Alma Mater Studiorum - Università di Bologna
DEPARTMENT OF ECONOMICS

Disclosure of Personal Information under Risk of Privacy Shocks

Francesco Feri
Caterina Giannetti
Nicola Jentzsch

Quaderni - Working Paper DSE N°875

Disclosure of Personal Information under Risk of Privacy Shocks

Franscesco FERI[1] Caterina GIANNETTI[2] Nicola JENTZSCH[3]

13th March 2013

Abstract

Companies are under an increasing pressure by policy makers to publicize data breaches. Such notification obligations require announcing the loss of personal data collected from customers, because of hacker attacks or other incidents. While notification is likely to impact on firms' reputation, we know little about the impact such notifications have on consumers with respect to disclosure of their personal data. We present the problem as a dynamic lottery with personal data under the risk of privacy shocks and experimentally study how the privacy breach notification changes an individual's behavior regarding data disclosure. Our results suggest that the notification induces individuals – disregarding the sensitivity of their data – to disclose more.

JEL-Classification: D43; L14; O30.

Keywords: Privacy, information sharing, data protection.

[1]Royal Holloway, University of London. Department of Economics. Email: francesco.feri@rhul.ac.uk

[2]*Email*: University of Bologna. Department of Economics. Email: caterina.giannetti@unibo.it

[3]Corresponding author: Deutsches Institut für Wirtschaftsforschung (DIW Berlin), Mohrenstrasse 58, 10117 Berlin, Germany, T. +49-(0)30-897-89-0, Fax +49-897-89-200, njentzsch@diw.de.

This research has benefited from discussions with a number of people. We would like to thank Alessandro Acquisti, Maria Bigoni, Laura Brandimarte, Pio Baake, Rainer Böhme, Paolo Crosetto, Alexia Gaudeul, Werner Güth, Kai-Lung Hui, Oliver Kirchkamp, Dorothea Kubler, Wieland Müller, Hans-Theo Normann, Sasha Romanosky, Volker Roth, Giancarlo Spagnolo and Georg Weizsäcker who provided valuable feedback. We would also like to thank seminar participants at the University of Bologna, University of Padua, DIW Berlin, Max Planck Institute of Jena, and ESA Conference 2012. We are deeply indebted to Dr. Rainer Metschke of the Data Protection Office of Berlin (in memoriam) for his support and helpful advise. Procedure Code of the Data Protection Officer of Berlin: 531.1068. Nicola Jentzsch acknowledges the funding under the Google Research Award for the project "Incentive-compatible Mechanism Design for Privacy".

1 Introduction

Companies collect an increasing amount of personal data on consumers, which arises as by-product in economic transactions. Personal details encompass payment behavior, preferences and lifestyle and are used for marketing purposes or risk assessment. Although many companies display privacy policies, data security remains imperfect and little is known about individuals' risk perceptions and trade-offs with respect to personal data. Privacy breaches are now reported on almost a daily basis. A report published in 2009 quoted a staggering number of 285 million consumer profiles compromised in 2008 in the financial and other industries (Verizon (2009)). Breaches range from stolen credit card or account numbers (Volks- and Raiffeisen-Banks and PostBank in Germany) to mobile phone numbers (T-mobile) or personal data posted on social networks (100 million FaceBook profiles stolen in 2010). Yet, individuals seem to not take the risk of a potential privacy breach into account when disclosing information. Under these circumstances, firms are under increasing pressure by policymakers to disclose data breaches that have occurred due to hacker attacks or other improper handling of personal information. Such notification obligations are creating a risk to company reputation, as they expose poor security practices. They also increase the costs of data collections for firms due to possible litigation and class action and increase costs of security bureaucracy, as consumers have to be notified about potential breaches. These costs aside, there are direct costs of data breaches that firms have to cover.[1] Since 2002, data breach notification laws have been enacted in an increasing number of states, of which some (such as California) consider an expansion of obligations.[2] In the U.S., there is a heated debate, whether such notifications are necessary and reach their intended effect. Critics argue that notification obligations might impose unnecessary costs for both firms and consumers (see Romanosky et al. (2010)). For example, when the harm is low, unnecessary notification may desensitize individuals, preventing them from acting when a serious threat exists. An increasing number of notifications lead consumers to become numb: "Notification letters are being sent so frequently, consumers are almost becoming immune to the daily announcements that personal information has been breached" (Kobus (2011)).[3] In Europe, the European Commission introduced with the E-privacy Directive a notification obligation for telecom and Internet Service Providers in 2009. Firms have to notify individuals about security breaches, if the breach could adversely affect them by resulting in identity theft, fraud, physical harm, humiliation

[1] A study in the U.S. puts the organizational costs of data breaches at about USD 5.5 million, see 2011 Cost of Data Breach Study: United States, see Press Release, https://www.symantec.com/about/news/release/article.jsp?prid=20120320_02

[2] A list is provided here: State Data Breach Notification Laws, http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf

[3] There is also an expert discussion on the effectiveness presented in Wired, http://www.wired.com/threatlevel/2009/03/experts-debate/

or damage to reputation. The latter is interesting insofar as the psychological impact of privacy breaches are explicitly mentioned. It is now discussed at the EU level to expand the scope to all sectors (including financial services). A recent report by the European Network and Information Security Agency (ENISA (2011)) discusses the situation in Europe and gives examples such as Germany, United Kingdom or Spain that have introduced data breach notifications in their legislations.

This context motivates our research: Our main objective is to investigate how data breach notifications affect an individual's transaction behavior with respect to sensitive personal data. To the knowledge of the authors, there are no experimental studies in this area, especially, where personal data are affected. Therefore, our main contribution is to provide basic insights into the interaction of breach notification and individual disclosure behavior.

We present the problem as a dynamic lottery with personal information for which we synthetically generate sensitive personal data in the laboratory in form of the results of a logic test, which is similar to an intelligence test. The test result is connected to the real name of the participant. Thus, we intentionally introduce identification in order to create personal information. Identification of the individual creates the privacy concern, which does not exist if aliases are used. In our context, test results constitute sensitive information, because participants receive a dichotomous private signal of their type that is whether their test result is above or below the median of the group. Participants (i.e. "consumers") can then trade anonymously with firms or may choose to disclose this information (and identify themselves) in order to obtain a discount for a voucher sold to them. At the end of each period, chance determines for each consumer-firm pair if there is a *privacy breach* at the firm, meaning that the information of the consumer (name and test result) are potentially in danger to be revealed to the other participants at the end of the experiment. At the end of the experiment, chance will once again determine, whether there is *privacy shock* and therefore the revelation of the information to the audience in lab.

Our experiment considers two environments: one in which participants are informed at the end of each period about the realization (or not) of a privacy breach at the firm they dealt with (i.e. Notification treatment), and one in which participants are not informed about privacy breach (i.e. No Notification treatment). Derived from our model, we theoretically predict that good types (i.e. individuals above the median) will choose to disclose an optimal number of periods greater than bad types. Theory also predicts that the introduction of a data breach notification renders no differences between treatments in terms of data disclosure. This means that notification does not change probabilities with which individuals are 'hit' by a breach and therefore should not affect their behavior. Intuition, however, would suggest that notification will make consumers more sensitive – due to a salience effect – to the revelation of their private information, especially bad types will experience a greater impact compared

to good types.

Our results suggest that even though below-median individuals tend to disclose less personal information compared to above-medians, an indication for the sensitivity of the information, the notification of a privacy breach has not a statistically differential effect with respect to the type of individuals. In fact, our results suggest a significant reaction (in terms of disclosing more) for both types of individuals after receiving a privacy breach message. No significant effects arise from receiving a message that no breach has occurred. A possible explanation for this behavior is that individuals – contrary to the explained probabilities in the experiment about which the participants were fully informed – feel their information is already lost ('loss fallacy'). Another explanation is that they become numb to the notification as soon as they received one and as a consequence it does not influence their behavior in the theoretically expected way. As there is a difference in disclosure behavior between good and bad types, we cannot say that the personal data synthetically generated in the experiment is not sensitive and renders notifications are meaningless.

A caveat of our research, which we should state at the outset, is that we cannot use real financial or health data due to the exposure risks of laboratory participants. For example, participants could use compromised credit card data for malign purposes. However, our approach creates sensitive information in an academic environment. We regard this as basic research and caution against reading too much into the results from a policy perspective. Our results are more insightful for firms in aligning their competitive strategies. For example, notifications raise awareness of consumers with respect to data security issues, they affect trust in firms and might turn into a competitive disadvantage if there are ongoing security issues in a firm. However, if consumers are numb to notifications and do not change their disclosure behavior, no competitive disadvantage would arise.

2 Experimental Analyses of Privacy

Our research is located at the intersection of economics and psychology. It therefore draws on different literature strands. It is related to experimental economics, because it is the first work on a dynamic lottery with personal information. In fact persons reveal on a daily basis their personal data on the Internet and in other contexts, without the knowledge of probabilities with which their information might be compromised. It draws on game theory, because we use an incentive-compatible mechanism, which ensures truth-telling about personal information: our participants cannot lie about their name and test result or employ another strategy such as using aliases. We purposefully introduce identification, as there is no other way to create personal information linked to the natural identity of a person. Information

that is not linked to the natural identity will not be personal and not raise privacy concerns.[4] In this respect, it is also related to psychology, because of the social comparisons that we introduce as well as the privacy concerns analyzed.

Traditional experiments are devoted to situations where players act anonymously. Identification as a structural variable, however, activates emotions such as sympathy or fear and can therefore change the results predicted by theory (Camerer (2011)). An exploration of such a change is provided by Frey and Bohnet (1997), where identification is introduced in one-shot and repeated Dictator and Prisoner's Dilemma games. In these games identification has psychologically binding effects without being a constraint though. One-way identification in Dictator games results in less zero-sums devoted by the dictator to the receiver than predicted (Bohnet and Frey (1999)). In a field experiment, Jenni and Loewenstein (1997) show that people would spent more resources to 'save' identified individual victims compared to a statistical number of unidentified victims, because identification induces sympathy. In Charness and Gneezy (2008), identity is introduced in Dictator and Ultimatum games, where in the former a larger share is devoted, but in the latter strategic considerations crowd out 'identification effects.' We introduce the act of identification into a dynamic lottery, which is typically played with anonymous players. The novelty in our research is that persons' bet is not money, but with their personal data.

Our research is also related to Bohnet and Zeckhauser (2004) and Fehr and Schmidt (1999). In the former article, it is shown that a risky bet with a result due to chance induces more risky behavior, whereas a trust decision entailing the risk of betrayal by a fellow participant induces less risky behavior. Trust entails additional costs for individuals. This insight is linked to our experiment, where players are confronted with risky decisions in an environment of potential privacy shocks subject to chance and not trust. Individuals are informed about the risk with which their information is compromised.

In Fehr and Schmidt (1999), it is discussed that people might be subject to inequity aversion. The authors show that there are subjects who dislike inequitable outcomes and experience inequity if they are worse off in material terms than the other players. It is discussed that there are persons who dislike inequitable outcomes. Inequity is experienced if they are materially worse off than the other players. We endow our players with private information about their type (their performance compared to the group's median), which renders them being 'unequal' and induces sensitivity about this inequality. Dhar and Wertenbroch (2010) explain there is a strategic preference for self-signaling, which our participants would achieve by disclosing information about their type, and there is evidence on the effects that such signaling has on utility, where self-signaling effects also derive from the context. We use

[4]This is the difference between personal and private information: personal information can be private or not, but it is linked to an identity. Private information must not be linked to an identity.

therefore an academic context (a University laboratory), students and subjects and the result of a logic test.

Further, our research is also related to salience as discussed in DellaVigna (2009). We introduce salience and connect it with notification by informing subjects if a breach has occurred or not. Without such notification, there is no salience, as individuals are not informed about the breach that occurred at the firm.

The aforementioned experiments aside, there is also a rising number of experimental works on privacy – all of which are one-shot games. We differ from these works by capturing the dynamics in decisions about personal information with a two-period setting and the cumulative risk associated with personal information being disclosed to multiple firms.

In Huberman et al. (2005) a reverse second price auction is introduced to obtain the private value for personal information, where they used weight and age of individuals for information sale. Our work is associated with this paper, as we obtained private valuation of the test result by implementing a reverse second price auction (for a different set of participants). From these auctions, we gained the approximate discount participants obtain for information revelation. In Huberman et al. (2005) the authors show that deviation from the group's mean asymmetrically impacts on the price demanded for the information. However, we find that neither age nor weight are entirely private information, both can be approximately derived by just looking at a person. There are a number of other papers, which we will not discuss in greater detail here due to the different methodological approach taken by them (Acquisti and Grossklags (2005) and Spiekermann et al. (2009)). These works, however, do not use an incentive-compatible mechanism.

We should mention Acquisti and Grossklags (2007) as their work inspired our research. The authors explored the gap between willingness-to-sell versus the willingness-to-protect personal information.[5] The authors generate a quiz score and ask their subjects about the price for which they are willing to sell their data. For those who sold, the information was announced to the group and individuals could leave the lab. The latter we introduce as well, but we also differ in several aspects. First, we introduce dynamics as a succession of decision tasks and we experiment with information of greater sensitivity by explicitly creating inequality among participants. We also introduce a probability of a privacy breach and a privacy shock, such that individuals are uncertain about whether information is disclosed at the end of the experiment.

There are also related field experiments. In Andrade and Weitz (2002) a web-survey is conducted on how companies may induce self-disclosure by individuals. They show that the reputation of a company and the display of a privacy policy induces disclosure, whereas the offer of a reward for the information reduces disclosure. In our experiment, the firms encoun-

[5]Individuals sell their information for some amount z, but are not willing to protect it for the same amount z.

tered induce information revelation by providing a discount for the data. In Beresford et al. (2012), the willingness-to-pay for privacy is explored. Participants were confronted with two identical stores that differed only in the information requested - where one shop requested more sensitive information. In the treatment where the prices of the stores were equal, individuals bought from both equally often, whereas in the treatment were prices differed, all chose the cheaper store, although it required more information disclosure. In our experiment, one firm is encountered per period, but they all request the same information. John et al. (2009) online experiments show that more control over the publication of personal data decreases the individuals' concerns and increases their willingness to disclose sensitive information. This is related insofar as our participants retain total control if they do not disclose information.

To summarize, we contribute to this literature in several important aspects. First of all, we introduce the act of identification into a dynamic lottery, which is typically played with anonymous players. Second, with respect to the other experiments on privacy, we produce sensitive information inside the laboratory and we explicitly create inequality among subjects in order to have information of greater sensitivity. More precisely, we endow our players with private information about their type (their performance compared to the group's median) which denotes them as 'unequal'. Finally, as explained in greater detail in the next section, in order to study the effect of a notification breach, we introduce a *privacy breach* and a *privacy shock*, such that individuals are uncertain about whether information is disclosed at the end of the experiment.

3 Personal Data Disclosure: Experimental Challenges

The core of the privacy problem is whether personal information is regarded as sensitive by the subjects involved, and whether its disclosure generates potentially adverse welfare effects for individuals or not. The legal definition states that personal information is "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*;" (Article 2(a), European Data Protection Directive of 1995). Evidence from Singapore, for example, shows that individuals seem to rank, in terms of sensitivity, credit cards numbers, contact details (telephone) and identification card numbers over employment, nationality and religion (Hui (2006)).

We decided to create information that is sensitive in the context of a university and students, and that cannot be used to materially damage the participants. In other contexts the information needed for sensitivity would differ, for example, in finance it would be credit card

numbers. More specifically, we decided to produce information in the form a result of a test score. Other researchers have implemented IQ tests in the laboratory as well (see Ariely and Norton (2005)).[6] This choice has several advantages. First of all, with this set-up we avoid working with data in the laboratory, which can be used outside of the laboratory for malign purposes. In addition, we can confront individuals in a dynamic lottery with the trade-offs of revealing their private information. This lottery differs from traditional ones where individuals can lose money, because our players can only lose private information when the information is leaked to "the public". Finally, as our experiment aims to capture the interaction between a primary transaction (on a market for a generic good) and the secondary transaction entailing a consumer's information, we let the students play this lottery, and trade this information, with computerized firms in the lab.[7]

Before presenting the experimental design in detail, however, two concepts must be defined: privacy breach and privacy shock.

Definition 1 *A privacy breach occurs when private and personal information stored in a firm is compromised, which may subsequently either be disclosed to the public or not.*

There are different origins of privacy breaches, which are attributable to human processes or system failures. Examples are security leaks, employee fraud or hacker attacks. A breach that occurred in a firm is not always disclosed to the public by the firm. It must be disclosed, however, if there is a legal notification obligation (the so-called data breach notification).

Definition 2 *A privacy shock is a sudden (unexpected) change in the distribution of private and personal information among market participants. In such a situation, information is revealed to third parties or otherwise used without the consent of the subject.*

In our setting, a privacy breach occurs when a firm is attacked during one of the transaction periods. This does not automatically mean personal data collected by the firm is disclosed to the public. However, in the case where it is disclosed to the public, i.e. to other participants in the experiment, we speak about a 'privacy shock.' The event of a shock is generated by the co-incidence of a *breach plus a random draw of a specific period* at the end of the experiment. This will be discussed in greater detail below.

[6] It must be noted that we do not work with a full-scale IQ test. These tests last more than an hour and the IQ results need to be calculated in a way related to the peer group. Therefore, we used only some questions from an IQ test and called explained to participants that they would encounter a logic test with questions similar to an IQ test.

[7] In our experiment, firms are not playing any decisive role in terms of choice to be made. We thus decided to use computerized firms, which do not involve trust issues. Moreover, involving humans on the other side of the market would have also given rise to tricky problems under the German data protection law, which we discussed with the Data Protection Officer in charge.

4 Experimental Design and Theoretical Predictions

In order to study the effect of a breach notification on the disclosure behaviour of individuals, we consider two treatments: one with *Notification* and one *No Notification*. In the treatment with notification participants are informed at the end of each period whether a privacy breach occurred or not at the firm they were dealing with, whereas in the treatment without notification participants do not receive any kind of message after they dealt with firms. In the following we explain more in detail the timing and the design of our experiment, along with a discussion on the theoretical predictions.

4.1 The Timing

In both treatments, at time 0, participants (i.e. consumers) undertake an *incentivized* logic test. They are then informed about the result of their test and how they performed compared to their peers. More specifically, they are privately informed on whether their score is above or below the median result of the group of participants in the experimental session. In period 1 and 2, participants take over the role of a consumer who encounters one (computerized) firm per period.[8] Firms sell a homogeneous good at price P, which is represented in this experiment by a voucher to be spent in a big store offering a wide range of DVDs, books, and CDs. Consumers have the option of selling their private information to the firm in order to obtain a discount d on the price of the voucher, to buy the voucher at full price, or to simply refuse any deals with the firm. Therefore, as long as the consumer does not disclose the information to any firms, the information remains private. The value of the discount, d, has been determined through several privacy auctions. These where reverse Vickrey auctions run with different participants, who could sell their information for a low ask price. We conducted these auctions to calibrate the discount. We additionally assume that the cost of disclosing the private information is equal to zero, even though consumers might have positive costs when disclosing information to a firm.[9]

At the end of the game, in both treatments, a privacy shock might realize for the consumer. In the lab, this shock is represented by the revelation of the information to the other participants in the session. A precondition for a privacy shock to occur at the end of the experiment is the realization of a privacy breach at the firm either in period 1 or 2. Thus, as already highlighted above, the difference between *privacy breach* and *privacy shock* is important in our context:

- **Privacy Breach.** There is a constant probability π in each period that data security

[8] Computerized firms are appropriate for the scope of the current experiment since our aim is to study consumers' behaviour in reaction of a breach notification.

[9] Consumers have positive costs related to disclosure when making an effort to type information into lengthy forms on a website, for example. Our forms were rather short.

in a firm is breached and $(1-\pi)$ that it is not breached. Even in the case where a consumer has sold his information, a privacy breach *does not automatically lead to public disclosure of personal information* (i.e. the privacy shock at the end).

- **Privacy Shock.** If a privacy breach occurs either in period 1 or 2, affected consumers will have the result of their test result revealed at the end of the experiment if and only if a random draw coincides with the period(s) in which consumers disclosed information. More precisely, such a shock only occurs in the co-incidence of the following events: the consumer has sold information either in period 1 or 2, in that very period a breach realized at the firm, and *exactly that period* is drawn at the end of the experiment.

Finally, the notification about the realization – or not – of the privacy breach only occurs in the treatment *with notification.*

To summarize, the timing of our experiment is

1. The test is undertaken at time 0. Participants are privately informed whether their score is above or below the median of the group.

2. In the first period, subjects can buy a voucher and sell their private information (i.e. their name and the test result) for a discount d. A privacy breach may occur with probability π (independent probability between subjects and periods). In the treatment *Notification,* participants are also informed whether a breach realized or not at the firm they dealt with.

3. In the second period, subjects can again buy a good and sell their private information for a discount d. A privacy breach may occur with probability π. In the treatment *Notification,* participants are once again informed whether a breach realized or not at the firm they dealt with.

4. At the end, a privacy shock may occur: for each subject, one period (1 or 2) is chosen at random (independently). If in the chosen period a privacy breach occurred, and the individual sold the private information, a privacy shock realizes: the personal information (i.e. the name and the test result) are revealed to the others.

4.2 Consumer Utility

Let $\tau_i \in \{v_{i,bad}, v_{i,good}\}$, where $v_{i,bad} \leq v_{i,good}$, be the value that the subject denoted by i attaches to the evaluation of his ability (in the test) by the others. That is, $v_{i,bad}(v_{i,good})$ is the value that he adds to his utility when others believe that his test was below (above) the median. In the following we consider the case where $v_{i,bad} = -v_{i,good} = 1$. By abuse of notation we denote by τ_i the type of the subject (-1 means that his test was below the median).

Let $s_{i,j} \in [0,1]$ be the probability by which subject *i* will sell or not the private information in period *j*. By $s_{i,j} = \{s_{i,1}, s_{i,2}\}$ we denote the strategy of individual *i*, by s_{-i} the set of strategies of all subjects different from *i* and by *s* the profile of strategy of all subjects. Let $b_i = b_i(s)$ denote the subject *i*'s second order beliefs about her type (*b* is the probability that $\tau_i = 1$). Beliefs are correct (rational) (Note, the value of *b* depends on the strategy chosen by all subjects).

Let $\beta_i \geq 0$ be a sensitivity parameter (of subject *i*) about the revelation of the private information and $\gamma_i \geq 0$ be a sensitivity parameter (of subject *i*) applied to the second order beliefs (i.e. beliefs on the beliefs that others have on the subject *i*).

Let $U_i(s_{i,}s_{-i}, \tau_i)$ be the individual *i*'s expected utility that depends on his strategy and the strategies used by others, then:

- $U_i(0,0,s_{-i},\tau_i) = \gamma_i b_i - \gamma_i(1-b_i)$
- $U_i(1,0,s_{-i},\tau_i) = U_i(0,1,s_{-i},\tau_i) = d + p_1\beta_i\tau_i + (1-p_1)(\gamma_i b_i - \gamma_i(1-b_i))$
- $U_i(1,1,s_{-i},\tau_i) = 2d + p_2\beta_i\tau_i + (1-p_2)(\gamma_i b_i - \gamma_i(1-b_i))$

where $p_1$is the probability of a privacy shock when the subject discloses the information only in one period, and p_2 is the probability of a privacy shock when the subject discloses the information in both periods. By denoting with $s_i\{x_1, x_2\}$a strategy where $x_{1,}x_2$are the probabilities to sell the private information in period 1, the probability of a privacy shock is given by

$$p(x_{1,}x_2) = ((1-x_1)x_2 + (1-x_2)x_1)\tfrac{\pi}{2} + \pi x_1 x_2$$

Hence, it directly follows that, when the subject sells the private information only in one period, the probability of a privacy shock is:

$$p_1 = \tfrac{\pi}{2}$$

and when the subject sells the private information in both periods the probability of a privacy shock is:

$$p_2 = \pi$$

4.3 Equilibrium Analysis

Now consider the simplest case where $\beta_i = \gamma_i = \beta$.

4.3.1 Treatment No Notification

In the treatment without notification, participants above the median (i.e. good types, $\tau_i = 1$) will always disclose their information, whereas participants below the median ($\tau_i = -1$) behave according to the following proposition:

Proposition (Equilibrium 1). It exists a Bayesian Nash Equilibrium where $s_i = \{1, 1\}$for all i with $\tau_i = 1$**.** For all i with $\tau_i = -1$

(a) Never disclose if $\pi\beta\frac{1-\pi}{2-\pi} \geq d,\ s_i = \{0, 0\}$

(b) Always disclose if if $\beta\frac{\pi}{2} < d,\ s_i = \{1, 1\}$

(c) Mix if $\pi\beta\frac{1-\pi}{2-\pi} < d < \beta\frac{\pi}{2},\ s_i = \{x_1, x_2\}$ when $d = \beta\frac{\pi}{2}\frac{2-2\pi}{2-\pi-p(x_1,x_2)}$

Proof. See Appendix.

4.3.2 Treatment with Notification

Participants in this treatment receive a message at the end of each period, which notifies them about the realization of a breach at the firm they dealt with. They can receive two types of message: *'A privacy breach has occurred*' in case the firm has been attacked, and the message '*No privacy breach has occurred*'. The presence of notifcation causes a larger set of strategies, because individuals can condition their action in the second period on the message they received. But this has no effect on the equilibrium actions because the probability to have the information (eventually) disclosed in the second period is independent from the realization in the first period of the privacy breach.

Proposition (Equilibrium 2).

With notification the equilibrium strategies are the same to those described in proposition 1.

Proof. See Appendix.

5 Experimental Results

The experiment was run between June and August 2012 at the Laboratory Technical University of Berlin, using z-Tree software (Fischbacher (2007)), and involving 228 participants for a total of 13 sessions. The average payoff was about 6 Euro in cash and 4 Euro in vouchers. Each session lasted for about one hour and did not start until all participants were familiar with the procedure. To ensure familiarity, we asked participants to solve various exercises.

We conducted the experiment for two environments (i.e., treatments *Notification* and *No Notification*). As explained above, in the treatment *Notification*, participants were informed about a privacy breach happened or not at the firms they dealt with, whereas in treatment *No Notification,* participants did not receive such a message.[10] However, in both treatments, at the end of the experiment, participants who sold their information to a firm, may experience a privacy shock, i.e. the revelation of the information to the other participants.

[10] A translation of the German instructions is available upon request.

5.1 Univariate Analysis

We are interested in studying the effect of the notification of a data breach on the disclosure behaviour of an individual. Thus, we focus on the number of periods individuals sold their data to a firm, during the experimental sessions. We identify: individuals who always disclosed their information, by means of a dummy variable *("Always Disclosed"*) equal to one if the participant sold the information to the firm in both periods of the game; individuals who never disclosed their information, by means of a dummy variable *("Never Disclosed"*) equal to one if the participant never sold the information during the experiment, and individuals who disclosed the information only once, by means of a dummy variable *("Disclosed Once"*) equal to one if the participant sold the information in one out of the two periods of the game. To see whether there is an effect, we first compare across treatments (*i.e. with* and *without* the notification message) the mean values of these dummy variables computed by keeping for each session their respective session averages. The results from these unpaired tests (in-between treatment comparisons subjects are not used as their own control) are reported in Table (2). The null hypothesis is that the two groups are drawn from two populations with the same mean (*TTEST*), median, and distribution (*MANN-WITHNEY*). In line with the theoretical predictions, all these tests seem to suggest that there is no treatment effect of the data notification breach, as all of them suggest to accept the null hypothesis. Similar conclusions are reached when comparing the results across individual types (not reported). However, when we compare these variables within the treatment sessions, distinguishing between the two types of message a subject received during the experiment (i.e. "*A breach has occurred*" and "*No breach has occurred*"), a strong and significant effect arises. Specifically, within treatments, we observe a highly and significant share of individuals who always disclosed the information after receiving the message that a breach has occurred.

5.2 Multivariate Analysis

To check the robustness of the previous results we perform a multivariate analysis that allows us to control for specific characteristics of individuals. We rely on an ordinal logit specification in which the dependent variable "*Disclose*" considers all the possibilities of information disclosure during the experiment, ranging from "*Never Disclosed*" to "*Always Disclose*d". In other words, we observe an individual disclosing k times the information (with $k = 0, 1, 2$) whenever the hypothetical number of times the participant is willing to disclose (the unobservable latent variable "Disclose*") does not pass a specific threshold c. In formula,

$$\begin{aligned}\Pr(Disclose = k) &= \Pr(c_k < Disclose^* \leq c_{k+1,}) = \Pr(c_k < x_i'\beta + u_i \leq c_{k+1,}) = \\ &= \Pr(c_k - x_i'\beta < u_i \leq c_{k+1,} - x_i'\beta) = F(c_{k+1} - x_i'\beta) - F(c_k - x_i'\beta)\end{aligned}$$

where u is logistic distributed with $F(z) = e^z/(1+e^z)$, the thresholds are assumed to be

strictly increasing ($c_k < c_{k+1} \forall k$), and $c_1 = -\infty$ and $c_{k+1} = \infty$.

The main specification includes the following variables among the regressors:

$$\beta_i' x = \beta_1 Below + \beta_2 Breach\, Message + \beta_{12} Below * Breach\, Message + \beta_3 No\, Breach\, Message + \beta_{13} No\, Breach\, Message * Below$$

where $Below$ is a dummy variable equal to one if the individual's results in the logic test was below the median and zero otherwise, $Breach\ Message$ is a dummy variable equal one if the individual received the message "A breach has occurred" and zero otherwise, and $No\ Breach\ Message$ is a dummy variable equal to one if the individual received the message "No breach has occurred" and zero otherwise. A full description of the other variables used in the analysis along with the main statistics is provided in Table (1).

The results for the estimated model are reported in Table (3), whereas the average of the marginal effects for the outcome "Always Disclosed" are reported in Table (4). The model is non-linear, therefore coefficients on the interaction terms (i.e. how the effect of one variable changes when the other variable in the interaction term changes), β_{12} and β_{13}, do not provide the change in the partial effect of the variables on the conditional mean function and care needs to be taken in the interpretation of the results (Ai and Norton (2003), Greene (2010), Karaca-Mandic et al. (2011)). In addition, in some cases, the results of hypothesis tests are an artifact of the functional form and do not necessarily have an economically meaningful content (Greene (2010)). Therefore, we report in Table (5) the estimated interaction effects, as well as marginal effects for specific groups.

In column *(a)* we start by adding as explanatory variables the dummy variable *Below,* which equals to one for those individuals whose performance in the logic test was below the median, and the dummy variable *Breach Message,* which is equal to one for those individuals who received, at the end of the first period, a message "A breach has occurred". As expected, individuals who were below the median tend to disclose less compared to individuals whose performance was above the median. This in fact accentuates that the information generated through the logic test is considered sensitive by those who scored below the median. To interpret these coefficients more easily (as well as the interaction terms) we can exponentiate them (Buis (2010)). The exponentiated coefficients (*odds ratio*) give the ratio by which the dependent variable changes for a unit change in an explanatory variable, that is: the effect of a unit increase of the independent variable on the probability of disclosing a higher number of times, while holding the other variables in the model constant. If the odds are greater than one disclosing the information is more likely to happen than not. If the odds are less than one then disclosing a higher number of times is less likely to happen. Related to the group of participants who were below the median, we expect to find 35% of participants who always disclose as we observe an odds ratio of 0.35 (i.e., exp(-1.062)). Similarly, we expected an odds

ratio that is 8.26 times higher among the participants who received the message "A breach has occurred". These results are robust across all specifications from columns *(b)* to (*l*) in which we progressively add various controls.

At this stage, it is important to underline that the ordinal logit makes a "parallel odds" assumption. That is, it assumes that only the cut-off parameters c_k is different across the changes in the number of periods participants disclose the information, whereas the slope coefficients of the link function (i.e. the parameters of interest) remain identical. This assumption may be inappropriate but can be tested through a likelihood ratio test. The results from this test supports the proportional odds assumption.

In column (*b*) we introduce the interaction term of the dummies *Below* and *Breach Message* to disentangle the effect of the message between the two types of participants (i.e. below or above the median). The interaction term is negative but not significant. The odds ratio is in this case 0.239 (i.e. exp(-1.432)), which means that the effect of the *Breach Message* on the number of periods, where below-median participants disclosed the information, is 0.239 times the effect of receiving such a message for above-median individuals. This effect is also clear in Table (5), where we report the average of marginal effects for different groups. In particular, we observe that the average marginal effects (i.e. the change in the probability of disclosing the information in a higher number of periods) after receiving the message "A breach has occurred" is higher for above-median participants in comparisons to below-median individuals (0.457 vs 0.311). However, the difference between the two groups (i.e. a difference-in-differences test), which is equal to the difference in the average of marginal effects (-0.143), and represents the interaction term, is not significant. This result, and the magnitude of these parameters, remains robust across the specifications from columns *(b)* to (*l*). We can thus conclude that, after receiving the message that a breach has occurred, individuals who performed poorly in the logic test will tend to disclose less than individuals who performed well, although this result is not statistically significant.

To disentangle the effect of the two types of messages the individuals received during the treatment sessions, we introduce in column *(c)* the dummy variable *No Breach Message,* which is equal to one for those individuals who received at the end of the of the first period the message "No breach has occurred". The coefficient on this variable is negative and individually not significant, meaning that individuals receiving a message "No breach has occurred" tend to disclose less. In this case, we expect an odds ratio of disclosing the information that is 0.80 times lower among the participants who received the message "No breach has occurred". The combined effect of this variable with the dummy *Breach Message,* which basically captures our treatment effect, is jointly significant at 5% level in all specifications but the last one (*l*), in which we include a dummy variable for each experimental session. However, when we look at the average across all individuals of marginal effects in Table (5), for both groups of par-

ticipants, we can conclude that the effect of this second type of message is never statistically significant.

We also explore for this type of message whether there is a different impact depending on the two types of individuals, by adding in column (*d*) an interaction term of the dummy variable *Below* with the dummy variable *No Breach Message*. In this case, the interaction term is negative. This means that below-median participants tended to disclose less compared to above-median participants, even after receiving this message. A reason could be that the No Breach Message primes them (once more after reading the instructions) on breaches that could occur. However in no cases, from columns *(*d) to (*l*), the differential effect of *No Breach Message* turned out to be significant.

From column (*e)* on, we start to add control variables which we collected at the end through a questionnaire at the of each experimental session. In column (*e)* we introduce a variable measuring the number of subjects known by each participant in the experimental session. We expected that the higher the number, the higher the privacy concern of participants, and therefore the lower the willingness to disclose the information. This result remains robust (i.e. about a 10% decrease in the probability of disclosing, see again Table (5)) and significant at 10% level across the various specification. In column (*f*) we include a variable that measures the privacy attitude of the participant relying on the well-known classification proposed in the past by Westin (Kumaraguru and Cranor (2005)), which distinguishes among 'privacy fundamentalists', 'privacy pragmatists' and 'privacy unconcerned'. This variable turns never out as significant. Results are substantially similar when we replace this variable with the traditional measure of risk aversion in unreported regressions (available upon request). These were derived from an incentivized lottery at the beginning of each experimental session. In a companion paper (Jentzsch and Giannetti (2012)), the Westin privacy types and the risk aversion turn out to be highly correlated. In column (*g*) we also include individual characteristics such as *Age*, *Height*, and sex (i.e. *Female*, a dummy variable equal to one for female), which are exogenous to our dependent variable. There is evidence that, in line with the experimental studies on risk aversion, individuals who are older tend to be less willing to take risks, reflected in disclosing less personal data. The overall effect of this group of variables, however, is not jointly significant. We include in column (*h*) dummy variables accounting for the level of education of participants' parents. The base category is a dummy variable equal to one if both parents have an *Abitur* (comparable to High-school diploma in the U.S.). These dummy variables are never significant, either alone or jointly. In column *(i)*, we additionally include a dummy variable equal to 1 if the individuals never accept cookies when using their computer.[11] Also in this case, this variable is significant, although only

[11]Cookie preferences map the individual's acceptance of being tracked on the Internet, which is related to privacy preferences.

at 10% level. Finally, in column *(l)* we include session dummies to the full specification in column (*i*). The results are robust to this last control.

We conclude that even though below-median individuals tend to disclose less personally sensitive data, the breach notification has no statistically differential effect with respect to the type of individual. This is in line with the decision model presented herein if the discount is large enough to compensate below-median individuals. In addition, we can observe a significant rise in disclosure for both types of individuals after receiving the message that a privacy breach happened. This is an unexpected result, which is rather surprising. Intuition would hold that bad types disclose less after receiving the message due to the salience effect. No significant effect arises from receiving a message that no breach has occurred, though.

6 Conclusions

We investigate the effect of a breach notification on consumer behavior with respect to disclosing personal data to firms in an economic transaction. We admit that our experiment is stylized, but a more real setting with financial information or health information was not feasible under the circumstances that we were eager to produce real personal data connected to the natural identity of the person in the laboratory. We have two key results. The first is in line with our expectations. Individuals that pass a social comparison with negative result tend to disclose this information a lower number of times compared to their peers. The second is that once individuals receive a breach notification, they tend to disclose more. This is an unexpected result, but in line with observations in the real world. Breach notifications do not drive consumers in masses away from firms. They seem to not reduce identity theft and they rarely result in such theft. It also seems that consumers ignore these notification messages. Consumers who do not change their behavior in the expected way do not discipline companies that are negligent with their personal data. If persons become increasingly numb to notifications, no competitive disadvantage from frequent breach notifications arises for firms – which is at the very core of this policy measure. We are aware that there is no straight generalization of results gained from an experiment with students and employees at a Technical University to consumers in general. Therefore, we regard our research more as qualitative evidence, which needs further backing by field experiments.

References

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. Security & Privacy, IEEE 3 (1), 26–33.

Acquisti, A., Grossklags, J., 2007. When 25 cents is enough: Willingness to pay and willingness to accept for personal information. In: Workshop on the Economics of Information Security (WEIS).

Ai, C., Norton, E., 2003. Interaction terms in logit and probit models. Economics letters 80 (1), 123–129.

Andrade, E., Weitz, B., 2002. Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. Advances in Consumer Research (Volume 29) 1, 351.

Ariely, D., Norton, M., 2005. Self-deception: How we come to believe we are better than we truly are. Working Paper, Sloan School of Management, MIT.

Beresford, A., Kübler, D., Preibusch, S., 2012. Unwillingness to pay for privacy: A field experiment. Economics Letters.

Bohnet, I., Frey, B., 1999. The sound of silence in prisoner's dilemma and dictator games. Journal of Economic Behavior & Organization 38 (1), 43–57.

Bohnet, I., Zeckhauser, R., 2004. Trust, risk and betrayal. Journal of Economic Behavior & Organization 55 (4), 467–484.

Buis, M., 2010. Stata tip 87: Interpretation of interactions in non-linear models. The Stata Journal 10 (2), 305–308.

Camerer, C., 2011. Behavioral game theory: Experiments in strategic interaction. Princeton University Press.

Charness, G., Gneezy, U., 2008. What's in a name? anonymity and social distance in dictator and ultimatum games. Journal of Economic Behavior & Organization 68 (1), 29–35.

ENISA, 2011. Data breach notifications in the eu, report.
URL http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn

Fehr, E., Schmidt, K., 1999. A theory of fairness, competition, and cooperation. The quarterly journal of economics 114 (3), 817–868.

Fischbacher, U., 2007. z-tree: Zurich toolbox for ready-made economic experiments. Experimental Economics 10, 171–178.

Frey, B., Bohnet, I., 1997. Identification in democratic society. Journal of Socio-Economics 26 (1), 25–38.

Greene, W., 2010. Testing hypotheses about interaction terms in nonlinear models. Economics Letters 107 (2), 291–296.

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

Hui, K., 2006. Consumer disclosure: the effects of company information presentation and question sequence. Unpublished manuscript, Department of Information Systems, National University of Singapore.

Jenni, K., Loewenstein, G., 1997. Explaining the identifiable victim effect. Journal of Risk and Uncertainty 14 (3), 235–257.

John, L., Acquisti, A., Loewenstein, G., 2009. The best of strangers: Context dependent willingness to divulge personal information. Available at SSRN 1430482.

Karaca-Mandic, P., Norton, E., Dowd, B., 2011. Interaction terms in nonlinear models. Health Services Research 47 (1pt1), 255–274.

Kobus, T., 2011. Data breach response: a year in review.
URL http://www.lexology.com/library/detail.aspx?g=0ae1065c-8cea-4a03-b97e-ca8cb2209017

Kumaraguru, P., Cranor, L., 2005. Privacy indexes: A survey of westin's studies.

Romanosky, S., Acquisti, A., Sharp, R., 2010. Data breaches and identity theft: When is mandatory disclosure optimal? TPRC.

Spiekermann, S., Berendt, B., Grossklags, J., 2009. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. Available at SSRN 761107.

Verizon, 2009. 2009 data breach investigations report. Verizon Business Risk Team.
URL resources/security/reports/2009_databreach_rp.pdf

A Appendix

Proof (Equilibrium 1). The result for individuals i with $\tau_i = 1$directly follows by the consideration that their utility is increasing in the probability of privacy shock. Then $s_i = \{1, 1\}$ is increasing in the probability of privacy shock. Then $s_i = \{1, 1\}$is a dominant strategy**.**

Case a) the subject *i*'s second order belief when his private information is not revealed at the end is:

$$b_i = \tfrac{1-\pi}{2-\pi}$$

Therefore the subject *i*'s utility can be written as:

- $U_i(0, 0, \bar{s}_{-i}, \tau_i) = \beta(\frac{1-\pi}{2-\pi} - \frac{1}{2-\pi}) = \beta(\frac{-\pi}{2-\pi})$
- $U_i(1, 0, \bar{s}_{-i}, \tau_i) = U_i(0, 1, s_{-i}, \tau_i) = d - \beta\frac{\pi}{2} + (1 - \frac{\pi}{2})\beta(\frac{-\pi}{2-\pi})$
- $U_i(1, 1, \bar{s}_{-i}, \tau_i) = 2d - \pi\beta + (1 - \pi)\beta(\frac{-\pi}{2-\pi})$

where $\bar{s}_{-i}$ denote the equibrium strategy of all other subjects.

Equilibrium conditions are:

1. $U_i(0, 0, \bar{s}_{-i}, \tau_i) \geq U_i(1, 0, \bar{s}_{-i}, \tau_i)$
2. $U_i(0, 0, \bar{s}_{-i}, \tau_i) \geq U_i(0, 1, \bar{s}_{-i}, \tau_i)$
3. $U_i(0, 0, \bar{s}_{-i}, \tau_i) \geq U_i(1, 1, \bar{s}_{-i}, \tau_i)$

These conditions are:

$\beta(\frac{-\pi}{2-\pi}) \geq d - \beta\frac{\pi}{2} + (1 - \frac{\pi}{2})\beta(\frac{-\pi}{2-\pi})$ (from 1 and 2)
$\beta(\frac{-\pi}{2-\pi}) \geq 2d - \pi\beta + (1 - \pi)\beta(\frac{-\pi}{2-\pi})$ (from 3)
Using some algebra we get:
$\pi\beta\frac{1-\pi}{2-\pi} \geq d$
$\pi\beta\frac{1-\pi}{2-\pi} \geq d$

Case b) the subject i's second order belief when his private information is not revealed at the end is:

$$b_i = \tfrac{1}{2}$$

Therefore the subject *i*'s utility can be written as

1. $U_i(0, 0, \bar{s}_{-i}, \tau_i) = 0$
2. $U_i(0, 0, \bar{s}_{-i}, \tau_i) = U_i(0, 1, \bar{s}_{-i}, \tau_i) = d - \frac{\pi}{2}\beta$
3. $U_i(0, 0, \bar{s}_{-i}, \tau_i) = 2d - \pi\beta$

Equilibrium conditions are:

1. $U_i(1,1,\bar{s}_{-i},\tau_i) \geq U_i(1,0,\bar{s}_{-i},\tau_i)$
2. $U_i(1,1,\bar{s}_{-i},\tau_i) \geq U_i(0,1,\bar{s}_{-i},\tau_i)$
3. $U_i(1,1,\bar{s}_{-i},\tau_i) \geq U_i(0,0,\bar{s}_{-i},\tau_i)$

These conditions are:

$2d - \pi\beta \geq d - \frac{\pi}{2}\beta$ (from 1 and 2 when $\tau_i = -1$)

$2d - \pi\beta \geq 0$ (from 3 when $\tau_i = -1$)

Using some algebra we get:

$d \geq \beta\frac{\pi}{2}$

$d \geq \beta\frac{\pi}{2}$

Case c) the subject i's second order belief when his private information is not revealed at the end is:

$$b_i = \frac{1-2\pi}{2-\pi-p(x_1,x_2)}$$

Therefore the subject *i*'s utility can be written as

1. $U_i(0,0,\bar{s}_{-i},\tau_i) = \beta(\frac{s-\pi}{2-\pi-p(x_1,x_2)})$
2. $U_i(1,0,\bar{s}_{-i},\tau_i) = U_i(0,1,\bar{s}_{-i},\tau_i) = d - \frac{\pi}{2}\beta + (1-\frac{\pi}{2})\beta(\frac{s-\pi}{2-\pi-p(x_1,x_2)})$
3. $U_i(0,0,\bar{s}_{-i},\tau_i) = 2d - \pi\beta + (1-\pi)\beta(\frac{s-\pi}{2-\pi-p(x_1,x_2)})$

In equilibrium we have $U_i(1,1,\bar{s}_{-i},\tau_i) = U_i(1,0,\bar{s}_{-i},\tau_i) = U_i(0,1,\bar{s}_{-i},\tau_i) = U_i(0,0,\bar{s}_{-i},\tau_i)$. Replacing the utilities and solving the equalities we get the result.

Proof (Equilibrium 2). We compute the incentive to sell information in the second period given a generic strategy $(s_{i,1}, s_{i,2})$ and in the case that in period 1 the information was sold. We consider two cases: *a)* a privacy breach has occurred and *b)* no privacy breach has occurred. By $u(1)$ denote the expected utility deriving from selling the information in period 2 and by $u(0)$the expected utility deriving from no to sell the info.

Case *a)*. In this case, when the individual receives the message "*a privacy breach has occurred*" he know that a privacy shock can happen to the information revealed in period 1 by probability $\frac{1}{2}$. Then $u(1) = 2d - \frac{1+\pi}{2}\beta + \frac{1-\pi}{2}(2b_i - 1)\beta$ and $u(0) = d - \frac{1}{2}\beta + \frac{1}{2}(2b_i - 1)\beta$. The incentives to sell the information in period 2 are: $u(1) - u(0) = d - \pi\beta b_i$. Case *b)*. In this case, when the individual receives the message "*no privacy breach has occurred*" he know that a privacy shock cannot happen to the information revealed in period 1. Then $u(1) = 2d - \frac{\pi}{2}\beta + (1-\frac{\pi}{2})(2b_i - 1)\beta$ and $u(0) = d + (2b_i - 1)\beta$. The incentives to sell the information in period 2 are: $u(1) - u(0) = d - \pi\beta b_i$. Then the incentive to sell information in period two are independent from the type of notification and are equal to the case *No*

Notification. In similar way we find that the incentives to sel information in period 1 are equal to those in the case *No Notification*. Directly follows that equilibria are the same to those on the case *No Notification*. QED.

Table 1: VARIABLE DESCRIPTION

Variable Name	Description	Mean	Std. Dev.	Min.	Max.	N
Disclose	Categorical variable equal to 0 if the subject never disclosed the information, to 1 if the subject disclosed the information once, and 2 if the subject disclosed twice the information during the experiment.	0.917	0.956	0	2	228
Below	Dummy variable equal to 1 if the subject is below the median result of the logical test in the experimental session.	0.43	0.496	0	1	228
Message Breach	Dummy equal to 1 if the subject received the message "A breach has occured" in the treatment session.	0.079	0.27	0	1	228
Message No Breach	Dummy equal to 1 if the subject received the message "No breach has occured" in the treatment session.	0.364	0.482	0	1	228
# Known Participants	Variable measuring the number of known participants by the subject in the experimantal session.	0.184	0.532	0	3	228
Privacy Aversion	Variable measuring the degree of privacy aversion of the subject (see ...)	2.596	0.492	2	3	228
Age	Categorical variable measuring the age of the subject in the experimental session.	2.083	0.899	1	4	228
Height	Categorical variable measuring the height of the subject in the experimental session.	2.447	0.557	1	3	226
Female	Dummy variable equal to 1 if the subject in the experimental session was a female.	0.39	0.489	0	1	228
Parents No Abitur	Dummy variable equal to 1 if none of the subject's partents has an Abitur.	0.241	0.429	0	1	228
One Parents Abitur	Dummy variable equal to 1 if one of the subject's partents has an Abitur.	0.368	0.483	0	1	228
Never Accept Cookies	Dummy variable equal to 1 if it the subject declared to never accept cookies on the computer.	0.329	0.471	0	1	228

Table 2: AVERAGE RESULTS ACROSS TREATMENTS

Never disclosed is defined as a dummy variable equal to one if the subject never disclosed the information during the experiment, **Disclosed Once** is defined as a dummy variable equal to one if the subject disclosed the information in one out of two periods during the experiment, and **Always Disclosed** is defined as a dummy variable equal to one if the subject always disclosed the information in the two periods of the experiment.

Between Treatment

	No Notification	*Notification*	TTEST	MANN-WITHNEY	MEDIAN
Never Disclosed	0.52	0.46	0.227	0.227	0.571
Disclosed Once	0.06	0.09	0.165	0.165	0.286
Always Disclosed	0.42	0.46	0.346	0.346	0.476

Within Treatment

	Message Breach	Message No Brech	TTEST	MANN-WITHNEY	MEDIAN
Never Disclosed	0	0.58	0.000	0.000	0.000
Disclosed Once	0.17	0.10	0.195	0.388	0.652
Always Disclosed	0.83	0.33	0.000	0.000	0.000

Table 3: ORDINAL LOGIT "DISCLOSE"

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
Below	-1.0619***	-1.0000***	-0.9928***	-0.8301**	-0.8975**	-0.9065**	-0.9529**	-0.9682**	-0.9953**	-1.0499***
	(0.277)	(0.283)	(0.284)	(0.367)	(0.369)	(0.371)	(0.384)	(0.384)	(0.387)	(0.402)
Breach Message	2.1111***	2.7709***	2.6644***	2.7330***	2.7400***	2.7374***	2.7237***	2.7222***	2.8439***	2.1669**
	(0.496)	(0.999)	(1.007)	(1.012)	(0.961)	(0.955)	(0.911)	(0.908)	(0.850)	(0.932)
*Below * Breach Message*		-1.4321	-1.4398	-1.6027	-1.6393	-1.6304	-1.5999	-1.5923	-1.3484	-1.3164
		(1.121)	(1.121)	(1.145)	(1.098)	(1.100)	(1.073)	(1.106)	(1.076)	(1.127)
No Breach Message			-0.2773	-0.1006	-0.0857	-0.0798	-0.1011	-0.1247	-0.1480	-0.6758
			(0.285)	(0.384)	(0.389)	(0.389)	(0.395)	(0.403)	(0.410)	(0.595)
*Below * No Breach Message*				-0.4194	-0.3288	-0.3352	-0.3650	-0.3664	-0.2705	-0.3198
				(0.579)	(0.587)	(0.587)	(0.596)	(0.600)	(0.612)	(0.635)
# Known Participants					-0.4971*	-0.4983*	-0.5086*	-0.5030*	-0.5676*	-0.5771*
					(0.283)	(0.282)	(0.293)	(0.292)	(0.294)	(0.331)
Privacy Attitude						-0.1094	-0.0801	-0.1063	-0.0797	-0.0067
						(0.285)	(0.289)	(0.293)	(0.294)	(0.314)
Age							-0.2623*	-0.2802*	-0.2898*	-0.2848*
							(0.159)	(0.164)	(0.164)	(0.167)
Height							-0.3011	-0.3060	-0.3595	-0.4236
							(0.266)	(0.266)	(0.272)	(0.280)
Female							-0.3029	-0.3058	-0.3069	-0.3408
							(0.305)	(0.305)	(0.302)	(0.314)
Parents No Abitur								0.1387	0.1089	-0.0411
								(0.358)	(0.364)	(0.402)
One Parents Abitur								-0.0977	-0.1796	-0.3461
								(0.348)	(0.351)	(0.358)
Never Accept Cookies									-0.5759*	-0.4810
									(0.311)	(0.341)
Session Dummies	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*Yes*
Cut 1	-0.3270*	-0.3012	-0.4091*	-0.3411	-0.4409*	-0.7289	-2.1014*	-2.2342*	-2.5463**	-3.0545**
	(0.193)	(0.195)	(0.229)	(0.251)	(0.257)	(0.800)	(1.167)	(1.225)	(1.230)	(1.296)
Cut 2	0.0572	0.0834	-0.0230	0.0456	-0.0496	-0.3373	-1.7006	-1.8328	-2.1400*	-2.6297**
	(0.190)	(0.193)	(0.226)	(0.248)	(0.255)	(0.799)	(1.161)	(1.217)	(1.223)	(1.291)
Log likelihood	-193	-192	-192	-191	-190	-190	-186	-186	-184	-179
N	228	228	228	228	228	228	226	226	226	226

*p<0.10,** p<0.05, ***p<0.01

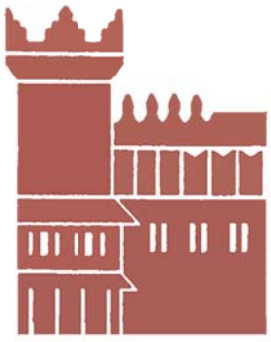
Table 4: AVERAGE MARGINAL EFFECTS: OUTCOME "ALWAYS DISCLOSE"

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
Below	-0.2257***	-0.2379***	-0.2358***	-0.2343***	-0.2402***	-0.2423***	-0.2489***	-0.2515***	-0.2428***	-0.2453***
	(0.053)	(0.058)	(0.058)	(0.058)	(0.058)	(0.058)	(0.059)	(0.058)	(0.059)	(0.060)
Breach Message	0.4487***	0.3942***	0.3759***	0.3686***	0.3629***	0.3632***	0.3601***	0.3606***	0.3978***	0.2900***
	(0.099)	(0.065)	(0.070)	(0.070)	(0.069)	(0.070)	(0.069)	(0.071)	(0.068)	(0.103)
No Breach Message			-0.0585	-0.0546	-0.0441	-0.0434	-0.0494	-0.0542	-0.0509	-0.1511
			(0.060)	(0.060)	(0.061)	(0.061)	(0.061)	(0.062)	(0.062)	(0.097)
# Known Participants					-0.1036*	-0.1038*	-0.1045*	-0.1032*	-0.1151**	-0.1118*
					(0.058)	(0.058)	(0.059)	(0.059)	(0.059)	(0.063)
Privacy Attitude						-0.0228	-0.0165	-0.0218	-0.0162	-0.0013
						(0.059)	(0.059)	(0.060)	(0.060)	(0.061)
Age							-0.0539*	-0.0575*	-0.0588*	-0.0552*
							(0.032)	(0.033)	(0.033)	(0.032)
Height							-0.0619	-0.0628	-0.0729	-0.0820
							(0.054)	(0.054)	(0.055)	(0.054)
Female							-0.0622	-0.0627	-0.0623	-0.0660
							(0.062)	(0.062)	(0.061)	(0.060)
Parents No Abitur								0.0287	0.0223	-0.0080
								(0.074)	(0.075)	(0.078)
One Parents Abitur								-0.0199	-0.0360	-0.0661
								(0.071)	(0.070)	(0.068)
Never Accept Cookies									-0.1168*	-0.0931
									(0.062)	(0.065)
Session Dummies	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*No*	*Yes*
Log likelihood	-193	-192	-192	-191	-190	-190	-186	-186	-184	-179
N	228	228	228	228	228	228	226	226	226	226

*p<0.10,** p<0.05, ***p<0.01

Table 5: AVERAGE MARGINAL EFFECTS: GROUPS AND INTERACTION TERMS

Model	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
Breach Message (Below)	0.311***	0.310***	0.309***	0.308***	0.306***	0.299**	0.299**	0.295**	0.292**
	(0.117)	(0.117)	(0.117)	(0.117)	(0.121)	(0.122)	(0.123)	(0.125)	(0.132)
Breach Message (Above)	0.457***	0.456***	0.457***	0.458***	0.458***	0.459***	0.460***	0.461***	0.462***
	(0.075)	(0.075)	(0.075)	(0.071)	(0.071)	(0.068)	(0.068)	(0.065)	(0.065)
*Below *Breach Message (Diff-in-Diff)*	-0.146	-0.146	-0.148	-0.151	-0.152	-0.160	-0.161	-0.166	-0.170
	(0.140)	(0.140)	(0.140)	(0.139)	(0.141)	(0.142)	(0.142)	(0.142)	(0.148)
No breach Message (Below)		-0.067	-0.109	-0.108	-0.107	-0.119	-0.120	-0.115	-0.110
		(0.052)	(0.076)	(0.077)	(0.077)	(0.077)	(0.077)	(0.077)	(0.078)
No Breach Message (Above)		-0.143**	-0.102	-0.101	-0.101	-0.102	-0.104	-0.108	-0.108
		(0.067)	(0.090)	(0.089)	(0.089)	(0.089)	(0.089)	(0.090)	(0.084)
*Below *No Breach Message (Diff-in-Diff)*			-0.007	-0.007	-0.007	-0.017	-0.016	-0.007	-0.002
			(0.118)	(0.118)	(0.118)	(0.118)	(0.119)	(0.119)	(0.115)



Alma Mater Studiorum - Università di Bologna
DEPARTMENT OF ECONOMICS

Strada Maggiore 45
40125 Bologna - Italy
Tel. +39 051 2092604
Fax +39 051 2092664
http://www.dse.unibo.it