technology, the quantum formalism has been applied for several descriptions of indeterminate and contextual phenomena. Bruza et al. (2008) entangles words and their meanings[27]. In their work they show that in certain contextual situations, the semantics of words represented as vectors combine in a way that instances of combined words are neither typical for one nor the other constituent. Piworawski and Lalmas (2009) come up with a vector model for information retrieval based on quantum interaction[28]. Flender

et al. (2009) applies quantum effects to data and process models and describes how part-whole relationships and view updates appear under a new light[29,30]. One of the earliest approaches to a generalization of quantum effects is the model of a State-Context-Property (SCoP)-System and can be found in Aerts and Gabora (2005)[31,32].

With their contribution to behavioral economics, Lambert-Mogiliansky et al. (2009) present an approach to modeling decision situations in which preferences (types) of agents emerge indeterminately as the outcome of an interaction process between agent and environment[25]. According to quantum theory, decision situations are modeled as observables, i.e. linear operators. The decision making itself is analogous to the measurement process in quantum experiments. It projects the initial state of an agent into the subspace of the preference space associated with the eigenvalue corresponding with the choice made, i.e. the type or preference is not revealed as it wasn't determined prior to the choice; rather it is constructed with the choice made. The authors come up with an example from cognitive psychology showing that cognitive dissonant behavior can be modeled in terms of type indeterminacy. Their example draws from a study about workers in risky industries neglecting safety regulations. Before starting a risky job, however, workers were reasonably averse to risk. In cognitive psychology, this phenomenon is called cognitive dissonance[33]. People modify their types or preferences in response to discomfort arising from conflicting preferences, e.g. not using safety tools despite high risk awareness. Both decision situations can be modeled as observables with eigenvalues of two choices. Job seekers are either adventurous (1) or habit prone (2) whereas workers are either risk-averse (1) or risk-loving (2) when it comes to applying safety measures at work. Lambert-Mogiliansky et al. (2009) showed that both decision situations do not commute and thus preferences are incompatible.

In the following we consider the privacy paradox in a similar fashion. For a complete description of the privacy paradox stated preferences and actual behavior are necessary but mutually exclusive observations. Privacy behavior is not irrational due to incomplete information about risks or limited cognitive capacity. The disparity between the two decisions comes from the fact that subjects are not in the same state. Like in the job seeking example, the situation where consumers make a decision about their valuation of privacy is represented by an operator that does not commute with the operator representing the situation where consumers actually disclose or conceal data.

Two decision situations involving a sequence of two non-commuting privacy decisions are given. For each decision there are two choices. For an observable X there is a decision about privacy valuation to be made. Choice x_1 stands for a high valuation, choice x_2 refers to a low valuation. Another observable refers to Y. Here subjects disclose personal data with choice y_1, or they conceal personal data with choice y_2.

In a first scenario users are confronted with decision situation Y. Either they disclose data (y_1) or they refrain from disclosure (y_2). The initial state of the user X is written in terms of a linear superposition of two eigenvectors representing

choices. Superposition states afford to get actualized in relation to a specific context, or observation.

$$|\psi\rangle = a_1|x_1\rangle + a_2|x_2\rangle \tag{1}$$

where $a_1^2 + a_2^2 = 1$. The vectors can be written in terms of eigenvectors of Y.

$$|x_1\rangle = b_{11}|y_1\rangle + b_{12}|y_2\rangle \tag{2}$$

$$|x_2\rangle = b_{21}|y_1\rangle + b_{22}|y_2\rangle \tag{3}$$

The superposition state $|\psi\rangle$ is now written in terms of of eigenvectors of Y.

$$|\psi\rangle = (a_1 b_{11} + a_2 b_{21})|y_1\rangle + (a_1 b_{12} + a_2 b_{22})|y_2\rangle \tag{4}$$

The probability that a subject discloses personal data is expressed as follows.

$$\begin{aligned}\mathbf{Pr}_Y(y_1) = \langle y_1|\psi\rangle^2 &= (a_1 b_{11} + a_2 b_{21})^2 \\ &= a_1^2 b_{11}^2 + a_2^2 b_{21}^2 + 2a_1 a_2 b_{11} b_{21}\end{aligned} \tag{5}$$

In a second scenario users first value their privacy (X), then they decide if they disclose personal data (Y).

$$\begin{aligned}\mathbf{Pr}_{YX}(y_1) = \mathbf{Pr}_X(x_1)\mathbf{Pr}_Y(y_1|x_1) + \mathbf{Pr}_X(x_2)\mathbf{Pr}_Y(y_1|x_2) \\ = a_1^2 b_{11}^2 + a_2^2 b_{21}^2\end{aligned} \tag{6}$$

Now we can give a formal representation of the privacy paradox.

$$\mathbf{Pr}_{YX}(y_1) < \mathbf{Pr}_Y(y_1) \tag{7}$$

The privacy paradox occurs in case of a positive interference between both decision situations, i.e. $2a_1 a_2 b_{11} b_{21} > 0$. In quantum physics, the interference effect occurs due to matter and energy both exhibiting wave-like and particle-like properties but not both at the same time, i.e., not within the same context. In different contexts or experimental arrangements some matter seems more particle-like than wave-like. With reduced values of energy (change of context) the same matter will be more likely to show wave-like qualities than particle-like properties. All the information about a particle is encoded in its wave function, which is analogous to the amplitude of a wave at each point in space. This function evolves according to a differential equation (the Schrödinger equation) and so gives rise to interference. Interference occurs when the interaction of two or more waves, e.g., one wave representing observer and the other one standing for the observed system, influences their direction of propagation characterized by crests and troughs. When two or more waves reach the same point in space at the same time, they either add up (the crests arrive together which is called in-phase) or cancel each other out (the crest from one wave meets a trough from another wave which is called out-of-phase). The state of a wave-like property is called superposition or potentiality state and represented as a vector $|\psi\rangle$. Its linear combination, the superposition or addition of two or more states, resembles an interference pattern typical of waves.

We assume data is disclosed $|\psi\rangle = |y_1\rangle$. Moreover, we assume that most users disclose personal data while at the same time being highly concerned about their privacy. This assumption is reasonable as empirical studies witness generous data disclosure despite high risk awareness (cf. section 2). Let $\mathbf{Pr}(x_1|\psi) = 0.8$ and $\mathbf{Pr}(x_2|\psi) = 0.2$. Accordingly, $|a_1| = \sqrt{0.8}$ and $|a_2| = \sqrt{0.2}$ and likewise $|b_{11}| = \sqrt{0.8}$ and $|b_{21}| = \sqrt{0.2}$.

In order to get the probability of y_1 in Y we use (5).

$$\begin{aligned} 1 = \langle y_1|\psi\rangle^2 &= a_1^2 b_{11}^2 + a_2^2 b_{21}^2 + 2a_1 a_2 b_{11} b_{21} \\ &= 0.64 + 0.04 + 2a_1 a_2 b_{11} b_{21} \\ &= 0.68 + 2a_1 a_2 b_{11} b_{21} \end{aligned} \tag{8}$$

(8) implies that the interference effect is positive and equals $1 - 0.68 = 0.32$. In context X the probability for disclosing data is given by (6). It is the same sum as in (5), but without the interference term.

$$\mathbf{Pr}_{YX}(y_1) = 0.68 \tag{9}$$

The privacy paradox occurs due to $\mathbf{Pr}_Y(y_1) > \mathbf{Pr}_{YX}(y_1)$. The choices between low/high privacy valuation and data disclosure/concealment are observations of two incompatible types (or preferences) represented by two noncommuting observables. Privacy valuation refers to an abstract perception of risk. The decision to disclose data refers to a motivational perception of concrete benefits. The two modes are incompatible, the subject is cognitively dissonant.

4 Transparency and Trust

Our economy increasingly relies on personal data. Many service providers offer their services for free and collect personal data in exchange. At the same time consumers become increasingly transparent with regard to their preferences and this raises concerns over the erosion of their privacy. Moreover, the disparity between stated preferences and actual behavior, i.e. the privacy paradox, may not only turn out to be disadvantageous for consumers. Also for service providers this may have negative consequences. Consumers confronted with their paradoxical behavior, e.g. when finding out about their personal data being used without consent, may react with resentment, which may cause damage to customer relationships[1].

From an economic point of view, the challenge is to find the right balance of measures to ensure trusted relationships between market participants. There are several options to handle privacy. Ensuring privacy through law usually lacks behind and privacy-enhancing technology is hardly accepted. Policy makers suggest providing more information about possible privacy threats will help them to make better decisions. Such information may be provided by companies, peers, or consumer advocacy groups. However, it is questionable that even with complete transparency and unbounded rationality individuals would act consistently.

As proposed here abstract risk awareness of privacy threats and concrete privacy decisions are not interchangeable, i.e. disclosing personal data prior to becoming aware of privacy risks does not equal the raising of risk awareness before revealing personal information. Privacy decisions do not commute as subjects may alter their preferences indeterminately, i.e. at the time an actual decision is made. Signaling consumers that there is uncertainty in their privacy decisions which is not due to lack of information but indeterminacy may prevent them from reacting with resentment once they find out about the state of their privacy.

In the near future we will look at transparency mechanisms bearing the potential to reduce the disparity between stated preferences and actual behavior. Privacy statements were not found to be effective[22]. They rather suggest an information surfeit.

References

1. Adams, A.: The Implications of Users' Multimedia Privacy Perceptions on Communication and Information Privacy Policies. In: Proceedings of Telecommunications Policy Research Conference (1999)
2. Akerlof, G., Dickens, W.: The Economic Consequences of Cognitive Dissonance. The American Economic Review 72, 307–319 (1982)
3. Müller, G., Flender, C., Peters, M.: Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung. In: Internet Privacy - Eine multidisziplinäre Bestandsaufnahme - A Multidisciplinary Analysis, pp. 143–189. Springer (2012)
4. Busemeyer, J., Wang, Z., Townsend, J.: Quantum Dynamics of Human Decision Making. Journal of Mathematical Psychology 50, 220–241 (2006)
5. Busemeyer, J.R., Lambert-Mogiliansky, A.: An Exploration of Type Indeterminacy in Strategic Decision-Making. In: Bruza, P., Sofge, D., Lawless, W., van Rijsbergen, K., Klusch, M. (eds.) QI 2009. LNCS, vol. 5494, pp. 113–127. Springer, Heidelberg (2009)
6. Westin, A.: Privacy and Freedom. Atheneum, New York (1967)
7. Spiekermann, S., Grossklags, J., Berendt, B.: E-Privacy in 2nd Generation E-Commerce: Privacy Preferences vs. Actual Behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce, pp. 38–47. ACM (2001)
8. Norberg, P., Horne, D., Horne, D.: The Privacy Paradox: Personal Information Disclosure Intentions vs. Behaviors. Journal of Consumer Affairs 41, 100–126 (2007)
9. Dwyer, C., Hiltz, S., Passerini, K.: Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. In: Proceedings of AMCIS 2007 (2007)
10. Sheehan, K., Hoy, M.: Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. Journal of Advertising, 37–51 (1999)
11. Sayre, S., Horne, D.: Trading Secrets for Savings: How Concerned are Consumers About Club Cards as a Privacy Threat? Advances in Consumer Research 27, 151–155 (2000)
12. Awad, N., Krishnan, M.: The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. MIS Quarterly, 13–28 (2006)
13. Acquisti, A., Grossklags, J.: Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy 3, 26–33 (2005)

14. Deuker, A.: Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services. In: Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G. (eds.) IFIP AICT 320. IFIP AICT, vol. 320, pp. 275–283. Springer, Heidelberg (2010)
15. Acquisti, A., Grossklags, J.: What Can Behavioral Economics Teach Us About Privacy? Digital Privacy: Theory, Technologies and Practices, 363–380 (2009)
16. Simon, H.: Models of Bounded Rationality: Empirically Grounded Economic Reason. The MIT Press (1997)
17. Dreyfus, H.L.: What Computers Still Can't Do: A Critique of Artificial Reason. MIT Press (1992)
18. Tversky, A., Kahneman, D.: The Framing of Decisions and the Psychology of Choice. Science 211, 453–458 (1981)
19. Acquisti, A., Grossklags, J.: Uncertainty, Ambiguity and Privacy. In: Fourth Annual Workshop Economics and Information Security (WEIS 2005), MA, pp. 2–3 (2005)
20. Acquisti, A., Grossklags, J.: Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. In: 2nd Annual Workshop on Economics and Information Security - WEIS, vol. 3 (2003)
21. Acquisti, A.: Privacy in Electronic Commerce and the Economics of Immediate Gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce, pp. 21–29. ACM (2004)
22. Berendt, B., Günther, O., Spiekermann, S.: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. Communications of the ACM 48, 101–106 (2005)
23. Tomasello, M.: Origins of Human Communication. The MIT Press (2008)
24. Milne, G.: Consumer Participation in Mailing Lists: A Field Experiment. Journal of Public Policy & Marketing, 298–309 (1997)
25. Lambert Mogiliansky, A., Zamir, S., Zwirn, H.: Type Indeterminacy: A Model of the KT (Kahneman-Tversky)-Man. Journal of Mathematical Psychology 53, 349–361 (2009)
26. Atmanspacher, H.: Quantenphysik und Quantenalltag. In: Die Welt im Bild: Weltentwürfe in Kunst, Literatur und Wissenschaft seit der Frühen Neuzeit, pp. 293–305. Fink, Paderborn (2010)
27. Bruza, P., Kitto, K., Nelson, D., McEvoy, K.: Entangling Words and Meaning. In: Proceedings of QI 2008. University of Oxford (2008)
28. Piwowarski, B., Lalmas, M.: Structured Information Retrieval and Quantum Theory. In: Bruza, P., Sofge, D., Lawless, W., van Rijsbergen, K., Klusch, M. (eds.) QI 2009. LNCS, vol. 5494, pp. 289–298. Springer, Heidelberg (2009)
29. Flender, C., Kitto, K., Bruza, P.: Beyond Ontology in Information Systems. In: Bruza, P., Sofge, D., Lawless, W., van Rijsbergen, K., Klusch, M. (eds.) QI 2009. LNCS, vol. 5494, pp. 276–288. Springer, Heidelberg (2009)
30. Flender, C.: A Quantum Interpretation of the View-update Problem. In: Proceedings of the 21st Australasian Conference on Database Technologies, vol. 104, pp. 67–74 (2010)
31. Aerts, D., Gabora, L.: A State-Context-Property Model of Concepts and their Combinations I: The Structure of the Sets of Contexts and Properties. Kybernetes 34(1&2), 167–191 (2005)
32. Aerts, D., Gabora, L.: A State-Context-Property Model of Concepts and their Combinations II: A Hilbert Space Representation. Kybernetes 34(1&2), 192–221 (2005)
33. Festinger, L.: A Theory of Cognitive Dissonance. Stanford University Press (1957)