EXPERIMENTS ON PERSONAL INFORMATION DISCLOSURE: PAST AND FUTURE AVENUES

José Luis GÓMEZ-BARROSO

Dpto. Economía Aplicada e Historia Económica – UNED (Universidad Nacional de Educación a Distancia)

Pº Senda del Rey, 11. 28040 Madrid (Spain)

Tel.: +34 913988115

jlgomez@cee.uned.es

EXPERIMENTS ON PERSONAL INFORMATION DISCLOSURE: PAST AND FUTURE AVENUES

Abstract

When it comes to understanding the behavior of people when deciding whether to disclose personal information, just anecdotal evidence clearly suggests the need for experimental approaches. In spite of this, in the about fifteen years since the research on online privacy behavior emerged as a distinct field of scientific enquiry, experiments are but a few when compared to surveys and theoretical approaches, even adopting a broad definition of experiment. This article reviews all the experiments already done in the area and it also proposes a research agenda. Experimental techniques not only guide the building of descriptive theories but also serve to demonstrate or prove the adequacy of assumptions present in normative theory.

Keywords

personal information; experiment; privacy; normative theory; descriptive theory; rational behavior; inconsistent behavior; meta-analysis; methodological review

1. INTRODUCTION

The importance of personal data for online markets is beyond doubt. Services and applications become more useful and appealing through their tailoring to users' needs and preferences –i.e., through the use of personal information. Even more importantly, targeted advertising is the business model on which relies the success of many of the most successful online giants. At the end of the day, it can be said that the exploitation of personal data is what allows the existence of a *free Internet*.

A great deal of personal data is collected covertly, without consent or even knowledge of users. While we communicate, access and exchange information using electronic communications networks, data records can be –are indeed– collected on who we are, where we are, what we do, and how we do it. Often, however, data are disclosed by users of online services and applications. Actually, almost every day, users have to take decisions about whether to reveal information about themselves. To understand the rules that drive this decision is of utmost importance for companies –given the economic value of personal data–, but also for policy-makers –given the potential conflicts of data collection with privacy protection rules– and even, obviously, for the people themselves.

It is no wonder, then, that academics turned their eyes towards this phenomenon. Personal information has emerged as a distinctive field aloof from traditional privacy issues (see Gómez-Barroso, 2018). In this particular domain, disclosure has become indeed the topic that dominates the research agenda. Departing some ten years ago from the first studies of the so-called "privacy paradox" –the term that describes the apparently irrational behavior of individuals when they make determinations about their personal data–, research design has evolved towards the exploration of more and more complex models and hypotheses (Barth and de Jong, 2017).

Through all this work, something has been made clear: disclosure of personal information is a multidimensional, evolving and context-dependent notion, and no single framework will be able to catch the huge variety of situations and behaviors. In spite of this evidence, most efforts keep going on the direction of building a comprehensive model able to explain as many as possible of the motivations and concerns that guide the *consistent* behavior of people (see Li, 2012). This could be plausible as a basic common ground is always needed when starting to study an unexplored topic. However, it is clear that not all the people all the time behave consistently. While always true whatever the situation, this is particularly critical when talking about disclosure of personal information. This clearly makes the topic a matter for experimental research, as the study of any *inconsistent* behavior is closely linked to the conduction of experiments. The necessity for experimental research to advance our understanding of consistent behavior does not seem at first sight so obvious. However, experiments could be, and have been indeed, a strong driver for the building of normative theories.

Against this background, there is wide room to experimentally explore individual's behavior as, up to now, the number or scientific papers published in the area is small and do not show any recent significant increase. This is evidenced in this article, which conducts a review of the literature on experiments –taking the term in a fairly broad sense– investigating the behavior of people when disclosing personal information. It analyzes and systematizes all these works, revealing the paths that researchers have walked until the present. It then proposes a research agenda that can guide future studies in the area. These are the two largest sections of the article. They are preceded by a theoretical framework that considers the disclosure of personal data as a decision-making process. The conclusions close the article.

2. THE DISCLOSURE OF PERSONAL INFORMATION AS A DECISION-MAKING PROCESS

On an almost daily basis, people have to choose whether to fulfill the information required by the webpage that is given them access to a free download, whether to accept the request of sharing

the location made by an online retailer, whether to log in when visiting a favorite site, whether to post about their lives. Most people know –at least vaguely– that unintended consequences can derive from those actions. Understand why finally they do this or that –or do not– fits perfectly with the subject that the decision theory posits: the analysis of the behavior of an individual in the presence of options when the consequences resulting from this choice are imperfectly known.

Normative –or prescriptive– decision theories are the first that come to assist in understanding personal data revelation. They study how decisions should be made in order to be considered as *rational*. Rational decision-making implies maximizing expected utility. Subjective utilities are commonly used: when we make decisions, or choose between alternatives, we try to obtain as good an outcome as possible, according to some standard of what is good or bad *for us*. Motivations for disclosing personal information are varied but data holders are always supposed to obtain a *net* benefit when disclosing (Gómez-Barroso et al., 2018). This benefit is many times linked to social or psychological rewards. Social network sites are a prime example of it. Consumers also receive a benefit in the form of better services when they disclose their data. The privacy calculus theory –disclosure of information is derived from a calculation in which alternative options are assessed considering possible outcomes– is a direct adaptation of this cost-benefit (risk-benefit) analysis (Li et al., 2010; Wang et al., 2016).

However simple this rule for action may seem, it is clear that it is not. Estimates of objective probabilities –needed to reasonably calculate expectation values– face incomplete and asymmetric information. More important, the process of decision does not take place in a vacuum. Preferences, beliefs, personality traits, attitudes, abilities, "social contracts" and norms influence a person's values –i.e., subjective utilities– and cognitive processes, and therefore the corresponding behaviors. To take account of these additional constraints or conditions when people decide whether to disclose personal data, a number of theories have been *borrowed* from psychology, political science, sociology or economics. Li (2012) already identified nothing less than fifteen theories that have been used to address the issue of privacy-driven behavior –at an individual level– from different perspectives with varied emphases.

Most of these theories share the goal of comprehensively understand privacy behavior, and, consequently, personal data disclosure. All of them try to uncover the keys for a rational, let's better call it *consistent*, behavior. Indeed, through the addition of explanatory factors and the use of more complex theories, online users, whose behavior was once considered irrational, are *coming to their senses*. It should be recalled that the earlier studies soon revealed an apparently irrational behavior of individuals when they make determinations about their personal data: while they are worried about privacy, their actions do not mirror that concern. However, as the so-called "privacy paradox" has been studied in a greater depth, it has gained nuances and complexities. Some of the most recent studies *unravel* the privacy paradox (Aguirre et al., 2015), *unpick* it

(Zafeiropoulou et al., 2013), consider that it *would disappear when analyzed in a new approach* (Dienlin and Trepte, 2015), or directly *solve* it (Baek, 2014). Many others directly try to explain users' behavior without even talking of a paradox (among many others, Knijnenburg et al., 2013; Taddei and Contena, 2013). All the theoretical supports used in these works are –or function as– normative theories as they aim to explain how people *ought* to behave considering a number of conditions or constraints.

However, most people –at least sometimes– do not behave as they ought. In other words, they violate the basic axioms of rationality/consistency in their actual disclosing of information. Normative theories assume three fundamental unrealistic traits: unbounded rationality, unbounded willpower, unbounded selfishness (Jolls et al., 1998). These first two traits are good candidates for modification in the case of disclosure of personal information: bounded rationality derives from the fact that the thoroughness of the analysis is constrained by limited cognitive abilities; bounded willpower comes out in situations where people, for self-control reasons, fail to make the choice they know is best. In those cases, descriptive –positive– theories, which study how decisions are actually made, seem to be the only help. Descriptive theories can indeed be put up as bounded rationality is not the same thing as optimizing under additional constraints but is not irrationality either. There is an *irrational logic* behind particular disclosure decisions –which is what makes them worth of study; nothing could be learned from purely hazardous actions. The need of accepting limits and making simplifying assumptions can even be derived after a process in which users make conscious efforts to take decisions according to a formally rational process.

The study of inconsistent behavior when disclosing personal data has not kept pace with the study of normative behavior, even if Acquisti and Grossklags (2008) already alerted on the fact that "*individuals' privacy relevant behavior may be best understood in terms of bounded rationality, and behavioral biases*". While Kokolakis (2017) cites about 50 references –excluding articles on ethical and legal aspects– in his literature review of the privacy paradox, there is just a handful of articles intended to describe positive theories of how people behave in particular settings. The alternative review presented by Barth and de Jong (2017) seems to qualify this statement but, as they acknowledge, "*attitude and intention are not actual behavior and actual behavior is seldom measured in the studies*". Their conclusion indeed does no more than support the basic principle –no single framework will be able to catch the huge variety of context-dependent behaviors. Consequently, there is ample room for theories that complement –rather than qualify or replace– general normative models.

3. THE EXPERIMENTAL STUDY OF DISCLOSURE DECISIONS

A descriptive theory starts with observations of how people choose in specific situations and attempts to describe their behavior as systematically as possible. Thus, a descriptive theory is primarily inductive (Rapoport, 1989). In practice, the merits of descriptive theories are to a great extent evaluated in accordance with their goodness of fit to the behavioral patterns found in experiments conducted either in the laboratory or in the field –which means real-settings. Therefore, this approach draws mainly on insights and methods from experimental economics and social and cognitive psychology.

Conversely, experimental techniques not only guide the building of descriptive theories but also serve to demonstrate or prove the adequacy of assumptions present in normative theory. This has been the case for personal data revelation experiments. Virtually all experiments conducted in the area aim for assessing the impact of factors characterizing rational behavior as the following review of literature makes it clear.

This review includes all kind of experiments: field experiments or controlled (laboratory) experiments, either conducted online or face-to-face; economic (rewarding participants and no deception) or psychological experiments. The very concept of experiment is not narrowly defined, rather the contrary. Works that employ survey-like methodologies in which participants take hypothetical choices are here considered. Preibusch (2015) states that the problems present in surveys about privacy also apply to these works, "erroneously labelled as experiments".

For the sake of clarity –though admitting the fact that not every article may perfectly fit into a given category–, the works found in the literature review are sorted along five dimensions of research:

- Experiments on the existence of the privacy paradox itself.
- Experiments on the importance of trust and (perceived) control as mediators of self-disclosure.
- Experiments on the impact of incentives (either monetary or in the form of customized products).
- Experiments on the willingness to pay for privacy protection.
- Experiments on *nonrational* behavior.

Table 1 provides an overview of the classification set out that can help to understand it.

3.1. Experiments on the existence of a privacy paradox

Indirectly, a great number of the collected experiments deal with the so-called privacy paradox. In particular, many of them try to clarify the role of particular variables within an explanatory theoretical model. Two papers, however, asked about the existence of the paradox itself. Not surprisingly, one of them is the oldest article identified in the literature review.

- Spiekermann et al. (2001) confirmed the privacy paradox: in spite of their explicit privacy concerns, the majority of participants in their experiment did not live up to their self-declared preferences.

  After having filled out a questionnaire, 171 students were given the opportunity to shop online for digital cameras or winter jackets. In the process, they interacted with an "anthropomorphic 3-D shopping bot that assisted participants", who introduced personal questions in a dialogue around product features and usage.

- Norberg et al. (2007) reported the results of two studies showing the existence of the paradox, i.e. people said one thing (intended to control revelation) and then acted differently when engaged in marketing exchanges (actually provided personal particulars).

  Firstly, participants were asked their intentions to disclose particular pieces of personal information. Several weeks later, these subjects were then asked to pass those same pieces of personal data to a team member who supposedly represented a commercial company (either a bank or a pharmaceutical company). Samples of 23 and 83 students participated in the two experiments.

3.2. Experiments on trust and control

Trust is one the primary factors considered in every theory describing the rational behavior of online users, in particular when making their mind up about whether to disclose personal information. The mediating role of trust is simply assumed and just one experiment investigates its true function on behavior (and curiously enough, not finding the anticipated link).

- Norberg et al. (2007), described above, suggested that personal considerations of trust and risk help explain the privacy paradox. However, they could not conclude that trust has a relevant impact on individuals' *actual* personal data disclosure. Trust was measured using a three-item scale of how trustworthy, honest, and sincere subjects perceived the business.

Most experiments focus not on trust itself but on its antecedents. In order to make a rational decision on whether to trust or not a particular website, people are prone to rely on environmental cues such as brand name, look of the website, the advice of people close to them, and third-party

privacy certifications; however, the online privacy statement is frequently the primary and sometimes the only source of information. The effectiveness of certifications and in particular of privacy policies has been profusely (considering the size of the whole corpus) studied:

- Spiekermann et al. (2001), cited before, found that two different privacy statements – participants were told either that navigational data would be handed on to a renowned European company, or that their data would be transferred to an unspecified entity without knowing what further use would be made of them– had no influence on the amount of information revealed.

- Andrade et al. (2002) concluded that the completeness of the privacy policy and the reputation of the company decrease the concern of consumers over self-disclosure.

  114 undergraduate students filled in a questionnaire after having being presented with a website homepage containing the website's privacy statement. Privacy policy (extensive vs. brief) and company reputation (high vs. low) were manipulated, as it also was (see below in the incentives section) the offer of a reward.

- Miyazaki and Krishnamurthy (2002) showed that the mere display of an Internet-seal-of-approval logotype improves user perceptions regarding privacy statement and increases anticipated disclosure rates (particularly for *high risk* consumers).

  They conducted two experiments in which different homepages and website privacy statements were administered on paper to 204/35 subjects who were enrolled in academic programs for full-time workers. The first experiment utilized six actual website privacy policies with the seals of approval manipulated, while the second experiment examined the presence or lack of the seal logotype.

- Liu et al. (2004) found that a reasonable assurance of privacy protection (privacy policies or similar procedures adhering to basic privacy principles) has a significant effect on whether an individual trusts an e-commerce website.

  A fictitious e-commerce bookstore was developed for the study. In the group receiving the "high privacy" treatment, the four privacy principles proposed by the FTC (i.e., providing people notice that personal data will be collected prior to the actual collection; providing access to the data; providing people with a choice to allow the company to use or share the data; providing reasonable assurance that data are kept secure) were included. A second version of the site did not include any of those principles. A total of 212 undergraduate and graduate students participated in the experiment.

- Jensen et al. (2005) concluded that most significant variables affecting the online behavior are trust signs present on webpages and the presence of a privacy policy, "*though users seldom consulted the policy when one existed*".

  The experiment was conducted online; participants were recruited through advertisements posted on academic websites and sent to mailing lists. Eight pairs of mock e-commerce webpages were presented to each participant. They had to select which of the two sites they would prefer to buy from.

- Xie et al. (2006) showed that privacy notices are instrumental to the request of information, in spite of the sensitivity of the solicited information. They also found a strong relationship between reputation of the company and accurate disclosure of personal information by individuals.

  Eight treatment combinations were created combining the presence of a privacy notice (including a third-party authentication of the privacy statement by TRUSTe), the use of cues to foster reputation, and a reward (a $20 gift voucher for participants who agreed to share accurate information) on the website of an online store. The 147 subjects who took part in the experiment were drawn from a professional customer database.

- Gideon et al. (2006) concluded from their experiment that when privacy policies can be easily compared, people may be willing to seek out the most privacy friendly website. This had a more noteworthy effect for purchases of privacy-sensitive items.

  Authors used a "privacy-enhanced search engine" that displayed search results annotated with information about the privacy policy of the site. Some of the 24 students that participated in the experiment were instructed to first purchase one non-privacy-sensitive product (a surge protector) and then a more sensitive product (a box of condoms) using it, while the control group was asked to make identical purchases using a standard search engine (same results were provided but without displaying any privacy information).

- Pan and Zinkhan (2006) found that the existence of a privacy policy can build shopper's trust in the store. Additionally, they concluded that the exact wording of the privacy statement does not have any significant effect.

  In a first experiment, two versions of a shop website –being the privacy statement absent or very noticeable– were presented to 60 students who had to envision themselves purchasing a gift for a friend. In a second experiment, the number of versions was three, splitting the first treatment (presence of a privacy policy) into two –short and straightforward versus long and legalistic statements.

- Arcand et al. (2007)'s findings showed that perceived control is positively influenced by the mere presence of a privacy policy. Yet reading it does not necessarily produce a significant effect neither on perceived control nor on trust. Having said that, the effect is higher when the privacy statement is presented in an opt-in format.

  In a first experiment, 219 participants (registered in a consumer database) visited a fake travel agency website displaying a privacy statement whose reading was optional. In a second study, 209 subjects visited one of the three built for the experiment versions of an existing music website. These three versions were identical except for the presence and format of the privacy statement (no privacy statement, opt-in format, opt-out format).

- Hui et al. (2007) concluded that the mere existence of a privacy statement induced more subjects to pass personal information. This was not the case for a privacy seal.

  109 undergraduate students were invited to participate in a consumer survey into mobile devices that required disclosure of personal particulars. In different treatments, the number of required data items and the assurance of privacy protection –through a statement with or without seal– were manipulated.

- Joinson et al. (2010) found that only the combination of a weak privacy policy with low trust (a consequence of manipulating cues) was able to substantially reduce the disclosure of personal data. When a weak policy was combined with high trust, or low trust with a strong policy, there was no confirmation that self-disclosure was impacted.

  The participants in their experiment were 181 Internet users recruited via advertisements on websites seeking volunteers for surveys. The first page of a web survey on "life experiences and season of birth" showed either a strong or a weak privacy policy. The survey was hosted on an educational domain in the high trust condition, whereas in the low trust condition it was hosted on a domain designed to create doubts about its trustworthiness.

- Tsai et al. (2011) repeated the experiment of Gideon et al. (2006). Indeed, they are the same authors, just replacing a member of the research team. They again concluded that when information about privacy is made more noticeable and accessible, consumers are likely to purchase from those stores who are supposed to better protect their privacy.

  More than 200 participants were recruited with flyers posted around town and online. On that occasion, the products selected for the experiment were a pack of batteries and a sex toy.

- Malaga (2014) tried to gauge the effectiveness of strong and weak privacy policies. However, based on the data gathered in his experiment, the goal changed to understanding why website visitors almost never click on privacy policies.

  The author created a real website that offered car insurance and then contracted with a company that would pay for each forwarded auto insurance. The site was setup with the typical privacy policy link at the bottom of the page. Two different privacy policies ("highly restrictive" / "no protection") were used. In total 2,313 unique visitors accessed the site. Out of those visitors 269 completed the form and clicked on the submit button; only 7 visitors clicked on the privacy policy link.

- Capistrano and Chen (2015) assessed the perceived importance and relevance of privacy policies. While not clearly defined, the term importance seems to be linked to the existence (reading by users) of the policy, and the term relevance to its appropriateness (understanding by users). They concluded that relevance is affected by the length of the policy, while visibility and specificity of the policy affects both its importance and relevance. Additionally, there is an interaction effect of information sensitivity on the policy's visibility towards perceptions on the importance of having a privacy policy.

  300 students visited a fake website offering electronic gadgets such as laptops and mobile phones. They were asked either low or high sensitive information. Participants were then instructed to read through the website's privacy statement. Length, visibility and specificity (common terms vs. ambiguous, technical, and legalese terms) of the policy were manipulated.

- Steinfeld (2016) showed that subjects are likely to read privacy policies, even rather carefully, when those are presented by default. On the contrary, most people avoid the reading of the policy when they are given this option. It is remarkable that those who, in this second condition, chose to read the privacy statement spent considerably less time on the reading than those who, in the first condition, were "obliged" to read it.

  Eye tracking methodology was used in a experiment for which 128 undergraduate students were recruited. The default group was presented with the privacy policy by default, followed by the sentence: "I have read and agree to the terms of service" and an unmarked checkbox; the non-default group saw the same unmarked checkbox and sentence, but the reading of the privacy statement was optional.

- Martin (2016) found that consumers rely mainly upon informal privacy norms instead of upon privacy notices. According to her results, the privacy notice is a loud signal to consumers about the trustworthiness of the website; indeed, invoking formal contracts about privacy makes respondents trust websites less. Conversely, violating informal

privacy norms negatively impacts trust in the website even when the information exchange conformed to –or was not mentioned in– the privacy notice.

A factorial vignette survey was conducted. Each respondent was presented with a set of vignettes and then asked to evaluate each hypothetical situation. Vignettes varied based on the website purpose (banking, photo sharing, search, travel), the type of information tracked or received by the website, the use made of the data (tailoring of services, offering of discounts, placement of advertisements, as well as a possible secondary use of data), and the length of time the data is stored. Approximately 400 respondents recruited via Amazon Mechanical Turk each rated 40 vignettes.

- Rodríguez-Priego et al. (2016) studied whether what they called *nudges*, i.e. changes to the online environment, can cause modifications in privacy behavior. Nudges did not alter the amount of personal data revealed, but had an influence in the fact that participants took notice of the privacy link.

  The experiment was conducted with the participation of 3229 subjects recruited from different sources in four European countries. A supposedly new search engine was evaluated by participants. Nudges were implemented as changes in the features of the mock search engine (e.g. inclusion of an anthropomorphic character, showing of the user's IP address, highlighting of the previous browsing activity, or changes in the look-and-feel to increase informality).

- Strahilevitz and Kugler (2016) found ineffective the explicitness of privacy policies: in spite of the fact that many participants read closely the excerpts of the privacy policy to which they were presented, subjects who read an explicit policy language and those who read an ambiguous/imprecise language did not differ in their judgment of what their assent would really mean.

  1382 experimental subjects (recruited from a professional panel) were asked to read either language from actual (at the time) Facebook, Yahoo and Google's privacy policies (relative to the use of facial recognition software and automated content analysis on e-mails), or language from old policies that at some point in the past had been considered to be inadequate to inform users about privacy practices ("the pre-lawsuit language").

Moving the antecedents of trust towards the not-so-rational side, three articles adopt a very different approach exploring the effect of positive and negative impression made by a website on users' trust and concerns.

- Li et al. (2011) observed that emotions elicited by the initial overall impression of a website act as a first barrier to disclosure of personal data. Later, when users enter the stage of information exchange, fairness-based levers redress privacy behavior.

  A real commercial website –a supplier of Internet fax service– was mimicked. After interacting for a while with the website, 175 students were instructed to fill out a survey that measured their initial emotions before doing anything else. Then, they were asked to complete an evaluation of the sign-up form of the company's 30-day free trial program; the form was used to manipulate information sensitivity.

- Wakefield (2013) revealed that an enjoyable first visit to a previously unknown website affects positively privacy concerns –which are diminished– and trust –which is increased.

  The 301 respondents –recruited by an online marketing research firm– were instructed to act as if they had the money available to purchase a product in the website they visited (either an appliance website or a pool table website). Enjoyment was measured using semantic differentials anchored by enjoyable, exciting and pleasant, while the negative affect items were derived from a scale previously used to measure negative affectivity in the consumption experience.

- Kehr et al. (2015) showed that the assessment of risks and benefits in each individual situation mediates the effect of dispositional factors –such as trust– on personal information revelation; in particular, consumers underestimate the risks associated to data disclosure when the user interface elicits a positive emotional response in them.

  The 480 participants –recruited via Amazon Mechanical Turk in USA, and by a market research company in Switzerland– examined a smartphone application that collected driving behavior data. They were instructed that the processing of either lowly or highly sensitive personal data was needed to achieve an optimal functionality of the application; at the same time, the application was introduced by an either neutral-affect or positive-affect (cute and appealing) screenshot.

Finally, perceived control (over collection and processing of personal data) is another factor commonly integrated in theoretical models. For instance, it is the variable that extends the theory of reasoned action transforming it into the theory of planned behavior, widely used in the area. A few experiments have investigated the link of perceived control with data disclosure.

- Taylor et al. (2009)'s results showed that the effects on data disclosure due to privacy concerns are mitigated by increasing perceived control over the information disclosed.

  The authors built an online travel website. 394 undergraduates were told that the website had been developed by a start-up business and asked to try it out so as to provide feedback

about its functionality and appeal. Data disclosure was either implicit or explicit. Cash compensation was another treatment of the experiment (see below).

- Brandimarte et al. (2013) found that perceived control over disclosure plays a primary role when deciding whether sharing personal data.

  In two experiments, about 200 participants were invited to join a new campuswide networking website that was said to be populated with profiles created by automatically transferring the information provided during a survey (40 questions, with dissimilar level of intrusiveness, related to the daily living on campus and in the city of the respondent). In a third experiment, 134 participants were recruited to complete a survey on "ethical behaviors". Participants were differently informed about the accessibility by others to their answers.

- Tucker (2014) showed that after an enhancement of perceived control over privacy users were nearly twice as likely to click on personalized advertisements. The increase in effectiveness was larger when using more unique private information to personalize messages and for target groups that were more likely to use opt-out privacy settings. Advertisements that targeted but did not use personalized text remained unchanged in effectiveness.

  Data from a randomized field experiment conducted by a nonprofit organization to optimize its advertising campaigns on Facebook were used. The organization randomized whether the advertisement was explicitly personalized to match data from the user's profile. In the middle of the field experiment, Facebook changed its privacy policy introducing an easy-to-use privacy control interface, and giving users new controls over their data. In total, advertisements were shown to 1.2 million users and received 1,995 clicks.

- Hughes-Roberts (2015) provided evidence that reminding individuals of their privacy at the time of the decision produces more privacy-conscious behavior.

  Similarly to the previously described experiment, 62 participants were asked to create a profile on a new social network site addressed to university students by answering a number of questions that varied in the sensitivity of personal information requested. Participants were allowed to review their answers and make amendments based on suggestions from a dynamic privacy score that improved as amendments were made, encouraging in this way privacy-oriented behavior.

- Song et al. (2016), see below on experiments on incentives to disclose, concluded that giving consumers more control over their personal information and adding intimate cues

to messages moderate the negative effects of personalized messages on their privacy risk perceptions.

- Hermstruwer and Dickert (2017) showed that, instead of empowering people to make a free and informed choice over consent, salient ex ante consent options may push people into conformity. A right to be forgotten (right to deletion), however, seems to reduce neither privacy valuations nor "chilling effects".

  The experiment consisted of three stages. In the first stage, participants engaged in a dictator game; then, they were offered to be paid for publishing information about how they behaved; in the third stage, participants were given the right to have this information "forgotten". The first treatment variation consisted in changing the order of the first two stages. The second treatment variation consisted in changing the default of the right to be forgotten. Four sessions were run with a total of 122 participants recruited using a web-based online recruitment system.

3.3. Experiments on incentives to disclose

When deciding whether to disclose personal data, two are the main incentives to which a rational user could respond: a better service, and money.

The first sub-group among those experiments deals therefore with customization. Customized services are the heads of a coin whose tails show the –necessary– use of personal data. A handful of experiments explore the trade-off between anonymity and personalized, more useful, services.

- Annacker et al. (2001) hinted at the fact that users accept personal information requests to a greater extent than expected, on condition that this improves product features.

  In an experiment whose design is virtually the same as that of Spiekermann et al. (2001), 39 students were invited to assess 112 questions that could possibly be posed by an electronic sales agent in an online store. Indeed, questions were borrowed from a real sales agent selling two product categories –a winter jacket, a compact camera– in a premium department store.

- Ward et al. (2005) analyzed whether consumers were willing to further disclose personal information in return for price discounts or a personalized service. The conclusion was negative throughout. The surveyed were even cynical when both benefits were offered simultaneously. Additionally, the results also showed that the participants were worried about and reluctant to disclose financial information but, contrarily, willing to provide personally identifiable data.

320 students were said that, to get an online bookstore membership card, some items of personal information were going to be requested. Personal income, as well as name and address details were either requested or not. Price discounts of 30% and personalized service were other treatments.

- Li and Unger (2012) suggested that under certain circumstances, a high-quality recommendation service can outweigh the influence of privacy concerns; this effect is more pronounced in the case of high transaction value services. Additionally, users who are likely to use personalized services are also likely to pay for them.

  Participants across different experimental conditions (high or low degree of privacy, high or low quality of personalization, and either finance or news as industry domain) were presented with different scenarios. They were inquired about the chances of using such a service. They then were asked about privacy concerns, privacy protection, and quality of personalization. Close to 200 respondents were recruited through social networks, forum postings and direct e-mailing.

- Mothersbaugh et al. (2012) found that customization benefits become less appealing (but effects over perceived control and privacy concerns become stronger) as sensitivity of requested information increases. Conversely, the perception of benefits derived from customization can overcome the adverse impact of sensitive information requests in conditions in which control is high or concern is low.

  The online experiment used a fictitious online TV program. Three variables were manipulated: customization of the website (lower vs. higher), estimated use of the program guide (lower vs. higher), degree of control over data (lower vs. higher). 776 nonstudent Internet users, over 18 years old, were recruited by instructed students.

- Sutanto et al. (2013) showed that personalized service increases application usage; in their experiment, however, users engaged in transactions more frequently only when the service was also privacy-safe –i.e., users' personal information was not transmitted to third parties.

  During three months, 629 users downloaded one of the three versions of the mobile advertising application (non-personalized vs. personalized, either nonprivacy- or privacy-safe) that authors had developed and uploaded to the Apple's app store. All applications allowed users to save advertisements for later consideration; unsaved advertisements were deleted on the next occasion the application was launched. Frequency of use of the application and number of advertisements saved were registered.

- Kobsa et al. (2016) concluded that client-side personalization (keeping personal data on the users' device) influences positively users' attitudes towards personalization, but personalization carried out in the cloud (personalization is detached from any connection consumers may have with a specific provider, i.e. its reputation) does not work well. Personalization made by a reputed company cause a more pronounced impact on users with low concerns and low "self-efficacy" (a person's belief in her cognitive resources and capabilities required to cope with privacy-related problems).

  The hypotheses were tested in an online experiment using a smartphone application that gave personal recommendations on a broad range of topics. In the client-side condition, participants were told that all entered data would remain in their devices; in three other conditions, participants were informed that data will be sent to American Personalization/Amazon/the cloud, respectively. 390 participants were recruited via Amazon Mechanical Turk, through a similar corporate service, and also through posted recruitment advertisements.

- Song et al. (2016) concluded that an increase in the level of personalization increases consumers' privacy risk perceptions. As seen in the previous subsection, those perceptions are mitigated when consumers are given more control over their personal information and intimate cues are added.

  Authors designed three experiments based on an e-mail marketing campaign in which a bank sends e-mails to target consumers to promote its financial products. In the first experiment, 102 undergraduate students received one of four possible e-mail messages (moderately or highly personalized e-mail with or without control) and answered a questionnaire on their privacy risk perceptions. In experiment two (110 students) control was replaced by intimacy as a treatment, and in the third one (168 participants) control and intimacy were both observed.

The second sub-group of experiments in this category includes those papers that deal with monetary incentives. Is the offer of a reward, in particular cash, a way to induce people to disclose personal information? Additionally, some articles that try to put a price to particular pieces of personal information are also included. Though the conclusion is not so clear-cut (any behavioral scientist could talk about it), people are supposed to reveal those data when offered the amount they valued them.

- Andrade et al. (2002), cited before, concluded that the offer of a reward heightens concerns over self-disclosure.

- Ward et al. (2005), as stated a few paragraphs above, found ineffective price discounts strategies.

- Huberman et al. (2005) showed that the desirability of a trait, in relation to the group, is a key factor in the amount of money people demand to make public personal details. For instance, those subjects weighting slightly below average –what can be considered an "ideal" weight– required a small compensation to publicize this; by contrast, individuals with a greater weight –who might hence feel embarrassed or stigmatized– demanded a higher compensation.

  They conducted 10 sessions with 127 participants recruited through local colleges and mailing lists. A reverse second price auction was held; bids reflected how much money participants would ask to be paid for disclosing a particular piece of personal information.

- Xie et al. (2006), cited before, concluded that rewards –in the form of a monetary voucher– positively impacts the users' decision to provide accurate information in the case of personally identifying data but not in the case of demographic data.

- Cvrcek et al. (2006) deducted the value users attach to their location data. Participants were more sensitive to the goal of the data gathering than to the duration of the stockage or to the amount of data collected: the median of the bids almost doubled when they were told that the purpose of data use was commercial and not only academic. Differences across gender, nationality, and technical awareness were also revealed.

  A sample of 1200 primarily university students from five EU countries answered two online questionnaires. Among other questions, they were asked how much compensation would they require to take part in a remunerated (but fictitious) study during one month. Participants were told that an auction would be used to select participants. Changes in the use of the data and in the duration of the study were later suggested.

- Hui et al. (2007), cited before, showed that a monetary incentive has an actual influence on disclosure. As an incentive, participants in their experiment received a check upon completing the survey that varied from 1 to 9 Singapore dollars (US$0.60 to US$5.40).

- Taylor et al. (2009), cited before, found, on the contrary, that the relationship between privacy concerns and behavioral intentions is not affected by the offer of compensation (monetary or not). Compensation, however, intensifies the salience of trust to privacy concerns.

- Premazzi et al. (2010) examined the combined effects of compensation and trust when sharing information with unknown e-vendors. They found that in the presence of incentives individuals were more inclined to disclose data, though they had declared not to be willing to do so. Contrary to their expectations, compensation was more efficient to promote data disclosure in the low-trust condition than in the high-trust one. Indeed, in the

high-trust condition, monetary compensation resulted in lower data release than in the nonmonetary compensation and uncompensated conditions.

The 178 participants (recruited by a market research firm with the excuse of participating in a consumer research survey for a mobile phone operator) were presented with a fictitious prototype, "preview" of the company website, and then asked a number of questions about it. Trust was manipulated through a prior description of the company's profile. After registration, subjects received either a €20 coupon, or a gift valued at €20 (a wireless headphone), or nothing.

- Carrascal et al. (2011) found that individuals place more importance on personally identifying information linked to their online identity than on information linked to their online behavior. Items of the browsing history were valued at about €7, while other items such as age and address were given a higher valuation (about €25).

  A survey published in a major Spanish web portal was the way to recruit a total of 168 participants. They were instructed to install a browser plugin that was in operation for two weeks asking for valuations of personal information in different contexts. For obtaining an honest valuation, a reverse second price auction was used. Data from winners of the auctions were supposed to be used for commercial purposes for a period of six months.

- Acquisti and Grossklags (2012) found substantive differences in the individuals' willingness-to-sell personal data for the various types of information. The Social Security Number, health status and the content of personal e-mail were regarded as valuable and less tradable items by the participants.

  119 volunteers who were willing to participate in economic studies completed an online survey on e-commerce preferences. They were asked for how much money they would reveal some data items to a marketing company that supposedly wanted to buy their personal information.

- Steinfeld (2015) showed that money has a role to play when users take decisions on whether to reveal their offline identity, even when in an anonymous online setting. Interestingly, almost half of participants in the experiment used deception to benefit from the proposal without bearing the cost associated to their acceptance.

  The experiment was conducted in Second Life, a virtual world where users choose an avatar through which they maintain and live a complex virtual life. Participants were offered varied small sums of money (form 0 to 250 *Linden dollars*, equal to USD1.01) in exchange for access to their Facebook profile. The request came from a formal research body, unfamiliar to the users. 203 individuals participated in the study.

- Lee et al. (2015), on the contrary, coincided with other previous studies when concluding that monetary incentives increase information privacy concerns when sensitive information is requested.

  The webpage of a popular Korean e-commerce store was replicated and modified for evaluating four different conditions: high/low sensitive requested information combined with no monetary reward / monetary reward (entry to a draw to win a mobile device or a $10 coupon). The 370 participants –recruited by an online survey agency– were solicited to fill out a questionnaire after browsing a randomly assigned webpage.

- Hirschprung et al. (2016) found that valuating privacy is possible in several realistic scenarios, and particularly when a financial reward is used as an incentive to disclose personal information.

  195 participants recruited using Amazon Mechanical Turk were offered a discount on a future purchase in exchange for the permission to let a (fictitious) e-commerce website use their personal data in forthcoming transactions. After several iterations, the replies to the offers allowed authors to set upper and lower boundaries so it would be possible to conclude that the value of privacy falls inside this range. Six items were included in the experiment. The "adult toy" had the slowest rate of convergence, whereas "rechargeable batteries" had the fastest.

- Feri et al. (2016), see below on experiments on nonrational behavior, found as a secondary result that subjects who experienced a negative outcome when passing a social comparison (i.e., they were below the median of the group) were less likely to accept a voucher to disclose this information.

- Babula et al. (2017) reported that about 45% of the participants in their experiment decided to provide information in return for a hypothetical discount. The differentiation due to the type of product (intimate or neutral good) was not statistically significant.

  A website of a pharmacy with a basket containing a product (condoms or cosmetics) was presented to 489 first-year university students. The price of both products was equal and amounted to PLN 50. They were offered a discount of PLN 10 in return for filling in a short questionnaire (height, weight, date of birth, and date of birth of their next of kin). Name and address were initially asked, as necessary for the fictitious dispatch of goods.

3.4. Experiments on willingness to pay

As we have just seen, people can accept money in return for personal data. Conceptually, a very different question is whether people is willing to spend money to protect their data.

- Tsai et al. (2011), cited before, concluded as an additional finding from their study that some consumers are willing to pay a premium to purchase from privacy-friendly e-commerce companies when information about privacy practices is presented in a way that is easily accessible. The participants kept any money left over after the purchases were completed, encouraging so participants to transact with businesses with cheaper prices.

- Preibusch et al. (2013) reached a very different result. In their experiment with two competitors selling the same product at the same price, the store asking for fewer personal details did not monopolize the market. Moreover, when a trade-off between price and privacy was offered to participants, a wide majority of them chose to buy from the cheaper but more privacy-invasive store.

  Two online stores selling DVDs were presented to 225 participants (pre-registered as interested in laboratory experiments), the second of them asking for more invasive personal information. In one of the treatments the price difference was one euro (€6 vs. €7 in the privacy-invasive shop); in the second treatment, the sale price was the same in both stores. Across both treatments, 74 participants bought a DVD.

  Beresford et al. (2012) is another outcome of the same experiment. The emphasis is put on the fact that the cheaper shop generated great disappointment with its privacy practices; quite the reverse, buyers in the shop with the highest price showed only weak dissatisfaction with price.

- Jentzsch et al. (2012) conducted a very similar experiment and also noticed how most experiment's participants bought from the more privacy-invasive store if price was cheaper, though a *non-negligible proportion* of them chose to pay a premium for privacy.

  443 students were offered the option to purchase cinema tickets in two different online stores. The privacy-invasive provider sold tickets €0.50 cheaper than its competitor. After the finalization of the first transaction, subjects were given the opportunity to repeat the purchase with the following results: 152 individuals bought two tickets, 40 bought only one, and 251 did not buy any tickets.

  The experiment in laboratory was complemented by a hybrid and a field experiment using a website with the same features as in the laboratory. The field experiment had 2,300 visitors but just 10 buyers. The hybrid one (students and friends) had 750 visitors and 16 bought tickets. Those additional experiments confirmed the trends saw in the laboratory.

- Strahilevitz and Kugler (2016), cited before, concluded as an additional result that only just over one-third of the participants showed readiness to pay any money to prevent automated access to the content of their e-mails –intended to be used for targeted

advertising. The median willingness to pay for the non-intrusive version of the e-mail service was $15 per year.

- Spiekermann and Korunovska (2017) reached the conclusion that market awareness or "asset consciousness" is the single most determining aspect affecting willingness to pay for one's personal data. Furthermore, people who build a sense of psychological ownership of their data value it more.

  1269 Facebook users were told to imagine that the social network will close down deleting all the personal data on the platform. In two conditions, paying would allow them to safeguard their data either downloading them to a hard drive or transferring them to another social network. In two other conditions, they were told that a "trustworthy" third-party company was interested in buying all this data of theirs; by paying participants could not only safeguard their data but also avoid the sale.

3.5. Experiments on nonrational behavior

Taken separately, willingness to accept money for personal data and willingness to pay for privacy are two perfectly rational positions. The irrationality comes when subjects present the well-studied-in-other-fields disparity between them (endowment effect). An article examined this effect as well as order effects. A second one secondarily analyzed the same effect without reaching clear conclusions.

- Acquisti et al. (2013) obtained as a main result –in spite of the title of their article– that the value people place on their personal information when they have to decide how much money they would accept to release otherwise private data is notably different than the amount of money they would be willing to pay to protect otherwise public data. The order in which proposals arrive is also important.

  In a field experiment, shopping mall patrons were given gift cards that would enable them to purchase anything from any online or physical shop on condition that they completed a survey. In reality, the survey was a decoy aimed at creating a credible explanation for the gift cards that subjects were offered. Across all conditions, subjects –a total of 349 females– had to choose between two options: a $10 anonymous card or a $12 non-anonymous card.

- Spiekermann and Korunovska (2017), cited before, additionally concluded that the amount of money requested by respondents that could sell their data was greater than the amount that other participants –it should be underlined the *other*– were willing to pay for avoid the

selling of theirs. However, they agreed that it could not be stated that this observation was –at least in part– due to the gap between willingness to pay/to accept.

In a fifth condition of their experiment, participants had no possibility of avoiding the sale of their data; the question in this case was whether they would claim part of the money earned by Facebook and, if so, how much.

The usefulness of a reference point for an action such as personal information disclosure –in which self-limits and values are not always clearly defined– seems to be obvious. However, just one article on the topic has been found.

- Keith et al. (2014) concluded that individuals seem to be taking into account their original reference point of benefits when making risk decisions despite the fact that real risk would have not changed. They become risk averse when in a "gain" situation and risk seeking when in a "loss" situation. Increasing the benefits of information disclosure may thus have the counterintuitive effect of dragging out user disclosure as the perception of risk grows.

  568 undergraduates participated in a field experiment. They were incentivized to track other players of a geo-caching game using a players directory and social network, as well as to complete an optional player profile where to share personal details. Game points –convertible into gift cards and prizes– were awarded for every type of data made public. The points awarded were adjusted up or down over time.

Cases of availability heuristics, i.e. the tendency to judge probability based on recent information and examples, are described on several articles –though the word heuristic is mentioned in just one of them.

- Sundar et al. (2013) concluded in their experiment that individuals who were primed with a benefit heuristic (a futuristic and very-convenient-for-users vision of personalized services) tended to report more information, while those who were primed with which they call a fuzzy boundary heuristic (an example of the risks of the personalization) were less likely to reveal their data. However, the influence of personalization cues was not significant.

  99 participants (method of recruitment undisclosed) took part in two studies. The first study was intended to explore perceptions of the audience of an online video (which in reality served to prime one of the two privacy-related heuristics with a stimulus video clip). The second one investigated usability of two e-commerce stores, either a personalized or a generic version. Participants were then asked to fill in a questionnaire (framed as a consumer survey) that included questions requesting private information.

- Baek (2014) found that people's opinion about online privacy –note that this study gathered opinions and not choices, which may make questionable its inclusion in this group of articles– are swayed after receiving a message including a *counterargument*. The persuasion effect was pronounced among those having limited online skills or those who considered strong the argument presented in the message.

  79 undergraduate students received one of two –similarly persuasive– messages called the "disclosure message" and the "protection message". The protection message advocated a stronger governmental regulation of private ISPs' gathering of personal data on the Internet. The disclosure message, on the contrary, advocated industry self-regulation, with the argument that users could receive better services if personal data were more easily accessed by ISPs.

- Nofer et al. (2014) found a huge impact of a security breach on consumer behavior. Meanwhile, a privacy violation reduces trust in the long term but does not influence consumer decisions in the same way.

  In a laboratory experiment, 118 undergraduate students had to determine how much of their own money they were willing to invest in a financial product issued by an unreal bank. Two treated groups were confronted respectively with a security incident (the bank recently lost customer data) and a privacy incident (the bank recently transferred personal information to another firm without clients' permission).

- Feri et al. (2016) also showed that breach notifications induce a group of individuals – those who regard their information as personally sensitive– to disclose less information to a company.

  The experiment had two parts. In the first part, the 228 participants (no data about how were recruited) conducted an IQ test wit the aim of creating sensitive personal information. The second part consisted of two periods. In each period participants made a decision about whether to buy a real shopping voucher. The voucher was offered at €3 but could be given at a lesser price of €1 on condition that subjects disclose their name and the information about their position on the ranking of test results (respect to the median of the session) to the experimenter. There was a risk that the information passed to the experimenter became revealed to the rest of participants: in each period, a data breach occurred with a probability of 0.5.

- Marreiros et al. (2017)'s results indicate that the exposure to objective threats or benefits of releasing personal data does not necessarily modify privacy behavior. Rather, people are inattentive and their dormant privacy concerns may manifest only when consumers are reminded of their privacy.

Declared privacy concerns, self-disclosure of personal details, and choice of recipient of a donation (either a charity advocating for privacy or a charity not directly related to privacy issues) was observed in a group of 508 participants (recruited from a crowdsourcing community whose members volunteer for academic studies). As experimental manipulations, extracts from newspaper articles –providing facts that highlighted a positive, a negative or a neutral aspect of companies' privacy practices– were used.

- Babula et al. (2017), cited before, found that priming –in the form of an article about a loosely related subject read at the beginning of the study, or as comments concerning the online store that solicited data– reduced the willingness to make data available.

  In an experiment different from the described in a previous section, participants saw a simulation of a price comparison website. They were informed that the two best offers were displayed. The presence of comments from other customers –such as *the transaction was problem-free, but I do not understand why I need to give my personal data*– affected significantly the choice of the store with a (ten percent) cheaper product. Before the start of the experiment, half of the respondents read an article concerning Google and its policy on the use of information and advertisement positioning.

Framing –the fact that people tend to act based on the framework within which the situation is presented– is another well-known cognitive heuristic.

- Acquisti and Grossklags (2012), described before, reframed the marketer's offer (first presented as an outright purchase of data) as a discount on an item participants wanted to purchase or a service they wanted to use. This experimental condition provided nuanced results: the percentage of participants who categorically declined the data sale increased; however, in parallel a considerable number of participants reduced their monetary demands for disclosing highly personal details.

A particular case among framing effects is the adherence to the default option. In particular, the *suspicion* that the behavior is actually influenced by the opt-in or opt-out framing of the consent form is so strong that three articles have addressed the question.

- Johnson et al. (2002) reported that opting-in does not equal opting-out. Indeed, about twice as many people agreed to participate in a survey when receiving the positive frame with a positive default than when both frame and default were negative.

  277 participants (from an online panel) were asked if they agreed to be contacted with further opportunities to participate in online surveys about health. They were randomly assigned to each receive one of the four question formats (alternatives expressed as a positive option or a negative option; checked or unchecked default). In a second

experiment (235 Internet users drawn from the same panel) the question formats were extended adding two "no default" options.

- Lai and Hui (2006) also illustrated how different permutation of frames and default preferences can affect the level of consumer participation. However, consumer participations under opt-in and opt-out converge when privacy concern is high.

  A total of 68 undergraduate students were solicited to assess their impression of the website of an up-and-coming telecommunications firm. Frames (choice/rejection) and default statuses (checked/unchecked) were operationalized by altering elements on the registration page. A second experiment (120 students) employed a similar design as the first one, but a program to track whether the subjects clicked on the privacy policy was installed and, as a final step, participants were directed to a questionnaire to assess an individual's privacy concern.

- Baek et al. (2014), in the same line of the two previous studies, found some evidence of the influence of the frame of the consent form. The framing effect is more significant among people with "weak" attitudes toward privacy, among those with little or no experience of privacy infringement, and when data are linked to the online activity –such as opinions expressed on the Internet or browsing.

  445 respondents, recruited from an online panel, participated in an online survey. Under the opt-out frame participants were instructed to check pieces of personal information that they would like to see protected from a list of unchecked items (no protection as the default condition); under the opt-in frame, participants were asked to uncheck data they deemed not to be worthy of protection from a list of checked items (full protection as the default condition).

Cues that induce disclosure of personal information are another avenue in the study of nonrational behavior.

- Mukherjee et al. (2013) found evidence that monetary cues increase propensity to disclose personal data.

  In two similar experiments, participants (83/88 undergraduate students) were told that personal information was being collected to be shared with an e-commerce firm. They were requested to rate their willingness to reveal pieces of personal information (experiment 1), or asked to actually fill up the data in text boxes (experiment 2). The picture of a currency note was printed in the background of the questionnaire presented to the experimental group, while the control group saw a scrambled version of identical picture.

– Peer and Acquisti (2016) concluded that people treat reversibility as a cue to the sensitivity of the information they are asked to disclose, what leads them to disclose less when reversibility or irreversibility is made explicitly salient beforehand.

  In several experiments, participants –more than 200 in each experiment, recruited from Amazon Mechanical Turk website and from a university-based pool– were presented with different situations (to take part in a study about "personality assessment"; to provide their opinion on a large-scale survey; to test their personality). They were asked to answer several personal, and at times intrusive, questions. Some of the participants were not told anything beforehand, whereas the other participants were explicitly told that they will (reversible condition) or will not (irreversible condition) have the option to change their responses before their final submission.

Dimension of research	Primary focus	Main result	Paper	Remarks / Secondary results
Experiments on the existence of a privacy paradox	Disparity between declared privacy concerns and behavior	Privacy paradox confirmed	*Spiekermann et al. (2001)*	
			Norberg et al. (2007)	
Experiments on trust and control	Mediating role of trust	No relevant impact of trust on disclosure	*Norberg et al. (2007)*	
	Effectiveness of procedures for assurance of protection (in particular privacy policies)	Presence of a privacy policy is effective	*Liu et al. (2004)*	
			Jensen et al. (2005)	See below 'Privacy policies are ignored'
			Xie et al. (2006)	Relationship between reputation of the company and accurate disclosure
			Pan and Zinkhan (2006)	See below 'No influence of the features of privacy statements'
			Arcand et al. (2007)	See below 'No influence of the features of privacy statements'
			Hui et al. (2007)	See below 'A seal-of-approval logo is not effective'
		Influence of the features of privacy statements	*Andrade et al. (2002)*	Completeness of the policy and reputation decrease concerns
			Gideon et al. (2006)	When policies can be easily compared, people choose privacy friendly websites
			Tsai et al. (2011)	When information is noticeable and accessible, people choose privacy friendly websites
			Capistrano and Chen (2015)	Length, visibility and specificity of the policy are important
		No influence of the features of privacy statements	*Spiekermann et al. (2001)*	
			Pan and Zinkhan (2006)	No significant effect of the exact wording of the statement
			Arcand et al. (2007)	No significant effect of the reading of the policy (but the effect is higher when in an opt-in format)
			Joinson et al. (2010)	Significant effect only when a weak privacy policy is combined with low trust
			Martin (2016)	People rely on informal privacy norms instead of upon privacy notices
			Strahilevitz and Kugler	No significant effect of the reading of the policy

			(2016)	
		Privacy policies are not read	*Jensen et al. (2005)* *Malaga (2014)* *Steinfeld (2016)*	Policies are read, even rather carefully, only when they are presented by default
		A seal-of-approval logo is effective	*Miyazaki and Krishnamurthy (2002)*	
		A seal-of-approval logo is not effective	*Hui et al. (2007)*	
		Changes to the online environment (*nudges*) are effective	*Rodríguez-Priego et al. (2016)*	Influence on noticing the privacy link but not on disclosure
	Effect of user interface on trust and disclosure	Significance of the emotional response elicited by a website	*Li et al. (2011)* *Wakefield (2013)* *Kehr et al. (2015)*	When in the stage of information exchange, fairness-based levers redress privacy behavior
	Effect of measures to increase perceived control	Perceived control mitigates concerns	*Taylor et al. (2009)* *Brandimarte et al. (2013)* *Tucker (2014)* *Song et al. (2016)*	
		Reminders of privacy produces more privacy-conscious behavior	*Hughes-Roberts (2015)*	
		Salient information and consent options push people into conformity	*Hermstruwer and Dickert (2017)*	
Experiments on incentives to disclose	Trade-off between anonymity and personalized services	Willingness to disclose information in return for a personalized service	*Annacker et al. (2001)*	
			Li and Unger (2012)	Users who are likely to use personalized services are also likely to pay for them
			Mothersbaugh et al. (2012)	Only in conditions in which control is high or concern is slight
			Sutanto et al. (2013)	Only when the service was also privacy-safe
			Kobsa et al. (2016)	Only when the service was also privacy-safe
		Unwillingness to disclose information in return for a personalized service	*Ward et al. (2005)*	Participants particularly concerned about providing financial information
			Song et al. (2016)	See above 'Perceived control mitigates concerns'
	Effectiveness of monetary incentives	Rewards or price discounts are ineffective	*Andrade et al. (2002)* *Ward et al. (2005)*	On the contrary, increase of concerns

			Taylor et al. (2009)	
			Lee et al. (2015)	On the contrary, increase of concerns
		Rewards or price discounts are effective	*Xie et al. (2006)*	Not in the case of demographic data
			Hui et al. (2007)	
			Premazzi et al. (2010)	Compensation is more efficient in the low-trust condition than in the high-trust one
			Steinfeld (2015)	Almost half of participants in the experiment used deception
			Babula et al. (2017)	
			Feri et al. (2016)	Those who experience a negative outcome when passing a social comparison are less likely to accept
		Users are (supposedly) willing to sell data (i.e,, data has a price)	*Huberman et al. (2005)*	Desirability of a trait, in relation to the group, is a key factor in the amount of money demanded
			Cvrcek et al. (2006)	Participants were more sensitive to the object of the data gathering than to the duration of the stockage
			Carrascal et al. (2011)	Online identity is valued more than online behavior
			Acquisti and Grossklags (2012)	The Social Security Number, health status and content of e-mail are the less tradable items
			Hirschprung et al. (2016)	
Experiments on willingness to pay	Willingness to spend money to protect personal data	Willingness to pay a premium to purchase from privacy-friendly companies	*Tsai et al. (2011)*	
		Unwillingness to pay a premium to purchase from privacy-friendly companies	*Preibusch et al. (2013) / Beresford et al. (2012)*	
			Jentzsch et al. (2012)	A *non-negligible proportion* of participants chose to pay the premium
			Strahilevitz and Kugler (2016)	Only one-third of the participants showed readiness to pay any money
		Market value awareness is the most determining aspect	*Spiekermann and Korunovska (2017)*	
Experiments on nonrational behavior	Existence of an endowment effect	Money asked to disclose data is different than money willing to pay to protect it	*Acquisti et al. (2013)*	
			Spiekermann and Korunovska (2017)	No evidence that results are due to the gap between willingness to pay/to accept
	Use of a reference point	Evaluation of outcomes is dependant on the current situation	*Keith et al. (2014)*	Participants become risk averse when in a “gain” situation and risk seeking when in a “loss” situation
	Evidence of availability	Behavior is influenced by recent	*Sundar et al. (2013)*	

	heuristics	information and examples	*Baek (2014)* *Nofer et al. (2014)* *Feri et al. (2016)* *Babula et al. (2017)*	Persuasion effect was pronounced among those having limited online skills A security breach has a greater impact than a privacy violation
		The exposure to objective threats or benefits does not modify behavior	*Marreiros et al. (2017)*	Privacy concerns may manifest only when consumers are reminded of their privacy
	Existence of a framing effect	The frame of the whole context has an influence	*Acquisti and Grossklags (2012)*	Nuanced results
	Adherence to the default option	The frame of the consent form has an influence	*Johnson et al. (2002)* *Lai and Hui (2006)* *Baek et al. (2014)*	Limited influence when privacy concern is high
	Effectiveness of cues	Monetary cues increase propensity to disclose personal data	*Mukherjee et al. (2013)*	
		Reversibility is a cue to the sensitivity of the information	*Peer and Acquisti (2016)*	

Table 1. Classification of experiments on online disclosure of personal information

4. EXPERIMENTS ON PERSONAL DATA DISCLOSURE: SUGGESTIONS FOR FUTURE WORK

4.1. The study of rational behavior

There is rationality behind the choosing of performing experiments on rational behavior. Several arguments can be brought up, considering that the researched topics have a particular significance for personal information-driven markets. Namely, companies have a strong interest on understanding the possible impact of incentives, and on figuring out the ways to relieve privacy concerns. Likewise they are particularly keen on users' willingness to pay for privacy as it would open the door to innovative business models. Furthermore, the effectiveness of privacy policies and seals is in the major interest of decision makers, as long as the standard regimes of privacy protection keep featuring in "notice and consent" policies.

Therefore, it is expected that researchers will continue exploring these paths. The basic premise stated in the introduction (the disclosure of personal information is a multidimensional, evolving and context-dependent notion and no single framework will be able to catch the huge variety of situations and behaviors) shall require a repetition of experiments in different conditions, flirting at times with not-so rational behavior and so thinning the barrier between both types of experiments. The three cited works that assess the impact of the impression made by a website on trust are good examples of this grey area.

On a theoretical level, experiments shall continue to reassert –or to withhold, or to redefine– the links between concerns, attitudes and behavior, or between mediating factors and any of these variables. The list of possible connections is long and those that are present in most explanatory models –such as the role of trust or control– will keep being privileged.

Rather than on the topics, the challenge lies on the design of the experiments. With a research agenda dominated by the privacy paradox, the immediate advantage of experiments is to directly observe actual behavior and not mere intentions. However, in a significant part of the experiments described in the previous section participants, while immersed in an experimental setting, are finally asked about their feelings or intentions. Other works involve asking individuals to make hypothetical choices. This begs the question of what would qualify as an experiment. Preibusch (2015), who claims that "[true] experiments rather than surveys or hypothetical choices are needed for delivering valid insights to decision makers" explain the methodological requirements of "valid privacy experiments". However, his practical advice adheres to experimental –strictest– standards in economics. The experimental standards in psychology, in contrast, are comparatively laissez-faire, allowing for a wide variety of practices (Hertwig and Ortmann, 2001). The two approaches

might be seen as complementary rather than contradictory (Ariely and Norton, 2007), also when conducting privacy choice experiments. Moving to more specific aspects of the design, Bélanger and Crossler (2011) call for research on privacy to recruit a broader diversity of population profiles.

4.2. The study of inconsistent behavior

As seen in the previous section, only a very few of the not so many experiments conducted in the area of online disclosure of personal data explore the inconsistent behavior of users. That means that, in this case, there is a long way ahead. In the next lines, a description of *possible* heuristics is provided. The "possible" remark should be underlined. It is obvious that their validity can not be a priori stated. They are proposed based on anecdotal evidence and on the scrutiny of companies' activities as firms have indeed developed expertise in exploiting behavioral processes and can even uncover, and trigger, consumer frailty at an individual level (Calo, 2014).

According to the classic definition, heuristic principles reduce the arduous task of assessing probabilities and predicting values to simpler judgmental operations; generally, heuristics are rather helpful, but sometimes they lead to systematic and severe errors (Tversky and Kahneman, 1974). In the case of the disclosure of personal information, a number of heuristics may work. The following ones have been already cited in the literature review made in the previous section:

- *Availability heuristic.* There is a tendency to judge probability based on the difficulty one has in recalling an event. Public information campaigns or recent news about personal information databases leaks or data misuse can affect exposure, making the risks seem more prevalent.

  As seen before, this is the heuristic that so far has received more attention.

- *Use of a reference point.* Decisions about privacy are not formed in the vacuum. There is an expectation on what data companies ask and what data are usually disclosed. Equally, there is an expectation of what is "appropriate" to disclose in a social network. The reference point may be influenced by the context.

  The existence of reference points is one of the –apparently– most evident heuristics that we all, in a way or another, refer to. The experiment cited in the previous section (Keith et al., 2014) addresses it from a restricted perspective. There is a wide scope for further analysis.

- *Framing effects.* The wording of a question influences preferences, in particular when the question refers to sensitive data. The order in which information is asked for is also important as not all the questions about themselves are similarly received by people – once

reached the *limit of acceptability*, people may refuse to continue or even may want to leave. A third effect can arise from the circumstances and justification for data collection, both in the specific and general contexts (in this last regard see Steinfeld, 2017, though conclusions are based on a survey and not on an experiment).

Similarly to the previous case, framing effects seem a priori to have a pervasive influence on disclosure decisions. Again, this is still an unexplored field of research as the previously cited article (Acquisti and Grosslaks, 2012) is but one of many possible examples.

- *Adherence to the default option*. Rational models suppose that people have well-formed preferences, However, people may have not formed preferences over many of the choices they face. If this is the case, the default option fills the void of preferences. In this regard, the default option can perform much like a reference point.

  The effect of opt-in versus opt-out defaults has been already studied but many other experiments about the influence of *untouched* settings can be imagined.

Other heuristics that might be effective in influencing or directing privacy behavior can be added to the list (a list that is obviously far from exhaustive):

- *Immediate reward / Payment decoupling*. "Consumption" (i.e., access to a service obtained after data disclosure, or benefits derived from personalization of applications and services) and "payment" (potential misuse of personal information) are not closely linked as they are separated substantially in time. As a result, we may be in presence of present-biased preferences. An extreme discounting of the future can lead to procrastination behavior when taking actions to defend privacy.
- *Visceral factors*. Linked to the aforementioned heuristic, a special class of projection biases happen as a result of emotions and physical drives or feelings. When a person is in a *hot state* –when a visceral factor is active–, the instantaneous utility function may significantly differ from the expected –regular– utility function.
- *Recency/primacy effect*. People update their beliefs quickly when the information –in particular privacy notices– is easy to understand, displaying a recency effect. On the contrary, when the information is complicated and requires real cognitive effort to discern it, the initial beliefs must probably persist (i.e., a primacy effect is present).

On a separate issue, the same comments about the methodology and design of the experiments made on the previous subsection apply whatever the goal of the experiment.

5. CONCLUSION

Understanding the behavior of people when deciding whether disclosing personal information has become a key issue for companies but also for policy-makers and society at large. Just anecdotal evidence openly suggests the need for experimental approaches. Indeed, as seen before, early studies on the area already claimed for exploring this path. In spite of this, in the about fifteen years since the research on online privacy behavior emerged as a distinct field of scientific enquiry, experiments are but a few when compared to surveys and theoretical approaches, even adopting a broad definition of experiment.

This, of course, is not in contradiction with keeping on the work towards building normative theories that assist on the comprehension of personal data disclosure decisions. While focused on experimental studies, this article strives to reconcile different approaches. Indeed, normative and descriptive theories are not mutually exclusive. Actually, positive theories are in many cases the basis to advance normative theories. Even more, experiments can help to make normative theories more solid.

The article serves as a repository for all –to the best knowledge of authors– the experiments already done in the area and it also proposes a research agenda. It should benefit future research that in turn will help us to understand how individuals face real life decisions about whether to disclose personal information. Hopefully this knowledge will be useful for promoting fairer business practices and more effective privacy regulations.

6. REFERENCES

Acquisti, A., Grossklags, J., 2008. What can behavioral economics teach us about privacy?. In *Digital Privacy. Theory, Technologies, and Practices*, A. Acquisti, S. Gritzalis, C. Lambrinoudakis and S. De Capitani di Vimercati, (eds.), Boca Raton: Auerbach Publications, 363-377.

Acquisti, A., Grossklags, J., 2012. An online survey experiment on ambiguity and privacy. *Communications & Strategies 88*, 19-39.

Acquisti, A., John, L.K., Loewenstein, G., 2013. What is privacy worth?. *The Journal of Legal Studies*, *42*(2), 249-274.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., Wetzels, M., 2015. Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34-49.

Andrade, E.B., Kaltcheva, V., Weitz, B., 2002. Self-disclosure on the Web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, *29*(1), 350-353.

Annacker, D., Spiekermann, S., Strobel, M., 2001. e-Privacy: Evaluating a new search cost in online environments. In *Proceedings of the 14th Bled Electronic Commerce Conference – e-Everything: e-Commerce, e-Government, e-Household, e-Democracy*, Bled: University of Maribor, 292-308.

Arcand, M., Nantel, J., Arles-Dufour, M., Vincent, A., 2007. The impact of reading a Web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, *31*(5), 661-681.

Ariely, D., Norton, M.I., 2007. Psychology and Experimental Economics – A gap in abstraction. *Current Directions in Psychological Science*, *16*(6), 336-339.

Babula, E., Mrzygłód, U., Poszewiecki, A., 2017. Consumers' need of privacy protection – Experimental results. *Economics & Sociology*, *10*(2), 74-86.

Baek, Y.M., 2014. Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, *38*, 33-42.

Baek, Y.M., Bae, Y., Jeong, I., Kim, E., Rhee, J.W., 2014. Changing the default setting for information privacy protection: What and whose personal information can be better protected?. *Social Science Journal*, *51*(4), 523-533.

Barth, S., de Jong, M.D.T., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Bélanger, F., Crossler, R. E., 2011. Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1041.

Beresford, A., Kubler, D., Preibusch, S., 2012. Unwillingness to pay for privacy: A field experiment. *Economics Letters*, *117*(1), 25-27.

Brandimarte, L., Acquisti, A., Loewenstein, G., 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340-347.

Calo, R., 2014. Digital market manipulation. *The George Washington Law Review*, *82*(4), 995-1304.

Capistrano, E., Chen, J., 2015. Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, *42*, 24-31.

Carrascal, J., Riederer, C., Erramilli, V., Cherubini, M., de Oliveira. R., 2011. Your browsing behavior for a big mac: economics of personal information online. In *Proceedings of the 22nd international conference on World Wide Web*, New York: ACM, 189-200.

Cvrcek, D., Kumpost, M., Matyas, V., Danezis,G., 2006. A study on the value of location privacy. In *Proceedings of the Fifth ACM Workshop on Privacy in Electronic Society – WPES '06*, NewYork: ACM, 109-118.

Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285-297.

Feri, F., Giannetti, C., Jentzsch, N., 2016. Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior & Organization*, *123*, 138-148.

Gideon, J., Egelman, S., Cranor, L., Acquisti, A., 2006. Power strips, prophylactics, and privacy, oh my!. In *Proceedings of the Second Symposium on Usable Privacy and Security SOUPS '06*, New York: ACM, 133-144.

Gómez-Barroso, J.L., 2018. Uso y valor de la información personal: Un escenario en evolución. *El Profesional de la Información*, *27*(1), 5-18.

Gómez-Barroso, J.L., Feijóo, C., Martínez-Martínez, I.J., 2018. Privacy calculus: Factors that influence the perception of benefit. *El Profesional de la Información*, *27*(2), 336-343.

Hermstruwer, Y., Dickert, S., 2017. Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge. *International Review of Law and Economics, 51*, 38-49.

Hertwig, R., Ortmann, A., 2001. Experimental practices in economics: A methodological challenge for psychologists?. *Behavioral and Brain Sciences*, *24*(3), 383-403.

Hirschprung, R., Toch, E., Bolton, F., Maimon, O., 2016. A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, *61*, 443-453.

Huberman, B.A., Adar, E., Fine, L.R., 2005. Valuating privacy. *IEEE Security & Privacy*, *3*(5), 22-25.

Hughes-Roberts, T., 2015. Privacy as a secondary goal problem: an experiment examining control. *Information & Computer Security*, *23*(4), 382-393.

Hui, K.L., Teo, H.H., Lee, S.Y.T., 2007. The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Jensen, C., Potts, C., Jensen, C., 2005. Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1-2), (203-227.

Jentzsch, N., Preibusch, S., Harasser, A., 2012. *Study on monetising privacy. An economic model for pricing personal information*, ENISA Deliverable – 2012-02-27, Heraklion: European Network and Information Security Agency, https://www.enisa.europa.eu/publications/monetising-privacy

Johnson, E.J., Bellman, S., Lohse, G.L., 2002. Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters*, *13*(1), 5-15.

Joinson, A.N., Reips, U.D., Buchanan, T., Schofield, C.B., 2010. Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, *25*(1), 1-24.

Jolls, C., Sunstein, C.R., Thaler, R., 1998. A behavioral approach to Law and Economics. *Stanford Law Review*, *50*(5), 1471-1550.

Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

Keith, M.J., Babb, J.S., Lowry, P.B., 2014. A longitudinal study of information privacy on mobile devices. In *Proceedings of the 47th Hawaii International Conference on System Sciences*, Washington: IEEE, 3149-3158.

Knijnenburg, B., Kobsa, A., Jin, H., 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, *71*(12), 1144-1162.

Kobsa, A., Cho, H., Knijnenburg, B.P., 2016. The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology*, *67*(11), 2587-2606.

Kokolakis, S., 2017. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers, & Security*, *64*, 122-134.

Lai, Y.L., Hui, K.L., 2006. Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns. In *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research*, New York: ACM, 253-263.

Lee, H., Lim, D., Kim, H., Zo, H., Ciganek, A.P., 2015. Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, *34*(1), 45-56.

Li, H., Sarathy, R., Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62-71.

Li, H., Sarathy, R., Xu, H., 2011. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Li, Y., 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471-481.

Li, T., Unger, T., 2012. Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, *21*(6), 621-642.

Liu, C., Marchewka, J.T., Lu, J., Yu, C., 2004. Beyond concern: a privacy–trust–behavioral intention model of electronic commerce. *Information & Management*, *42*(1), 127-142.

Malaga, R.A., 2014. Do web privacy policies still matter?. *Academy of Information and Management Sciences Journal*, *17*(1), 95-99.

Marreiros, H., Tonin, M., Vlassopoulos, M., Schraefel, M.C., 2017. 'Now that you mention it': A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization*, *140*, 1-17.

Martin, K., 2016. Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online. *Journal of Legal Studies*, *45*(S2), pp S191-S215.

Miyazaki, A.D., Krishnamurthy, S., 2002. Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs*, *36*(1), 28-49.

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., Wang, S., 2012. Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, *15*(1), 76-98.

Mukherjee, S., Manjaly, J., Nargundkar, M., 2013. Money makes you reveal more: consequences of monetary cues on preferential disclosure of personal information. *Frontiers in Psychology*, *4*, article 839.

Nofer, M., Hinz, O., Muntermann, J., Roßnagel, H., 2014. The economic impact of privacy violations and security breaches: A laboratory experiment. *Business, & Information Systems Engineering*, *6*(6), 339-348.

Norberg, P.A., Horne, D.R., Horne, D.A., 2007. The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

Pan, Y., Zinkhan, G.M., 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331-338.

Peer, E., Acquisti, A., 2016. The impact of reversibility on the decision to disclose personal information. *Journal of Consumer Marketing*, *33*(6), 428-436.

Preibusch, S., Kubler, D., Beresford, A., 2013. Price versus privacy: an experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research*, *13*(4), 423-455.

Preibusch, S., 2015. How to explore consumers' privacy choices with behavioral economics. In *Privacy in a Digital, Networked World – Technologies, Implications and Solutions*, S. Zeadally and M. Badra (eds.), Cham: Springer, 313-341.

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., Hofacker, C.F., 2010. Customer information sharing with e-vendors: The roles of incentives and trust. *International Journal of Electronic Commerce*, *14*(3), 63-91.

Rapoport, A., 1989. *Decision theory and decision behavior – Normative and descriptive approaches*. Dordrecht: Springer-Science+Business Media, B.V.

Rodríguez-Priego, N., van Bavel, R., Monteleone, S., 2016. The disconnection between privacy notices and information disclosure: an online experiment. *Economia Politica*, *33*(3), 433-461.

Song, J.H., Kim, H.Y., Kim, S., Lee, S.W., Lee, J., 2016. Effects of personalized e-mail messages on privacy risk: Moderating roles of control and intimacy. *Marketing Letters*, *27*(1), 89-101.

Spiekermann, S., Großklags, J., Berendt, B., 2001. Stated privacy preferences versus actual behavior in EC environments: A reality check. In *e-Finance*, H.U. Buhl, N. Kreyer and W. Steck (eds.), Berlin Heidelberg: Springer, 129-147.

Spiekermann, S., Korunovska, J., 2017. Towards a value theory for personal data. *Journal of Information Technology*, *32*(1), 62-84.

Steinfeld, N., 2015. Trading with privacy: the price of personal information. *Online Information Review*, *39*(7), 923-938.

Steinfeld, N., 2016. 'I agree to the terms and conditions': (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, *55*(B), 992-1000.

Steinfeld, N., 2017. Track me, track me not: Support and consent to state and private sector surveillance. *Telematics and Informatics*, *34*(8), 1663-1672.

Strahilevitz, L.J., Kugler, M.B., 2016. Is privacy policy language irrelevant to consumers?. *Journal of Legal Studies*, *45*(S2), pp S69-S95.

Sundar, S., Kang, H., Wu, M., Go, E., Zhang, B., 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key?. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems*), New York: ACM, 811-816.

Sutanto, J., Palme, E., Tan, C., Phang, C., 2013. Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, *37*(4), 1141-1164.

Taddei, S., Contena, B., 2013. Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in Human Behavior*, *29*(3), 821-826.

Taylor, D.G., Davis, D.F., Jillapalli, R., 2009. Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), pp 203-223.

Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A., 2011. The effect of online privacy information on purchasing behavior: an experimental study. *Information Systems Research*, *22*(2), 254-268.

Tucker, C., 2014. Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546-562.

Tversky, A., Kahneman, D., 1974. Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124-1131.

Wakefield, R., 2013. The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, *22*(2), 157-174.

Wang, T., Duong, T.D., Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531-542.

Ward, S., Bridges, K., Chitty, B., 2005. Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications*, *11*(1), 21-40.

Xie, E., Teo, H., Wan, W., 2006. Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behaviour. *Marketing Letters*, *17*(1), 61-74.

Zafeiropoulou, A., Millard, D., Webber, C., O'Hara, K., 2013. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?. In *Proceedings of the 5th Annual ACM Web Science Conference*. New York: ACM, 463-472.