The Economic Impact of Privacy Violations and Security Breaches

A Laboratory Experiment

In an experiment, the authors distinguish between the impact of privacy violations and security breaches on the subjects' trust and behavior. They focus on first-order effects and thus the direct consumer reaction. While privacy is of prime importance for building trust, the actual behavior is affected less and customers value security higher when it comes to actual decision making. Evidence is found for the so-called "privacy paradox" which describes that people do not act according to their privacy concerns.

DOI 10.1007/s12599-014-0351-3

The Authors

Dipl.-Kfm. Michael Nofer (✉)
Prof. Dr. Oliver Hinz
Chair of Information Systems, esp. Electronic Markets
TU Darmstadt
Hochschulstr. 1
64289 Darmstadt
Germany
nofer@emarkets.tu-darmstadt.de
hinz@emarkets.tu-darmstadt.de

Prof. Dr. Jan Muntermann
Chair of Electronic Finance and Digital Markets
University of Göttingen
Platz der Göttinger Sieben 5
37073 Göttingen
Germany
muntermann@wiwi.uni-goettingen.de

Dr. Heiko Roßnagel
Fraunhofer Institute for Industrial Engineering
Nobelstr. 12
70569 Stuttgart
Germany
heiko.rossnagel@iao.fraunhofer.de

Received: 2013-10-08
Accepted: 2014-03-26
Accepted after one revision by Prof. Dr. Karagiannis.
Published online: 2014-10-21

This article is also available in German in print and via http://www.wirtschaftsinformatik.de: Nofer M, Hinz O, Muntermann J, Roßnagel H (2014) Der ökonomische Einfluss von Privacyverletzungen und Securityvorfällen. Ein Laborexperiment. WIRTSCHAFTSINFORMATIK. doi: 10.1007/s11576-014-0440-4.

Electronic Supplementary Material
The online version of this article (doi: 10.1007/s12599-014-0351-3) contains supplementary material, which is available to authorized users.

1 Introduction

A series of cyber-attacks in recent years at global companies like Sony, Citigroup, Lockheed Martin, Google, and Apple have shown that even large companies are vulnerable to attacks that threaten the protection of their costumers' data. Most recently, 250,000 Twitter accounts (Kelly 2013) and up to 6.5 million LinkedIn user accounts have been hacked (Silveira 2012). These security incidents can lead to serious consequences for the affected companies. For instance, Sony had to close their PlayStation network and their Online Entertainment platform for several weeks in May 2011 after hackers had been able to get access to 77 million user accounts, extracting customer information such as passwords, home addresses, and dates of birth (Bilton and Stelter 2011). As a result, the company spent USD 170 million to cover the costs for increased customer support, data security improvements, and overall investigations into the incident.

In the long run, indirect consequences might be an even bigger threat to company success. Since privacy was identified as a major antecedent of trust, the relationship between existing and prospective clients and the company may permanently suffer. Several attempts to study the link between privacy, trust, and the intention to buy a product have been reported in literature, especially in the e-commerce environment, where trust plays an important role for business (Eastlick et al. 2006; Gefen 2000; Kim et al. 2008; Liu et al. 2005). These studies suggest a direct connection between privacy, security, and the buying intention, as well as a strong impact of privacy and security on trust in the company, which in turn influences the willingness to enter a business relationship.

Determining the impact of privacy violations and security breaches in monetary terms is quite challenging. This is due to the various factors that affect company success, so that the influence of privacy and security cannot easily be isolated from other effects. The event study methodology is often used to assess the economic impact of privacy and security incidents (Acquisti et al. 2006; Andoh-Baidoo et al. 2010; Cavusoglu et al. 2004; MacKinlay 1997). However, this approach is based on the strong

assumption that the market correctly and fully reflects the impact of the event (e.g., security breach) on the customers' behavior and that the effect can be isolated from other effects.

Against this background, the motivation of our study is to explore the causal effect of data protection violations on consumer behavior by conducting a laboratory experiment. The goal is to analyze and compare the economic impact of privacy violations and security breaches. For this purpose, we use one control and two treatment groups. Whilst no data protection problem occurs in the control group, the other two groups are confronted with a privacy and respectively a security incident of a fictional bank. We first provide general information about the bank (cf. the Appendix – available online via http://link.springer.com). For this we use information on one of the largest European banks from Wikipedia which we slightly adapted (e.g., changed the name). This description also includes information on (a) a privacy violation in the recent past, (b) a security breach in the recent past or (c) none of these incidents. After this short description of the bank's characteristics, subjects were informed of the investment conditions of this bank, which is identical for all three conditions. The subjects then have to decide how much of their own money they are willing to invest in a financial product offered by the fictional bank. The money invested can also be lost with a probability that is identical for all three scenarios. It is important to note that subjects are not aware of the other scenarios but only get the information for the group to which they were randomly assigned (see Sect. 5.1 for details).

We adapt the economic decision game called the "investment game", first introduced by Berg et al. (1995), in a way that allows us to compare the proportion of investments between the groups, thereby isolating the impact of security breaches and privacy violations, since all the other information on bank characteristics and investment conditions are identical for all participants. Beside this monetary impact, we also investigate how trust in the bank is affected and how trust in turn influences the willingness to invest. Thus, we can determine and compare the direct and indirect impact of privacy violations and security breaches on the investment amount. Many other studies investigate privacy and security issues from the viewpoint of the capital market and show the influence on share prices (Acquisti et al. 2006; Andoh-Baidoo et al. 2010; Cavusoglu et al. 2004). The stock market reflects the investors' expectations with regard to the company's future success. In contrast to these second-order effects, our study focuses on first-order effects, that is, the direct customer reaction to privacy violations and security breaches and thus offers a new way to quantify the impact of privacy and security issues. In addition, as a subordinate research goal, we aim to answer the question whether the so-called "privacy paradox" persists after a privacy breach occurred. The privacy paradox was demonstrated by researchers and means that consumers do not act according to their stated privacy concerns (e.g., Berendt et al. 2005; Dommeyer and Gross 2003; Norberg et al. 2007). So far, consumer behavior was studied without the occurrence of privacy or security incidents. We can therefore extend previous findings and test whether consumers change their behavior after a company suffers privacy breaches.

We first refer to work related to our study and then discuss the concepts of privacy and security, as well as their close link to trust and behavioral intentions. We present previous findings, emphasizing the meaning of trust for relationships and business activity in particular. We proceed with our research model and hypotheses, before we present the empirical results. We conclude the article with a discussion of the findings and ideas for future research.

2 Related Work

Following the own privacy policy is crucial for companies. Culnan and Armstrong (1999) show that fair behavior can build trust and that retention rates will be higher if clients perceive to be treated fairly. Thus, companies should behave in line with their rules, which should be externally communicated in order to increase the likelihood of obtaining personal information from consumers. In contrast, John et al. (2011) found that disclosing the own privacy policy and informing about data protection can actually lower consumers' willingness to provide personal information since privacy concerns increase. However, Hinz et al. (2011) found that honestly revealing the use of data can increase profits. This is also confirmed by Tsai et al. (2011) who show that the display of privacy policies positively influences the purchase intention and consumers even pay a price premium for more privacy protection.

Privacy violations also affect the company's reputation, a critical factor for long-term success. In a literature review, Yoon et al. (1993) report various findings about the role of company reputation and show empirically that the company's reputation has a direct and indirect impact on the intention to buy a product.

The impact of privacy violations and security breaches on a firm's value has been addressed by a number of empirical analyses on the basis of the event study methodology. Here, authors measure excess stock market returns of listed firms that have been affected by a corresponding event. Andoh-Baidoo et al. (2010) for example observe the impact of security breaches that have been reported in major US newspapers. They detect significant stock price reactions within an event period of three days starting one day prior to the event date. In contrast, Acquisti et al. (2006) address the impact of privacy violations on a firm's market value. Their results provide evidence for a significant but moderate price effect that can be observed during the two days subsequent to the publication. While event studies are well-recognized in empirical research, there exist a number of possible biases that can affect results (Campbell et al. 1997). One major problem results from uncertainty about the event dates when collecting them from financial publications. Other problems can result from non-trading or non-synchronous trading that for example occurs due to the fact that used closing prices do not have a common timestamp since they result from the last transaction of a trading day. As noted by Acquisti et al. (2006), limitations can also arise due to small sample sizes that would also be needed to "understand and contrast the impact of 'pure' security breaches compared to privacy ones", which also provides motivation for future research and to "study empirically the implications of privacy violations that go beyond their stock market influence" (p. 1579).

3 Theoretical Background

3.1 Privacy

There is no consistent definition of privacy and many researchers see it as a multidimensional construct (Foxman and

Kilcoyne 1993; Goodwin 1991; Prosser 1960). The ambiguousness may be due to the different areas where the concept of privacy is used and discussed. Generally, one can distinguish between physical privacy and information privacy (Smith et al. 2011). The former refers to an individual's ability to live undisturbed and without interferences within private surroundings. Information privacy has increasingly gained in importance since the beginning of the information age. Unless otherwise stated, we use privacy as a synonym for information privacy. One popular notion in political science comes from Westin (1967), specifying privacy as "the ability of individuals to control the terms under which their personal information is acquired and used".

The element of control is especially important for the relationship between companies and consumers due to the increasing collection of personal information in recent years. Goodwin (1991) defines consumer information privacy as "the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present".

We furthermore refer to Greenaway and Chan (2005) who make a distinction between consumer information privacy and organizational privacy which describes "how firms treat their customers' personally identifiable information". The simulated privacy breach, which is described below, affects consumers' privacy but is also a case of organizational privacy due to the unfair treatment of consumer information by the company.

Researchers have repeatedly shown that consumers are concerned about privacy and the way that companies treat their personal information (e.g., Berendt et al. 2005; Phelps 2000). Since the end of the 20th century, advances in information technology make it easier for companies to collect and distribute information. Therefore privacy concerns emerge especially with regard to the *secondary use of personal information* (Culnan 1993). Unauthorized secondary use exists when data is collected for one purpose but used for another purpose without the individual's permission. Smith et al. (1996) identified three other dimensions being central to the individual's privacy concerns. The *collection* of personal information reflects the fear that too much data about the individual is collected in society. Another area of concern is the *improper access*, which means that people within the organization have unjustifiable access to the customer information. The fourth dimension is an *error* in personal data, which might result from typing errors or accidental mistakes. Consistent across cultures, unauthorized secondary use of information was found to be the most important concern dimension for consumers (Milberg et al. 1995).

3.2 Security

For the purpose of our research, it is important to make a distinction between privacy and security, although some authors use these concepts interchangeably or summarize the concepts under new terms, such as "structural assurance" (Luo et al. 2010; McKnight and Chervany 2001–2002).

Security concerns increased significantly since transactions can be done over the Internet. Recent cyber-attacks at Sony or Citigroup show the vulnerability of today's technology. Consumers are afraid of criminal activities, such as information theft and data fraud (Suh and Han 2003). This is why many studies identified perceived security as a major antecedent of consumers' willingness to purchase from e-commerce stores (Belanger et al. 2002).

Kalakota and Whinston (1996) define a security threat as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse."

Smith et al. (2011) review more than 300 privacy articles and differentiate between privacy and security in such a way that security concerns result from concerns about: "*integrity* that assures information is not altered during transit and storage; *authentication* that addresses the verification of a user's identity and eligibility to data access; and *confidentiality* that requires data use is confined to authorized purposes by authorized people" (p. 996). Thus, security includes all steps to make the storage of personal information secure.

Security and privacy have certain aspects in common. Especially the *improper access* dimension of Smith's construct is related to security to the extent that a person might be able to get access to personal information. These cases include the well-known examples of security breaches such as hacker attacks or data theft by unauthorized persons. Thus, companies cannot protect the individual's privacy without security.

According to Ackerman (2004), security is a necessary but not sufficient precondition for the protection of an individual's privacy. Culnan and Williams (2009) as well as Solove (2006) also define security as being one part of privacy.

However, one distinctive feature is the ethical dimension. Even when the company has made every effort to ensure security, privacy can be still threatened by moral failings such as the unauthorized secondary use of information.

Culnan and Williams (2009) identify vulnerability and avoiding harm as the two parts of morality which are important in the relationship between companies and their customers. Vulnerability exists due to the asymmetrical distribution of information and control. The company has the power to decide how to deal with the information collected. Managers can treat customer information in accordance with ethical guidelines or they can harm the customers, for example, by unauthorized secondary use.

Foxman and Kilcoyne (1993) address ethical dimensions with regard to privacy and a company's marketing practices by showing corporate activities that potentially threaten consumers' privacy. They conclude that the relationship between firms and customers is seriously affected by privacy violations. Accordingly, the company should treat personal information in a way that is consistent with the customers' right to privacy. Straub and Collins (1990) believe that this right to privacy "can best be protected through self-regulating policies and procedures."

Our research builds on these observations on morality and ethics when differentiating between a privacy and security incident. The privacy violation in our study lies in the fact that the bank is transferring personal information to a cooperating insurance company without the client's permission. The security breach is a stolen CD with customer information which is now offered for sale (**Table 1**). We assume that public opinion would differentiate between both cases. While the company does not fulfill its moral responsibilities in the case of the privacy breach, the security incident is caused by unauthorized access and thus a criminal activity.

Table 1 Simulation of privacy and security breach in our laboratory experiment

Privacy Breach	The bank is transmitting personal data to a cooperating insurance company without the client's permission
Security Breach	The bank has lost customer data. A former bank employee has stolen a CD with personal information and is now offering it for sale

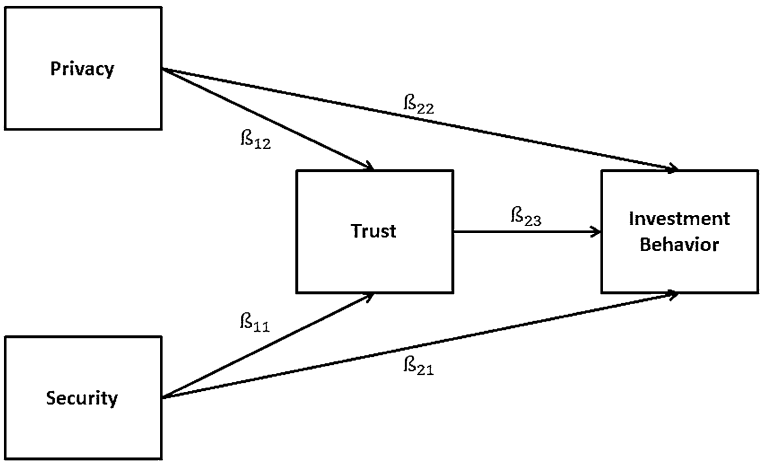

Fig. 1 Conceptual framework

3.3 Trust

Both privacy and security are important factors for building trust in a company. Trust is crucial in virtually all interpersonal relations and economic transactions (Hosmer 1995). The meaning of trust has been studied in various disciplines, such as psychology (Rotter 1971), sociology, (Granovetter 1985) and economics (Gefen 2000). This is why many definitions exist, often reflecting the perspectives from the different disciplines, but today most researchers see it as a multidimensional and context-dependent construct (Ganesan 1994; Rousseau et al. 1998).

Gefen et al. (2003) provide a detailed overview of previous conceptualizations of trust in the literature. Although definitions vary across disciplines, researchers from different disciplines agree upon some necessary conditions for trust. Trust becomes relevant if the situation involves uncertainty about the future outcomes, because the trustor does not have the complete control and must enter into risks, being dependent on the decisions of the trustee who can either act trustworthy or untrustworthy (Kee and Knox 1970). The relationship between trust and risk is a reciprocal one, "risk creates an opportunity for trust, which leads to risk taking" (Rousseau et al. 1998). There would be no need for trust if there was complete certainty about the behavior of the acting persons. The trustor will rely upon the trustee if he perceives three characteristics to be met (Bhattacherjee 2002; McKnight et al. 2002): ability (concerns about the competence of the trustee), integrity (concerns about the honesty and moral principles) and benevolence (concerns about the goodwill towards the trustor). The nature of trust depends on the degree of interdependence – another necessary condition – which means the reliance between trustor and trustee. Researchers across disciplines also see trust as a psychological condition, rather than a behavior or choice.

The necessary conditions for trust are reflected in the popular notion of Mayer et al. (1995) who define trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or confront that other party". In the context of this paper it is important to distinguish between general trust and initial trust. General trust develops over time based on experiences between the trusting party and the trustee. We focus on initial trust, which occurs "when parties first meet or interact" (McKnight et al. 1998). In this situation neither of the two parties has any kind of experiences by means of which the trustworthiness could be evaluated.

4 Research Model

For the purpose of our study, the following research model can be derived from previous academic work (**Fig. 1**).

We assume both a direct impact of privacy and security on the actual behavior and an indirect relationship between privacy, security, trust, and behavior. We will focus on the case from the financial industry and will examine the impact of privacy and security incidents on the investment behavior (i.e., purchase of a financial product offered by the bank).

Previous research shows that privacy and procedural fairness are important antecedents of trust. Consumers' trust in e-commerce companies, for example, is positively affected by the level of privacy protection and the attempts of the firm to ensure data security (Suh and Han 2003). Moreover, the perception of how the company is treating customer data also impacts this relationship (Liu et al. 2005). Gefen et al. (2003) found that the trust in an e-vendor increases when customers believe that the vendor does not gain any advantages from being untrustworthy. The authors also show that security mechanisms on a website are important antecedents of trust. Based on the results from an analysis of industries employing database marketing strategies, Milne and Boza (1999) infer that trust can be influenced by the likelihood that an organization is sharing information with third parties.

Hence, companies should behave in line with their own privacy policy, since consumers' expectations regarding what will be done with their data is built upon these organizational regulations (Culnan and Armstrong 1999). If a bank for example is transmitting customer information to a cooperating insurance company without the clients' permission and without mentioning it explicitly in their privacy disclosure, people might be displeased. As a result, one can expect that the trust in the company will suffer due to this privacy violation.

Hence, we hypothesize:

H1a: A security breach at a company has a negative impact on trust in the company.
H1b: A privacy violation by a company has a negative impact on trust in the company.

Only few studies examined the direct link between privacy, security, and purchase intentions. One of these studies was conducted by Eastlick et al. (2006) who found that consumers' privacy concerns can have a negative impact on the purchase intention towards an e-tailer. These findings are consistent with the results of studies in the field of direct marketing, suggesting that privacy concerns negatively influence purchase levels and direct marketing response (Milne and Boza 1999).

We will examine a case where from a rational point of view, people should behave equally, no matter whether a security or privacy problem exists or not, as the expected outcome does not change. However, empirical results suggest that the economic behavior can be influenced by feelings and emotions. For instance, people are more optimistic when they are in a good mood (Schwartz and Clore 1983) and risks can be judged differently, depending on the way the information is presented (Johnson and Tversky 1983). While standard finance theory posits that people act rationally, behavioral finance theory includes cognitive errors of human behavior (Statman 1999). For instance, there is evidence for the overreaction of stock markets following unexpected news events, as investors overweight recent information and underweight earlier data (De Bondt and Thaler 1985). It is therefore likely that privacy and security problems negatively impact the consumers' investment decision.

Collectively, these findings suggest:

H2a: A security breach at a company has a negative, direct impact on consumer behavior (*here: investment behavior*).

H2b: A privacy violation by a company has a negative, direct impact on consumer behavior (*here: investment behavior*).

Researchers focus more frequently on the impact of trust on behavioral intentions, particularly within business relationships. Many studies in e-commerce show that trust is a crucial determinant for the intention to buy a product. For instance, it was found that trust in the vendor significantly influences people's intention to purchase books on amazon.com (Gefen 2000). By studying the online shopping behavior of undergraduate students, Kim et al. (2008) show that consumers' trust influences not only the purchase intention, but also the actual purchase behavior. The authors invited students to visit at least two shopping websites and to search for products they were interested in. Before confirming the purchase, they were assigned to one questionnaire, either with questions about the website they were more likely to buy from, or with questions about the website they were less likely to buy from. Afterwards participants continued their purchase from the preferred website. The model created by McKnight and Chervany (2001–2002) also posits that the customer is more likely to purchase from a company if the company's behavior seems to be honest and predictable. As people perceive their financial information as especially sensitive (Woodman et al. 1982), the role of trust could also be important for investment decisions.

Hence, we hypothesize:

H3: Trust in a company positively impacts consumer behavior (*here: amount of investment*).

A great deal of studies and surveys show that there seem to be growing concern among consumers who fear that their personal information is not protected enough. According to a Gallup poll, 65 percent of Facebook users and 52 percent of Google users are worried about their privacy when using these Internet applications (Morales 2011). However, there is evidence that the actual behavior does not always reflect these general privacy concerns. The difference between intentions and behavior was described as the "*privacy paradox*" in the literature (Norberg et al. 2007; Smith et al. 2011). For instance, Spiekermann et al. (2001) compared the disclosing behavior of online shoppers with their previously stated privacy concerns. Surprisingly, participants have been willing to provide a great deal of private information (e.g., address), although reporting to be highly concerned about their personal data. Norberg et al. (2007) also show that people actually disclose far more personal information (e.g., financials, demographics) to a commercial enterprise than they intend to disclose. The dichotomy between stated intentions and actual behavior with regard to privacy suggests that people's trust in a company is more affected by a privacy breach than their behavior. We therefore assume that the intention-behavior gap persists after the occurrence of a privacy breach.

Hence, we hypothesize:

H4: A privacy violation by a company has a stronger negative impact on trust than on actual consumer behavior.

5 Laboratory Experiment

5.1 Method

In contrast to previous research that used event study methodology for showing the reaction of the capital market (second-order effect), we conducted a laboratory experiment in order to focus on the direct consumer reaction (first-order effect) to privacy and security incidents. Although this is an artificial environment and one must be careful when generalizing findings, there are many advantages of experiments: researchers have the opportunity to effectively manipulate the independent variables and control for other influences so that causal relationships can be identified, which is an advantage compared to other methods including event studies. Another reason for the popularity of this method is the possibility of an inexpensive implementation and replication that allows one to test the robustness of the findings.

The task for each subject was to decide about a financial investment. We used the investment decision as a cover story and did not reveal the real purpose of our study, namely the consumer reaction to different data protection violations. Cover stories have been successfully used in consumer research (e.g., Childers and Houston 1984; Gorn 1982). For instance, the cover story of Gorn (1982) comprised the selection of music for a pen commercial by the participating subjects. The actual purpose of the study was to show the relationship between the choice of the pen and the kind of music that was being played. Subjects were more likely to pick the color of the pen that was paired with liked rather than disliked music.

We applied a between-subject design, where all participants were randomly assigned to one of three groups. Every group received exactly the same information on the characteristics of the bank and the investment conditions. The information only differed with regard to a small detail about the privacy or security incident in the recent past of the bank. The participants in the control group were not confronted with any privacy or security breach. In the first treatment group we added the following sentence to the general description of the bank "The bank has recently been caught transmitting personal data to a cooperating insurance company without the client's permission." This clearly describes a privacy

violation. In the second treatment group we added the sentence: "The bank has lost customer data. A former bank employee has stolen a CD with personal information and is now offering it for sale." This describes the security breach. This additional treatment information was presented very shortly at the end of the bank description.

Participants had to indicate the amount of money they were willing to invest into a financial product given the investment plan offered by the bank. To create an economic decision situation that reflects this decision, we modified the so-called "investment game", first introduced by Berg et al. (1995). This experimental method allows the measurement of trust in another person by the following procedure: one person, the trustor, receives 10 US dollars which can be invested into a geographically separated person (the trustee) who is unknown to the trustor. As soon as the trustee receives the money, the invested sum is tripled. The trustee now can decide how much money s/he is willing to send back to the trustor and how much s/he will keep for her/his own. It is certainly rational for the trustee to keep all money as s/he does not know the trustor and this is a one-shot-game. The trustor can of course anticipate this behavior and should, from an economic point of view, not invest any money in the trustee. However, several experimental studies show that money is invested and people tend to trust even unknown persons (Bolle 1998; Forsythe et al. 1994). Thus, in this game, trust can lead to monetary gains.

In our case, we conducted a slightly adapted investment game. The trustee is not another person but the trustor has to decide how much money s/he is willing to invest into a financial product offered by a fictional bank. In the experimental instructions we provided information on the fictitious bank which was similar to those of real banks, as well as the conditions under which they could invest their own real money: in all groups the investment horizon was 10 years in which the performance of the invested capital was 7% per year, given a default rate of 10%. The subjects received EUR 10 in cash and were offered the possibility to invest this money. They could invest up to EUR 10 and received their interest-paying money back with a probability of 90% (=1-default rate) after the experiment which lasted about 15 minutes. However, there was no obligation to invest a share so that participants could also keep all the money and leave immediately. In this case, there was no chance to generate more than EUR 10 but also no risk to lose the money due to the default of the bank (i.e., an unlucky die roll).

In order to illustrate the rules, subjects received the following numerical example: "Assume that you invest EUR 5, then you keep the other EUR 5 in all cases. The invested capital is virtually doubled given that there is no default, for which the probability is 10%. Thus, the complete amount paid out is EUR 15 at the end of the experiment if there is no default, otherwise it is EUR 5." This example clarifies that there is an element of risk since the repayment of the invested money depends on the default of the bank.

Based on the roll of a die, every 10th participant did not get his investment back. The probability of a default was totally independent of privacy or security incidents. Differences among the different experimental groups in terms of trust and behavior are therefore irrationally caused by the different levels of privacy and security concerns. The uncertainty about future returns due to the possible default leads to a trust game between the trustor (= participant) and the trustee (= fictional bank). If participants place more trust in the bank, they are likely to invest a higher proportion of their capital.

In order to determine subjects' trust in the bank, we used a 7 item Likert scale (1 = strongly disagree, 7 = strongly agree; cf. the Appendix). This scale aims to measure trust as beliefs about the other party's honesty, dependability, reliability, and trustworthiness (Pavlou and Gefen 2004). We also control for demographic information since family status and gender have been previously shown to exert an influence on trust (Buchan et al. 2008; Gilbert and Tang 1998) as well as on the investment behavior (Barber and Odean 2001; Cohn et al. 1975).

5.2 Results

We recruited 118 undergraduate students on the university campus in order to participate in an investment experiment (cover story). We conducted the experiment in dedicated PC pools.

5.2.1 Descriptive Statistics

The average age of the students is 24 years, 88 out of the 118 participants are aged between 21 and 26. It should also be noted that the average income is rather low. The majority has a monthly income of EUR 900 or less. Only 2 participants are married, 61 participants live alone and 55 participants live in a relationship. These numbers are not very surprising due to the University background. On average, subjects invest EUR 6.07 into the fictional product of the bank.

While subjects in the control group, who were not confronted with any privacy or security incident, invest on average EUR 7.41 of their capital, this amount is reduced by EUR 1 (−16%) in case of a privacy violation and by EUR 3 (−39%) when a security breach leads to data theft. These numbers suggest that security breaches have a higher economic impact than privacy breaches. The following analysis will clarify the influence of both incidents on trust and the investment amount.

5.2.2 Model

With the following set of equations we tested our hypotheses.

$$\begin{aligned} Trust_i = {} & \alpha_1 + \beta_{11} \cdot Security_i \\ & + \beta_{12} \cdot Privacy_i \\ & + \beta_{13} \cdot FamilyStatus_i \\ & + \beta_{14} \cdot Gender_i + e_i \end{aligned} \quad (1)$$

$$\begin{aligned} IA_i = {} & \alpha_2 + \beta_{21} \cdot Security_i \\ & + \beta_{22} \cdot Privacy_i + \beta_{23} \cdot Trust_i \\ & + \beta_{24} \cdot FamilyStatus_i \\ & + \beta_{25} \cdot Gender_i + e_i \end{aligned} \quad (2)$$

where $Security_i$ is a dummy variable indicating whether a security breach occurred (1 = security breach, 0 otherwise); $Privacy_i$ is a dummy variable indicating whether a privacy breach occurred (1 = privacy breach, 0 otherwise); $Trust_i$ is the amount of trust of person i in the bank. IA_i is the investment amount that a person i is willing to invest into the bank. Subjects also provided information on family status (single = 1, in a relationship = 2, married = 3) as well as gender (1 = female; 2 = male).

We used seemingly unrelated regression analyses (SURE) as well as OLS in order to estimate the sets of Eqs. (1)

Table 2 Impact of security and privacy incidents on trust and investment behavior (SURE and OLS)

	Coefficient	Std. Error	t-Value	Coefficient	Std. Error	t-Value
Dependent variable: Trust in Bank						
	SURE			OLS		
α_1 (Constant)	5.07[a]	0.60	8.44	5.07[a]	0.61	8.26
β_{11} (Security breach)	−1.04[a]	0.29	−3.56	−1.04[a]	0.30	−3.48
β_{12} (Privacy breach)	−1.17[a]	0.29	−3.97	−1.17[a]	0.30	−3.88
β_{13} (Family status)	−0.08	0.23	−0.36	−0.08	0.23	−0.35
β_{14} (Gender)	−0.11	0.25	−0.44	−0.11	0.26	−0.43
Dependent variable: Investment amount						
	SURE			OLS		
α_2 (Constant)	1.64	1.77	0.93	1.64	1.81	0.91
β_{21} (Security breach)	−1.88[c]	0.72	−2.63	−1.88[b]	0.74	−2.56
β_{22} (Privacy breach)	−0.08	0.73	−0.11	−0.08	0.75	−0.11
β_{23} (Trust in bank)	0.95[c]	0.21	4.46	0.95[c]	0.22	4.34
β_{24} (Family status)	0.67	0.53	1.26	0.67	0.55	1.23
β_{25} (Gender)	0.14	0.58	0.24	0.14	0.60	0.23

[a] $p < 0.01$; Observations = 118; $R^2 = 0.14$

[b] $p < 0.05$; Observations = 118; $R^2 = 0.25$

[c] $p < 0.01$; Observations = 118; $R^2 = 0.25$

and (2). SURE method was introduced by Zellner (1962) for estimating regressions where disturbances correlate. In our case, trust as measured by the 7 item Likert scale is the dependent variable in Eq. (1) and is used as an independent variable in Eq. (2).

5.2.3 Results

The assumptions of the model are fulfilled. Problems with multicollinearity do not exist since all VIFs are below 4 (mean VIF Regression 1 on trust = 1.18; Regression 2 on investment amount = 1.24). The Breusch-Pagan test reveals that there is no heteroskedasticity so that we do not have to use robust standard errors.

As **Table 2** illustrates, both privacy and security incidents negatively affect the amount of trust in the bank, supporting H1a ($p < 0.01$) and H1b ($p < 0.01$). This is not very surprising and supports previous findings. However, our study allows the assessment of the impact of privacy and security incidents with respect to behavior and in monetary terms. First, we find that trust has a positive impact on behavior which supports hypothesis H3 ($p < 0.01$). We further observe that a security breach negatively influences the willingness to invest, supporting hypothesis H2a ($p < 0.01$). This result is interesting as it indicates that there is some additional latent influence of security breaches above and beyond the indirect influence through trust. Security breaches thus harm the relationship to the bank by lowering trust and above and beyond this impact there is some latent influence that additionally lowers the willingness to do business with this bank.

If we look at the impact of privacy violations on the investment amount, we do not observe a significant effect ($p > 0.1$). There is no direct influence of privacy violations on behavior besides the indirect effect through trust. We therefore have to reject H2b but we find support for H4 that privacy significantly exerts a stronger negative impact on trust (−1.17) than on the investment amount. This result empirically supports the privacy paradox, which means that privacy influences intentions and behavior differently. However, one has to remember that trust influences behavior (hypothesis H3) and privacy issues influence trust (hypothesis H1b) and therefore an indirect influence still exists.

5.3 Robustness Check

In order to test whether our sample of students is representative, we conducted a survey among the total population in Germany. Overall, 216 individuals took part in the nationwide survey. Our goal was to compare the privacy concerns as well as knowledge and experience of the students with the total population. We used the four dimensions of Smith's (Smith et al. 1996) instrument: errors, unauthorized secondary use, collection, and improper access. These dimensions contain privacy and security statements and subjects specify their agreement (e.g., "Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs") on a 7 point Likert scale. While the student sample has an average score of 5.597, privacy/security concerns of the total population have an average level of 5.573. These differences in concerns are statistically not significant (t-test, $p > 0.10$). Thus, results reveal that our students have the same level of privacy concerns as the total population.

We also collected information on the subjects' knowledge by asking whether subjects are aware of privacy and security risks and whether they have been a victim of a breach in the past (i.e., data theft). Results reveal a large amount of knowledge regarding privacy and security. Again, the t-test ($p > 0.10$) revealed no significant differences between both groups so that we can assume that

our sample of students is representative for studying the effect of privacy and security breaches on the investment behavior. While privacy concerns differ across countries (e.g., Dinev et al. 2006), they seem to be stable within one society. We therefore expect the same investment behavior of the total population, which is however subject to future research projects and cannot be finally clarified in this study.

6 Discussion

6.1 Summary

To the best of our knowledge, this is the first study quantifying the impact of privacy and security incidents by performing a laboratory experiment. While the general, indirect link between privacy, security, trust, and behavioral intention has been extensively studied in literature, the direct impact of privacy and security breaches has received less attention so far. Our results clearly reveal a first-order effect, that is, a direct consumer reaction to privacy and security incidents.

A surprising result at first sight is the stronger impact of the security breach on the investment amount. One explanation could be that people perceive their financial information as especially sensitive (Woodman et al. 1982) and therefore fear that criminals can get access to their data. With regard to the serious monetary consequences that can result from abuse of account passwords or credit card numbers, a bank customer might be primarily interested in the security of his personal data. Another reason might be that people already assume secondary use of information to some extent, since many cases of privacy violations have been reported in the press.

Thus, meanwhile, the transfer of personal information to another company might be perceived as unpleasant, but also as a conventional business practice that clearly lowers trust in the long-term but does not affect the real investment decision in the same way. For their investments people seem to be primarily interested in the competence of the bank, i.e. the ability to manage the money and to provide secure data systems. The experiment shows that privacy issues influence behavior only indirectly through trust while security issues influence behavior directly above the indirect influence through trust.

Our study therefore contributes to a better understanding of the privacy paradox which has been previously shown in the literature (Sect. 4). In contrast to previous research, we study consumer behavior after a privacy breach actually occurred. So far, intentions and behavior have only been compared in the absence of any privacy or security incident. Although privacy is of prime importance for building trust, we find that following a privacy breach, people still ignore their concerns when it comes to the actual investment decision. We can therefore conclude that a privacy breach lowers trust in the company but does not exert a direct influence on consumers' willingness to buy products from the affected company.

The consequences of these results for overall welfare can be illustrated by looking at the allocation of financial assets. In 2009, every German citizen held about EUR 16,628 of his/her capital in securities.[1] We can easily assume that the bank, that played the role model for our fictional bank, has a total of 15 million clients and around 400,000 new customers per year. These customers own securities worth approximately EUR 6.65 billion. A reduction of the investments by 39% (16%) would decrease the invested capital by EUR 2.59 (1.06) billion. If we assume an interest rate of 7%, this mistrust would cause a decrease of welfare by about EUR 182 million.

Recent data protection incidents show that companies around the world face enormous threats in this area. Every organization can easily become a target of cyber-attacks and data thefts. Hence, investment in security is required and this study introduces one method that allows assessing the expected monetary losses due to criminal activities which can be used to conduct costs-benefit analysis.

6.2 Limitations and Future Research

One limitation of our study is that the experiment was conducted in Germany, where data privacy is of a rather high value for the citizens compared to other countries (Singh and Hill 2003). This is also reflected by the stringent German laws, and one would expect that German consumers have high expectations with regard to data protection and get easily upset in case of privacy violations. This could lead to an overestimation of the impact of privacy violations.

There are already signs in the literature indicating differences in privacy concerns across societies. Bellman et al. (2004) found cultural values as an explanation for different levels of privacy concerns in 38 countries. Cho et al. (2009) showed that Internet users in Asia have less privacy concerns compared to western countries. According to Dinev et al. (2006), Italians have less privacy concerns than US citizens.

Cultural values also influence legislation. Milberg et al. (2000) found that the level of privacy concern exerts a positive influence on regulatory preferences for strong laws as well as government involvement. The authors conclude that "a universal regulatory approach to information privacy seems unlikely and would ignore cultural and societal differences." It is therefore possible that trust in the company is affected differently across countries, depending on laws and privacy concerns. Cross-cultural differences could be tested in future experimental studies.

Another avenue for future research is a further examination of the trust relationship between the company and the consumer. We focused on initial trust in this study as subjects in our sample had no prior experience with the bank and were only informed about the company by our instruction. In a long-term relationship, customers have multiple interactions and can develop trust based on their experiences with regard to the bank's service, reliability and overall behavior. Thus, future research can take these circumstances into account and focus on the reactions of existing investors to privacy and security problems.

In particular, there might be positive effects of security breaches on trust. Given that the bank makes great efforts to improve security measures, customers might perceive transactions with this bank as extremely secure. In our experiment, we informed subjects that the security breach occurred recently and that the CD is now circulating in the market place. Thus, the bank had probably not enough time to revise their security strategy. However, positive effects on trust might still be possible and can be specifically investigated in future research projects.

[1] Allianz Global Investors (2010).

We took a bank as an example to quantify the effects of privacy and security incidents. It would be interesting to compare the results with other industries, since customers usually express grave concerns about their bank data.

A further limitation, but similar to the original investment game setting of Berg et al. (1995), is the student sample. The impact of privacy and security breaches on the investment behavior might not be representative for the overall society. In our case, however, this limitation should not be severe as we are mainly interested in differences and not in absolute values. Moreover, the subjects in the sample are very likely to be important new customers and new investors in the near future.

Moreover, due to the results of our robustness check, we assume that our student sample is representative for the total population. We find evidence that privacy concerns do not differ across the society and we also observe the same privacy knowledge and experience. One can therefore expect the same investment behavior of the entire population when it comes to privacy and security incidents.

In sum, we are confident that our laboratory experiment is a good proxy for real behavior. The experiment allows a high level of control, which is very hard to realize in a field experiment or event studies. Furthermore, from a practical point of view, it appears rather unlikely to find a bank that is willing to simulate privacy or security breaches in order to conduct a field experiment.

We conclude that privacy and security breaches harm both the company as well as overall welfare. Further research in this area can help organizations to better understand the importance of data protection and the impact of security incidents and to take appropriate measures regarding the clients' protection with regards to privacy and security threats.

References

Ackerman M (2004) Privacy in pervasive environments: next generation labeling protocols. Personal and Ubiquitous Computing 8(6):430–439

Acquisti A, Friedman A, Telang R (2006) Is there a cost to privacy breaches? An event study. In: Proc 27th international conference on information systems, Milwaukee

Andoh-Baidoo FK, Amoako-Gyampah K, Osei-Bryson KM (2010) How Internet security breaches harm market value. IEEE Security and Privacy 8(1):36–42

Barber BM, Odean T (2001) Boys will be boys: gender, overconfidence, and common stock investment. Quarterly Journal of Economics 116(1):261–292

Belanger F, Hiller JS, Smith WJ (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. Journal of Strategic Information Systems 11(3-4):245–270

Bellman S, Johnson EJ, Kobrin SJ, Lohse GL (2004) International differences in information privacy concerns: a global survey of consumers. Information Society 20(5):313–324

Berendt B, Günther O, Spiekermann S (2005) Privacy in e-commerce: stated preferences vs. actual behavior. Communications of the ACM 48(4):101–106

Berg J, Dickhaut J, McCabe K (1995) Trust, reciprocity, and social history. Games and Economic Behavior 10(1):122–142

Bhattacherjee A (2002) Individual trust in online firms: scale development and initial test. Journal of Management Information Systems 19(1):211–241

Bilton N, Stelter B (2011) Sony says PlayStation hacker got personal data. http://www.nytimes.com/2011/04/27/technology/27playstation.html?_r=0. Accessed 2013-09-23

Bolle F (1998) Rewarding trust: an experimental study. Theory and Decision 45(1):83–98

Buchan NR, Croson RTA, Solnick S (2008) Trust and gender: an examination of behavior and beliefs in the investment game. Journal of Economic Behavior & Organization 68:466–476

Campbell JY, Lo AW, MacKinlay AC (1997) The econometrics of financial markets. Princeton University Press, Princeton

Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce 9(1):69–104

Childers TL, Houston MJ (1984) Conditions for a picture-superiority effect on consumer memory. Journal of Consumer Research 11(2):643–654

Cho H, Rivera-Sánchez M, Lim SS (2009) A multinational study on online privacy: global concerns and local responses. New Media & Society 11(3):395–416

Cohn RA, Lewellen WG, Lease RC, Schlarbaum GG (1975) Individual investor risk aversion and investment portfolio composition. Journal of Finance 30(2):605–620

Culnan MJ (1993) How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly 17(3):341–364

Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 10(1):104–115

Culnan MJ, Williams CC (2009) How ethics can enhance organizational privacy: lessons from the choice point and TJX data breaches. MIS Quarterly 33(4):673–687

De Bondt WFM, Thaler R (1985) Does the stock market overreact? Journal of Finance 40(3):793–805

Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Internet users' privacy concerns and beliefs about government surveillance: an exploratory study of differences between Italy and the United States. Journal of Global Information Management 14:4:57–93

Abstract

Michael Nofer, Oliver Hinz, Jan Muntermann, Heiko Roßnagel

The Economic Impact of Privacy Violations and Security Breaches

A Laboratory Experiment

Privacy and security incidents represent a serious threat for a company's business success. While previous research in this area mainly investigated second-order effects (e.g., capital market reactions to privacy or security incidents), this study focuses on first-order effects, that is, the direct consumer reaction. In a laboratory experiment, the authors distinguish between the impact of privacy violations and security breaches on the subjects' trust and behavior. They provide evidence for the so-called "privacy paradox" which describes that people's intentions, with regard to privacy, differ from their actual behavior. While privacy is of prime importance for building trust, the actual behavior is affected less and customers value security higher when it comes to actual decision making. According to the results, consumers' privacy related intention-behavior gap persists after the privacy breach occurred.

Keywords: Security, Privacy, Laboratory experiment, First-order effects

Dommeyer CJ, Gross BL (2003) What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of protection strategies. Journal of Interactive Marketing 17(2):34–51
Eastlick MA, Lotz SL, Warrington P (2006) Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment. Journal of Business Research 59(8):877–886
Forsythe R, Horowitz JL, Savin NE, Sefton M (1994) Fairness in simple bargaining experiments. Games and Economic Behavior 6(3):347–369
Foxman ER, Kilcoyne P (1993) Information technology, marketing practice, and consumer privacy: ethical issues. Journal of Public Policy & Marketing 12(1):106–119
Ganesan S (1994) Determinants of long-term orientation in buyer-seller relationships. Journal of Marketing 58(2):1–19
Gefen D (2000) E-commerce: the role of familiarity and trust. Omega 28(6):725–737
Gefen D, Karahanna E, Straub DW (2003) Trust and TAM in online shopping: an integrated model. MIS Quarterly 27(1):51–90
Gilbert JA, Tang TLP (1998) An examination of organizational trust antecedents. Public Personnel Management 27(3):321–338
Goodwin C (1991) Privacy: recognition of a consumer right. Journal of Public Policy & Marketing 10(1):149–166
Gorn GJ (1982) The effects of music in advertising on choice behavior: a classical conditioning approach. Journal of Marketing 46:94–101
Granovetter M (1985) Economic action and social structure: a theory of embeddedness. American Journal of Sociology 91(3):481–510
Greenaway KE, Chan YE (2005) Theoretical explanations for firms' information privacy behavior. Journal of the Association for Information Systems 6(6):171–198
Hinz O, Hann IH, Spann M (2011) Price discrimination in e-commerce? An examination of dynamic pricing in name-your-own-price markets. MIS Quarterly 35(1):81–98
Hosmer LT (1995) Trust: the connecting link between organizational theory and philosophical ethics. Academy of Management Review 20(2):379–403
John LK, Acquisti A, Loewenstein G (2011) Strangers on a plane: context-dependent willingness to divulge sensitive information. Journal of Consumer Research 37(5):858–873
Johnson EJ, Tversky A (1983) Affect, generalization, and the perception of risk. Journal of Personality and Social Psychology 45(1):20–31
Kalakota R, Whinston AB (1996) Frontiers of electronic commerce. Addison-Wesley, Reading
Kee HW, Knox RE (1970) Conceptual and methodological considerations in the study of trust and suspicion. Journal of Conflict Resolution 14(3):357–366
Kelly H (2013) Twitter hacked; 250,000 accounts affected. http://edition.cnn.com/2013/02/01/tech/social-media/twitter-hacked/index.html. Accessed 2013-09-23
Kim DJ, Ferrin DL, Raghav Rao H (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decision Support Systems 44(2):544–564
Liu C, Marchewka JT, Lu J, Yu C (2005) Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. Information & Management 42(1):289–304
Luo X, Li H, Zhang J, Shim JP (2010) Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. Decision Support Systems 49(2):222–234
MacKinlay AC (1997) Event studies in economics and finance. Journal of Economic Literature 35(1):13–39
Mayer RC, Davis JH, Schoorman FD (1995) An integrative model of organizational trust. Academy of Management Review 20(3):709–734
McKnight DH, Chervany NL (2001–2002) What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. International Journal of Electronic Commerce 6(2):35–59
McKnight DH, Cummings LL, Chervany NL (1998) Initial trust formation in new organizational relationships. Academy of Management Review 23(3):473–490
McKnight DH, Choudhury V, Kacmar C (2002) The impact of initial consumer trust on intentions to transact with a web site: a trust building model. Journal of Strategic Information Systems 11(3–4):297–323
Milberg SJ, Burke SJ, Smith HJ, Kallman EA (1995) Values, personal information, privacy and regulatory approaches. Communications of the ACM 38(12):65–74
Milberg SJ, Smith HJ, Burke SJ (2000) Information privacy: corporate management and national regulation. Organization Science 11(1):35–57
Milne GR, Boza ME (1999) Trust and concern in consumers' perceptions of marketing information management practices. Journal of Interactive Marketing 13(1):5–24
Morales L (2011) Google and Facebook users skew young, affluent, and educated. http://www.gallup.com/poll/146159/facebook-google-users-skew-young-affluent-educated.aspx. Accessed 2013-09-23
Norberg PA, Horne DR, Horne AA (2007) The privacy paradox: personal information disclosure intentions versus behaviors. The Journal of Consumer Affairs 41(1):100–126
Pavlou PA, Gefen D (2004) Building effective online marketplaces with institution-based trust. Information Systems Research 15(1):37–59
Phelps J (2000) Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing 19(1):27–41
Prosser WL (1960) Privacy. California Law Review 48(3):383–423
Rotter JB (1971) Generalized expectancies for interpersonal trust. American Psychologist 26(5):443–452
Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: a cross-discipline view of trust. Academy of Management Review 23(3):393–404
Schwartz N, Clore GL (1983) Mood, misattribution, and judgments of well-being: informative and directive functions of affective states. Journal of Personality and Social Psychology 45(3):513–523
Silveira V (2012) Taking steps to protect our members. http://blog.linkedin.com/2012/06/07/taking-steps-to-protect-our-members/. Accessed: 2013-09-23
Singh T, Hill ME (2003) Consumer privacy and the Internet in Europe: a view from Germany. Journal of Consumer Marketing 20(7):634–651
Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly 20(2):167–196
Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Quarterly 35(4):989–1015
Solove DJ (2006) A taxonomy of privacy. University of Pennsylvania Law Review 154(3):477–560
Spiekermann S, Grossklags J, Berendt B (2001) E-privacy in second generation e-commerce: privacy preferences versus actual behavior. In: Proc 3rd ACM conference on electronic commerce, New York
Statman M (1999) Behavioral finance: past battle and future engagements. Financial Analysts Journal 55(6):18–27
Straub DW, Collins RW (1990) Key information liability issues facing managers: software piracy, proprietary databases, and individual rights to privacy. MIS Quarterly 14(2):143–156
Suh B, Han I (2003) The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce 7(3):135–161
Tsai J, 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
Westin A (1967) Privacy and freedom. Atheneum Books, New York
Woodman RW, Ganster DC, Adams J, McCuddy MK, Tolchinsky PD, Fromkin H (1982) A survey of employee perceptions of information privacy in organizations. Academy of Management Journal 25(3):647–663
Yoon E, Guffey HJ, Kijewski V (1993) The effects of information and company reputation on intentions to buy a business service. Journal of Business Research 27(3):215–228
Zellner A (1962) An efficient method of estimating seemingly unrelated regressions and tests for aggregation bias. Journal of the American Statistical Association 57(298):348–368