Disclosure of Personal Information under Risk of Privacy Shocks

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

August 27, 2015

Abstract

Breaches of the security of personal data collected by firms are reported almost daily. Companies are under an increasing political pressure to notify individuals whose privacy as been breached. At the moment, we know virtually nothing about the behavioral impact of data breach notifications. We present the results of an experimental study designed to investigate how breach notifications change the individual's propensity to provide sensitive personal information to firms. In contrast to the theory (where breach notifications have no behavioral effect), our main result shows that notifications induce a sub-group of individuals to disclose less information to a firm, i.e. those with personally sensitive information.

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]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, Pio Baake, Maria Bigoni, Laura Brandimarte, Rainer Böhme, Paolo Crosetto, Alexia Gaudeul, Werner Güth, Kai-Lung Hui, Oliver Kirchkamp, Dorothea Kübler, 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

Breaches of security of personal data collected by companies are reported almost daily. These breaches occur due to hacker attacks or improper data handling practices.

A 2015 report identifies 79,790 data breaches in 70 contributing companies, which led to a loss of a staggering number of 750 million records (Verizon (2015)). Yet, most victimized individuals seem to ignore data breaches. The Ponemon Institute in the U.S. reports that – based upon estimates by the managements of the affected firms – only 2-4 percent of customers terminate their contractual relationship after receiving a data breach notification. One explanation of this puzzle could be that customers do not regard the resulting damage as great enough to change their behavior. Another is that consumers are numb considering the frequency and number of breaches reported in the news.

Even if consumers seem to have few concerns about violations of personal data, there is an increasing pressure on firms by policymakers in the U.S. and the European Union to report data breaches. In the U.S., an increasing number of states have enacted breach notification laws. In Europe, on the other hand, in 2009 the European Commission (EC) introduced a notification obligation for telecoms and Internet Service Providers (E-privacy Directive). The EC is now discussing if the scope of reporting should be expanded to all sectors.

Despite the extent of the problem, there is currently no rigorous research about the behavioral impact of data breaches. This void motivates our work. Our main objective is to investigate how data breach notifications affect the individual's behavior regarding disclosure of sensitive personal data. We present a novel experiment where the experimental subjects play a two-period lottery with their personal information. First, the participants conduct a logic test with questions from an IQ test and each individual is privately informed, if her test result is above or below the median of the group in the laboratory. In each of the two subsequent periods, an individual can decide to sell her name and the test result (i.e., if the test result is above or below the median) in order to obtain a shopping voucher at a discounted price. The name and the test result are denoted as *"personal information*."[1] After each period, chance determines whether a data breach has occurred or not. A data breach *does not automatically* lead to public disclosure of the personal information generated. This happens only if - at the end of the experiment - another random draw selects exactly the period in which the data was sold and a breach has occurred. In that case, the name and the test result of the individual are disclosed to the whole group in the laboratory (i.e., a '*privacy shock*' happens). We run two treatments that differ only in the information individuals receive at the end of each period: in the *Notification* treatment individuals are informed whether or not a data breach has occurred, in the *No Notification*

[1]The name and test result constitute personal information as defined by the EU Data Protection Directive 95/46/EC, where it is stated that personal data is any information relating to an *identified* or *identifiable natural person*.

treatment individuals do not receive any type of information. Note that in both treatments, the choice of selling their information is up to the participants, who have to balance if the benefits of a disclosure (i.e. the discount on the voucher) compensates for the perceived costs that arise from the potential diffusion of the information (i.e., the likely privacy costs).

Under the assumption that a privacy shock affects negatively the individual utility (if and only if the test result is below the median), economic theory predicts that: *i)* individuals with a test result above the median sell their personal information in both periods; *ii)* individuals with a test result below the median sell their personal information if and only if the discount is large enough; and *iii)* a data breach notification does not affect these decisions.

Our main results are the following: we observe that individuals with a test result below the median tend to be less likely to sell their personal information compared to individuals with a test result above the median. This empirical result confirms that the personal information generated in the laboratory (i.e., the test result tied to the name of the individual) is regarded as sensitive primarily by those that are below the median. Individuals with a test result below the median are less likely to sell their information in the second period, in particular after receiving the message that a data breach had occurred. This result suggests that the notification sensitizes individuals with a test result below the median. Finally, we find that a message stating that a data breach did not happen does not affect the decision to sell personal information.

Concerns about the diffusion of private/personal information are studied by Acquisti and Grossklags (2007), Huberman et al. (2005) and Beresford et al. (2012), among others.

Huberman et al. (2005) designed an experiment to elicit the value people place on their private data (their weight and age). Their subjects participated in a reverse second-price auction: the individual demanding the least price was paid the second-lowest bid price and in exchange of the revelation of the weight or age information to the other participants. While the information was verified, participants in this experiment remained anonymous. The main result is that the less socially desirable the revealed weight or age information was (compared to the group's average), the greater the price that a person demanded for releasing it. Acquisti and Grossklags (2007) investigate the gap between the willingness to sell and the willingness to protect personal information.[2] The authors generated a quiz score and recorded the weight of the experimental subjects. They then offered their participants the opportunity either to protect this information against the release to the other participants of the group or to sell this information and have it released to the group. Their main result is that individuals almost always choose to sell their information and almost never elect to protect their information even for small payments. Beresford et al. (2012) explore the willingness-to-pay for privacy in a field experiment. Participants were confronted with two identical stores that differed only in the information requested, as one shop requested more sensitive information (i.e., personal income). In the treatment where the prices of the stores were equal, individuals bought from both stores equally often, whereas

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

in the treatment where prices differed by one Euro, all participants chose the cheaper store, although it required personal income information.

Our research is related to these experiments as they use some kind of personal information to investigate how people evaluate it under different conditions: the first paper and the third paper use pre-existing information connected to an individual, the second one creates personal information by using a test score (as in our design). However, our work differs from these studies with regard to the main research question: the effect of a breach notification on the choice of personal information disclosure. In principle we could use the setup of Huberman et al. (2005) to investigate the effect of breach notification, by looking at how the evaluation of the personal information changes after the notification of a privacy breach. But we preferred to implement the disclosure of personal information for a fixed price as this is the way of transaction in many realistic situations.

Our work differs from these literatures in other aspects as well. First, we communicate to each participant, if her test is above or below the median of the group. This way we are able to classify individuals according to their potential concern about the diffusion of their information. In the cited studies the experimenter does not provide any information regarding the recorded characteristics of the group (mean, median or other statistics), although the self-perception regarding the sensitivity of the collected data is recorded through a questionnaire. By dividing the group of participants into two sub-groups (i.e., individuals with a test result above and those with one below the median), we increase the privacy concerns of some of our participants, as this allows for a social comparison among participants (see Azmat and Iriberri (2010)). A second key feature of our design is that participants do not remain anonymous, but are identified with their real name. The real name as well as the test result is verified by the experimenter, which introduces stronger privacy concerns compared to situations, where information is not tied to the real name. The third - and perhaps most important - feature of our experimental design is that the sale of personal information does not automatically lead to its disclosure at the end of the experiment. This feature allows us to use a two-period design[3] that is key in order to study the behavioral impact of a data breach notification.[4]

Other experiments study how identification of participants affects the behavior in Dictator Games (DG), Ultimatum Games (UG), Trust Games and Prisoner's Dilemmas (PD). For example, Frey and Bohnet (1997) and Bohnet and Frey (1999) demonstrate that removing anonymity increases "solidarity" among participants (i.e., the caring about the others' welfare). In these

[3]If the sale of personal information automatically leads to its disclosure after a privacy breach, the reserve price of the information goes to zero in the second period. It is 'burned' so to say and individuals would always sell it, because it is already lost.

[4]In a two-period setup, we are able to analyze the sale decision of an individual, who has been informed about a breach notification. The reason is that after a breach notification, the personal information is not automatically lost. It is only lost, once a shock co-incidentially also occurs. The reader is referred to the enclosed instructions for details.

experiments, the interaction in the PD situation under conditions of identification leads to a higher cooperation rate compared to a situation of anonymity. In DG identification leads to a greater allocation of monetary amounts to the counterpart. Identification in these experiments is implemented by participants either standing up in the class, by looking at each other in silence or by announcing names and hobbies. Similarly, Charness and Gneezy (2008) consider the effect of revealing the family name of a participant's counterpart in DG and UG. They find that in the DG the revelation of the name of the recipient results in more generous allocations, while in the UG it has no significant effect. These experiments highlight the impact of identification of the participants on their interactions with other individuals. While these experiments highlight how identification of participants affects the interactions between individuals, our design does not consider interaction among participants, i.e. the decision to sell personal information does not affect the payoff of the others.

The paper is organized as follows: in section 2 we describe the design of the experiment and the theoretical predictions; section 3 describes the main results and section 4 concludes.

2 Experimental Design

This experiment is designed to study the impact of privacy breach notifications on individual behavior. The experiment consists of two parts: the first is used to create sensitive personal information, the second part is used to study the decisions that individuals make with respect to their personal data. In the first part of the experiment, subjects took a logic test. It consisted of 22 questions drawn from an IQ test, which had to be answered within 17 minutes. For each correct answer, participants earned 30 Euro cents (up to a maximum of 6.60 Euros). At the end of the test, individuals were privately informed about their test result and whether they were above or below the median of the session (the exact message read: "You belong to the upper 50 percent of the group" in the case of an above-median result). We assume that individuals with a test result below the median have concerns with respect to the diffusion of this information to the other participants. Indeed there is evidence that results of a logic test create sensitivity in an academic environment. For example Azmat and Iriberri (2010) show that students care about social comparisons, once they can observe whether others are performing better or worse than the class average. Note that IQ tests have already been used in the laboratory environment, see for example Ariely and Norton (2005). We do not use personal financial or health information for two reasons: First, its truthfulness needs to be verified, otherwise subjects may simply lie about it, and secondly, real financial or health data can be used by other participants for illegal purposes. Our experimental design needed to undergo review of the Berliner Data Protection Officer (an official state institution) and we needed to limit the usage possibilities of the disclosed data, while at the same time creating sensitivity in order to obtain a privacy concern.

The second part of the experiment consisted of two periods. In each period participants could decide whether to purchase a real shopping voucher from a firm or not. The voucher was for a well-known multi-media store in Berlin with a face value of 4 Euros, but was offered at a price of 3 Euros to the subjects. This price could be further reduced to 1 Euro, if subjects provided the information about the position of their test result respect to the median of the session (either above or below) and their name to the experimenter.[5] The participants had three options: *(1)* to provide (or disclose) their personal information (name and test result with respect to the median of the session) to the experimenter in order to purchase the voucher at the reduced price of 1 Euro; *(2)* to purchase the voucher at its offered price (*3* Euro) under conditions of anonymity; *(3)* to not purchase the voucher at all.

The personal information provided to the experimenter was subject to the risk of being revealed to all participants according to the following procedure. In each period, a data breach occurred with the probability of .5. The probability was independently determined for each individual and period.

This breach, though, did not automatically lead to the revelation of the personal information to the group. The intuition is that data leaks do not always automatically lead to a realized damage for individuals. If a breach would have led to revelation, all individuals would have sold their information after the first breach. To avoid this effect, we implemented a random draw at the end of the second period (which was independently determined for each individual), which selected one of the two shopping periods. If the individual purchased the voucher at a reduced price in that selected period, and a data breach had occurred as well, the personal information provided in that period by the individual was revealed to all participants at the end of the session (so-called *'privacy shock'*).

At the end of the experiment, each subject's payment appeared on the screen. The subject had to write this payment on the receipt. The experimenter checked whether the correct payment was put in, and whether there was the correct name on the payment receipt. The name was verified by checking an official identity document (identity card or student card), which all participants of laboratory experiments at German universities have to bring. After the verification stage, the name and test result (i.e. being above or below the median) of those who chose to sell their personal information, and for whom the privacy shock had realized, was read aloud to the group by the experimenter.

We implemented two treatments in a total of 13 sessions: The first treatment was denoted as *No Notification*, and was exactly the procedure explained above. The second treatment, de-

[5]To create a realistic exercise, in the game participants sold their information to a computerized firm. The value of the discount had been determined upfront through several privacy auctions we conducted. These were reverse Vickrey auctions run with different participants, who could sell their name and test result by submitting bids. The participant, who submitted the lowest bid, won the auction, but received the amount of the second lowest bid as payment. The results from these auctions are available from the authors upon request.

noted as *Notification,* is identical to the *No Notification* treatment except that all individuals, who bought a voucher obtained at the end of each period a message whether a breach had happened or not (i.e. either the message: *'A privacy breach has occurred'* or the message *'No privacy breach has occurred'*. In the following these messages are denoted by *Breach Message* and *No Breach Message*).

Table (1) gives an overview of the treatments and notification procedures. Note that the realization of a data breach is a necessary (but not sufficient) condition for a *privacy shock*. This setup maintains the sensitivity of the information in the second period, even after a data breach has occurred in the first period (i.e. the information is not 'burned' after the first data breach).[6] In order to make this setup easy to understand for the subjects, we explained the privacy breach and shock with different case in the instructions (see the Table included in the instructions).

Based on the theoretical analysis reported in the Appendix, we briefly summarize the predictions for each treatment. In the *No Notification* treatment, subjects with a test result above the median sell their personal information, while subjects with a test result below the median sell their personal information only if the premium (price reduction) is sufficiently large to compensate for the disutility arising from a possible privacy shock. If the premium is too small, these subjects will prefer not sell their personal information.

In the *Notification* treatment the breach notification has no effects on the individuals' incentive to sell personal information.

The experiment was run between June and August 2012 at Technical University of Berlin laboratory to which the participants were invited. This invitation was neutral in order to not prime subjects on the issue of privacy. Altogether 228 subjects participated in a total of 13 sessions. The individuals were seated in booths with no possibility to visually or verbally communicate with each another. Each session lasted for less than one hour and did not start until all participants were familiar with the experimental procedures. In order to check the comprehension of the experimental procedures, subjects solved various exercises. The average payoff from the experiment was about 6 Euro in cash and 4 Euro in vouchers. The software used for programming of the game was z-Tree software (Fischbacher (2007)). The translation of the instruction from the original German version into English is included in the Appendix at the end of the paper.

3 Experimental Results

Table (2) describes the dataset. The main descriptive statistics are reported by treatment. Almost half of the subjects decided to disclose their personal information in order to buy the voucher at the discounted price. A negligible number of subjects decided to buy the voucher

[6] At an ex-ante stage the probability of a privacy shock affecting the first period is 0.25. After the notification of no breach the probability of a privacy shock affecting the first period is zero and 0.5 if a data breach is notified.

without discount, i.e. anonymously. There are not significant differences in the relative frequencies of information disclosure across periods and treatments (variables *Disclosure 1st period* and *Disclosure 2nd period*). At first glance, there is no significant treatment effect.

Table (3) reports the relative frequencies of information disclosure for the first period by treatment and test results (above or below the median). The top part of table (4) reports the differences in the relative frequencies of information disclosure between treatments by test result, along with the associated t-test, pr-test and Mann-Whitney test.[7] All these differences fail to be significant. Therefore, there is no evidence of a treatment effect in period 1, i.e. the notification device does not enhance the disclosure of *personal information*. The bottom part of table (4) reports the differences in the disclosure behavior between individuals with test result above the median and those with test result below the median by treatment. All these differences are negative and significant (-23.2 % and -34.8% respectively in the *No Notification* and *Notification* treatment). This result supports the assumption that the information we generated in the laboratory is sensitive, especially for individuals with a test result below the median.

> RESULT 1: Individuals with a test result below the median disclose their personal information less frequently compared to individuals with a test result above the median. The presence of a data breach notification does not affect the disclosure behavior in the first period.

Note that the first part of this result is in line with previous research on privacy showing that the less socially desirable the revealed personal information is, the greater is the price a person demands (e.g. Huberman et al. (2005)). Consistent with this observation, we find that individuals with a less desirable test result (i.e., they are below the median) are less likely to disclose this information for a fixed discount. The second part of the result can be interpreted in a way that the presence of a data breach notification (subjects were informed upfront through the instructions) does not improve the confidence of individuals in the first period, i.e. at an ex-ante stage.

To study the effect of the notification messages, we analyze the decisions taken in the second period. We further classify individuals by means of dummy variables according to the treatment, the action taken in the first period (i.e., did not buy a voucher, bought a voucher), the type of message received (i.e. *Breach Message*, *No Breach Message*) and their test result (above or below the median).[8] For example, with D_5 we denote the category of individuals who participated in the *No Notification* treatment (i.e. treatment=0), did not buy a voucher in the first period (buy=0) and had test results above the median (i.e., below=0). The categories $D_6, ..., D_{14}$

[7] The first two are parametric tests for mean-comparisons, which are suited for large samples (n>100) and binomial variable, respectively. The latter is a non-parametric test on the equality of two distributions.

[8] In this analysis, we combine individuals who bought a voucher under the condition of anonymity (case 2 on p. 6) with those who bought the voucher providing their personal information (case 1 on p. 6) as they are too few (less than 2% see Table (2)).

classify individuals in a similar manner. For each of these categories, Table (5) reports the sample probability of observing an individual purchasing the voucher at a reduced price in the second period (i.e. disclosing her *personal information* in the second period). For example, for individuals belonging to category D_5 the probability of disclosing *personal information* in period 2 is 0.145.

Table (6) reports the differences in the probability of disclosing *personal information* in the second period between different categories together with t-test, pr-test and Mann-Whitney. The top part of the table highlights the effect of the messages on the decision of disclosure in the second period by comparing the behavior of individuals with the same test result, who bought the voucher in period 1, but participated in different treatments. The only difference between two categories was whether the individuals received a data breach notification (if they participated in the notification treatment) or not. For example, the effect of the *Breach Message* on individuals with a test result above the median is given in the first row of the top part of Table (6) by the difference in the probabilities of disclosing *personal information* in the second period between categories D_{11} and D_6. This gives us the between-treatment effect of the message for individuals, who bought a voucher in the first period (i.e. buy=1) and who have a test result above the median (i.e. below=0). Similarly, we compute the effect of the *Breach Message* for individuals with a test result below the median (below=1, see $D_{13} - D_8$), and the effects of the variable *No Breach Message* for individuals with a test result above the median ($D_{12} - D_6$) as well as for those with a test below the median ($D_{14} - D_8$).

We find that the effect of the *Breach Message* on individuals with test result below the median is negative and significant. After receiving a *Breach Message* these individuals are about 50% less likely to disclose their *personal information* in the second period compared to individuals in the same position and participating in the *No Notification* treatment. On the contrary, the effect of the *No Breach Message* (i.e. individuals were informed that no breach had occurred) has no significant impact on the behavior of these individuals.

> RESULT 2: The *No Breach Message* has no effect on the disclosure of *personal information* of individuals. The *Breach Message* significantly reduces the probability to disclose *personal information* for individuals with a test result below the median, but not for individuals with a test result above.

Note that this result is based upon a comparison between sessions and shows that a *No Breach Message* does not improve the confidence of individuals while the *Breach Message* reduces the confidence of below-median subjects.

The bottom part of Table (6) highlights the effect of the messages on the disclosure decision in the second period comparing the behavior of individuals participating in the *Notification Treatment*. We now focus on the effect of receiving the different types of messages. Note that we cannot compare individuals that received a message with individuals that received no message,

as these are two qualitatively different situations. So the first two rows of the bottom part of the table report the difference in the probability of disclosure between individuals that received *two different types of messages* and with a test result above the median (first row, $D_{11} - D_{12}$) or below the median (second row, $D_{13} - D_{14}$). We observe that subjects with a test result below the median are less likely to disclose their information in the second period, after they have received a *Breach Message* compared to the situation of receiving a *No Breach Message.* This effect is negative (-44%) and significant (at 10% level). For above-median subjects, this effect is also negative, but it is smaller and not significant.

Finally, we compare the differences in the disclosure probability of below-median individuals with above-median individuals conditional on receiving a given type of message. After a *Breach Message* the probability of disclosing *personal information* is remarkably lower for below-median individuals in comparison to above-median subjects (-60% significant at 1% level). The same effect conditional on receiving a *No Breach Message* is smaller (-22% significant at 5% level).

> RESULT 3: In the second period, individuals with a test result below the median disclose less compared to those above the median. This difference is remarkably larger after a *Breach Message*. The probability to disclose *personal information* for below-median individuals is smaller after a *Breach Message* compared to after a *No Breach Message*. This effect is not observable for individuals with a test result above the median.

These results suggest that the existence of a notification procedure does not enhance the trust of individuals with sensitive personal information (i.e., with a test result below the median) when receiving a *No Breach Message*. On the contrary, both within- and between-treatment comparisons suggest a negative effect of the *Breach Message* on the rate of disclosure of personal information of below-median individuals.

4 Conclusions

In a laboratory setting, we investigated the effects of data breach notifications on the disclosure behavior of individuals with respect to personal information during an economic transaction with a firm and under the risk of a privacy shock. The personal information we used is represented by the name of a subject and the result (i.e., whether a subject was above or below the median of the group) of a logical test implemented at the beginning of the experiment. Participants could sell this personal information in two subsequent "shopping periods" to a firm in order to obtain a voucher at a discounted price. This setup is unique and represents a novel approach compared to previous research.

We present three key results. The first is that individuals who pass a social comparison with a negative outcome (i.e., they are below the median of the group) are less likely to disclose

this information in both treatments and periods. This result is line with other research, which highlights that test results are regarded as a sensitive information in an academic environment, because students care about social comparisons (e.g. Azmat and Iriberri (2010)). Moreover, it is aligned with privacy research showing that the less socially desirable the information is, the higher is the price asked for by subjects who sell this information (e.g. Huberman et al. (2005)). The second key result is that once below-median individuals receive a breach notification, they are less likely to disclose their data in the next period. The third result is that a *No Breach Message* does not have any discernible difference, i.e., it does not improve the trust in the firm receiving the personal information. The results from this experiment suggest that a notification procedure will have a significant behavioral effect only on a sub-group of consumers, i.e., those individuals who regard their information as personally sensitive. If this group is not relatively large in the market place, data notification breaches might not be an effective policy tool to increase data security in firms.

References

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).

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.

Azmat, G., Iriberri, N., 2010. The importance of relative performance feedback information: Evidence from a natural experiment using high school students. Journal of Public Economics 94 (7), 435–452.

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.

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.

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.

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

Verizon, 2015. 2015 data breach investigations report. Verizon Business Risk Team. URL `http://www.verizonenterprise.com/DBIR/2015/`

A Appendix: Theoretical Predictions

In this section we derive the theoretical predictions for the experimental design. All probabilities and procedures to realize a privacy shock are explained in section 2. In the following the action of *selling the personal information* is named *disclosure (of the personal information)*

Let $\tau_i \in \{v_{i,bad}, v_{i,good}\}$, where $v_{i,bad} \leq v_{i,good}$, be the value that the subject i assigns to the evaluation of her ability (in the test) by the others, i.e. $v_{i,bad}$ ($v_{i,good}$) is the value that she adds to her utility when others know that her 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 i where -1 means that her test result was below the median and 1 means that her test result was above the median. In each of the two periods individuals decide to provide the position of their test result with respect to the median in exchange of a prize d. Let $s_{i,1} \in [0,1]$ be the probability by which subject i will disclose her *personal information* in period *1* and $s_{i,2,a} \in [0,1]$ where $a \in \{0,1\}$ be the probability by which subject i will disclose her *personal information* in period 2 where $a = 0$ denotes disclosure in period 1 and $a = 1$ denotes no disclosure in period 1. By $s_i = \{s_{i,1}, s_{i,2,0}, s_{i,2,1}\}$ we denote the behavioral strategy of individual i, by s_{-i} the set of strategies of all subjects different from i and by s the set of strategies of all subjects.

At the end of the game the utility of an individual i depends on the decisions to sell or not the *personal information* and the realization of privacy shocks. After the realization of privacy shocks, every individual updates her beliefs about the type of subjects not affected by privacy shocks. Let b_{ij} denote the probability individual i assigns to the event $\tau_j = 1$ for all individuals j not affected by privacy shock i.e. $b_{ij} = Pr\left(\tau_j = 1 | nps_j\right)$ where nps_j denotes the event *'individual j had no privacy shock'*. Then, using the Bayes rule we can compute this probability as follows:

$$b_{ij} = Pr\left(\tau_j = 1 | nps_j\right) = \frac{\#\left(nps \& \tau_j = 1\right)}{\#\left(nps \& \tau_j = 1\right) + \#\left(nps \& \tau_j = -1\right)}$$

where $\#\left(nps \& \tau_j = 1\right)$ and $\#\left(nps \& \tau_j = -1\right)$ denote the number of individuals with $\tau_j = 1$, respectively $\tau_j = -1$, and not affected by privacy shocks. We assume that second order beliefs are equal to first order beliefs and we denote them by b_i.

Let $\beta_i \geq 0$ be a sensitivity parameter of subject i concerning the revelation of her *personal information* to the other participants 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 when her type is not revealed). Her utility at the end of the game is (when privacy shocks are realized):

$$u_i\left(\tau_i\right) = \#d + \left[\beta_i \tau_i\right]^I + \left[\gamma_i \left(2b_i - 1\right)\right]^{I-1}$$

where I is an indicator variable taking value 1 if individual i was affected by a privacy shock

otherwise it takes value 0, # is the number of times she disclosed her information. Given that we are interested in decisions taken before the realizations of the privacy shocks, we need to consider the individual i ex-ante utility. To compute it we need to define:

1. the expectations of b_i over all possible realizations of # $nps\&\tau_j = 1)$ and for a given strategy profile s, i.e.$b^e_{i,s} = E(b_i)$, i.e. Note that $b^e_{i,0} \leq b^e_{i,s} \leq b^e_{i,1}$ where $b^e_{i,1}$ is the value that it takes when all subjects disclose their *personal information* in both periods and $b^e_{i,0}$is the value it takes when all subjects with $\tau_i = -1$ do not disclose their *personal information* and those with $\tau_i = 1$ disclose in both periods.

2. The individual i's the probability to face a privacy shock as function of her strategy s_i, i.e. $p(s_i) = \frac{1}{4}\left(s_{i,1}\left(1 + s_{i,2,1} - s_{i,2,0}\right) + s_{i,2,0}\right)$

Given a strategy profile $s = (s_i, s_{-i})$, the expected utility of individual i when her type is $\tau_i \in \{0, 1\}$, is:

$$u^e_i\left(s_i, s_{-i}, \tau_i\right) = d\left(s_{i,1}\left(1 + s_{i,2,1} - s_{i,2,0}\right) + s_{i,2,0}\right) + p(s_i)\beta_i\tau_i + (1 - p(s_i)) \quad \gamma_i b^e_{i,s} - \gamma_i \quad 1 - b^e_{i,s})\big)$$

where the first term is the discount(s) subjects receive when selling their *personal information*, the second term is related to the (dis)utility arising from the realization of a privacy shock at the end of the game, and the last one is the (dis)utility due to other beliefs in the case of no privacy shock occurring at the end.

Now consider the case, where $\beta_i = \gamma_i = \beta$ for all i and concentrate the attention on symmetric strategies. In the treatment without notification, subjects behave according to the following proposition:

Proposition 1.

1. For all i with $\tau_i = 1$ $s_i = \{1, x, 1\} x \in [0, 1]$ **(**full disclosure**).**

2. For all i with $\tau_i = -1$ there exist values $d'' > d'$ such that:

   (a) if $d \leq d'$ then $s_i = \{0, 0, y\} y \in [0, 1]$ **(**no disclosure)

   (b) if $d \geq d''$ then $s_i = \{1, z, 1\} z \in [0, 1]$ if $d \geq d''$ **(**full disclosure)

   (c) if $d' < d < d''$ then$s_i = \{x_1, x_2, x_3\}, x_1, x_2, x_3 \in [0, 1], x_1 + x_2 > 0, x_1 +, x_3 < 2$ (partial disclosure).

Proof. *Part 1.* The result for individuals with $\tau_i = 1$ directly follows by the consideration that their expected utility is increasing in the probability of the privacy shock. It is directly verifiable that $s_i = \{1, x, 1\}$ is maximizing the probability of privacy shock for any value of x. Then in the following we will use that $s_i = \{1, x, 1\}$ $\forall$ i s.t. $\tau_i = 1$.

Part 2. Then we can focus our attention on individuals with $\tau_i = -1$. To keep notation simple, we denote by $u_i^e(s_{i,1}, s_{i,2,0}, s_{i,2,1})$ the expected utility of individual i of type $\tau_i = -1$, playing strategy $s_i = \{s_{i,1}, s_{i,2,0}, s_{i,2,1}\}$ and given the strategies s_{-i} of other players. This expected utility is $u_i^e(s_{i,1}, s_{i,2,0}, s_{i,2,1}) = d\left(s_{i,1}\left(1 + s_{i,2,1} - s_{i,2,0}\right) + s_{i,2,0}\right) - p(s_i)\beta + (1 - p(s_i))\left(\beta b_{i,s}^e - \beta\left(1 - b_{i,s}^e\right)\right)$ where $p(s_i) = \frac{1}{4}\left(s_{i,1}\left(1 + s_{i,2,1} - s_{i,2,0}\right) + s_{i,2,0}\right)$. Replacing $p(s_i)$ we get:

$$u_i^e(s_{i,1}, s_{i,2,0}, s_{i,2,1}) = d\left(s_{i,1}\left(1 + s_{i,2,1} - s_{i,2,0}\right) + s_{i,2,0}\right) + \beta\left(2b_{i,s}^e\left(1 - \frac{1}{4}\left(s_{i,1}\left(1 + s_{i,2,1} - s_{i,2,0}\right) + s_{i,2,0}\right)\right) - 1\right)$$

We claim that, given a strategy profile $\hat{s}$, the incentives to disclose *personal information* for an individual with $\tau_i = -1$ are equal across periods and, in period 2 do not depend on what was her choice in period 1. Given a strategy profile $\hat{s}$ the incentives to disclose in period 1 are given by $u_i^e(1, s_{i,2,0}, s_{i,2,1}) - u_i^e(0, s_{i,2,0}, s_{i,2,1})$ where $u_i^e(1, s_{i,2,0}, s_{i,2,1}) = d\left(1 + s_{i,2,1}\right) + \beta\left(2b_{i,\hat{s}}^e\left(1 - \frac{1}{4}\left(1 + s_{i,2,1}\right)\right) - 1\right)$, $u_i^e(0, s_{i,2,0}, s_{i,2,1}) = ds_{i,2,0} + \beta\left(2b_{i,\hat{s}}^e\left(1 - \frac{1}{4}s_{i,2,0}\right) - 1\right)$.

Agent i will disclose if and only if $u_i^e(1, s_{i,2,0}, s_{i,2,1}) - u_i^e(0, s_{i,2,0}, s_{i,2,1}) = d\left(1 + s_{i,2,1} - s_{i,2,0}\right) - \beta\frac{1}{2}b_{i,\hat{s}}^e\left(1 + s_{i,2,1} - s_{i,2,0}\right) \geq 0$ that is true when $d \geq \beta\frac{1}{2}b_{i,\hat{s}}^e$. In period 2 when in period 1 *personal information* was disclosed, agent i will disclose if and only if $u_i^e(1, s_{i,2,0}, 1) - u_i^e(1, s_{i,2,0}, 0) \geq 0$ where $u_i^e(1, s_{i,2,0}, 1) = 2d + \beta\left(b_{i,\hat{s}}^e - 1\right)$, $u_i^e(1, s_{i,2,0}, 0) = d + \beta\left(b_{i,\hat{s}}^e\frac{3}{2} - 1\right)$. Solving the inequality we find that it happens when $d \geq \frac{1}{2}\beta b_{i,\hat{s}}^e$. In period 2 (when in period 1 *personal information* was not disclosed), agent i will disclose if and only if $u_i^e(0, 1, s_{i,2,1}) - u_i^e(0, 0, s_{i,2,1}) \geq 0$ where $u_i^e(0, 1, s_{i,2,1}) = d + \beta\left(\frac{3}{2}b_{i,\hat{s}}^e - 1\right)$, $u_i^e(0, 0, s_{i,2,1}) = \beta\left(2b_{i,\hat{s}}^e - 1\right)$. Solving the inequality we find that it happens when $d \geq \frac{1}{2}\beta b_{i,\hat{s}}^e$. This proves the claim.

Case (a). Suppose that $d \leq \frac{1}{2}\beta b_{i,0}^e = d'$. Assume a strategy profile $\hat{s}$ where individuals with $\tau_i = 1$ disclose their *personal information* in both periods and agents with $\tau_i = -1$ are characterized by some level of disclosure of *personal information* (i.e. $s_{i,1} + s_{i,2,0} > 0$). Then $b_{i,\hat{s}}^e > b_{i,0}^e$ and $d < \frac{1}{2}\beta b_{i,\hat{s}}^e$. As a consequence of the previous claim, strategy profile $\hat{s}$ cannot be an equilibrium, because agents with $\tau_i = -1$ strictly prefer to not disclose. It directly follows that there is an unique equilibrium strategy profile that has to be characterized by no disclosure of *personal information*, i.e. $s_i = \{0, 0, y\} y \in [0, 1]$ for all i.

Case (b). Suppose that $d \geq \frac{1}{2}\beta b_{i,1}^e = d''$. Assume a strategy profile $\hat{s}$ where individuals with $\tau_i = 1$ disclose their *personal information* in both periods and agents with $\tau_i = -1$ are characterized by partial disclosure of *personal information* (i.e. $s_{i,1} + 1, s_{i,2,1} < 2$). Then $b_{i,\hat{s}}^e < b_{i,1}^e$ and $d > \frac{1}{2}\beta b_{i,\hat{s}}^e$. As a consequence of the previous claim, strategy profile $\hat{s}$ cannot be an equilibrium, because agents with $\tau_i = -1$ strictly prefer to disclose. It directly follows that there is an unique equilibrium strategy profile that has to be characterized by full disclosure of *personal information*, i.e. $s_i = \{1, y, 1\} y \in [0, 1]$ for all i.

Case (c). Suppose $d' < d < d''$. A strategy profile $\hat{s}$ where $s_i = \{1, y, 1\} y \in [0, 1]$ for all i with $\tau_i = -1$ cannot be an equilibrium. Indeed, by assumption $d < d'' = \frac{1}{2}\beta b_{i,1}^e$ and the previous

claim, there is incentive to not disclose. A strategy profile $\hat{s}$ where $s_i = \{0, 0, y\} y \in [0, 1]$ for all i with $\tau_i = -1$ cannot be an equilibrium. Indeed, by assumption $d > d' = \frac{1}{2}\beta b^e_{i,0}$ and the previous claim, there is an incentive to disclose. QED.

Participants in the *Notification* treatment receive a message at the end of period 1, which notifies them about the realization of a data breach. They can receive two types of message: *'A privacy breach has occurred'* and the message *'No privacy breach has occurred'*. The presence of notification causes a larger set of strategies, because in the second period individuals can condition their action on the message they received. Indeed a strategy has to state the actions to undertake in period 1 and in period 2, *a)* after no disclosure in period 1 and breach notification, *b)* after no disclosure in period 1 and no breach notification, and *c)* after disclosure in period 1 and breach notification, and finally *d)* after disclosure in period 1 and no breach notification. Let $s_{i,1} \in [0, 1]$ be the probability by which subject i will disclose her *personal information* in period *1* and let $s_{i,2,a,b} \in [0, 1]$, $a, b \in \{0, 1\}$, be the probabilities by which subject i will disclose her *personal information* in period *2* where $a = 0$ ($a = 1$) denotes no disclosure (disclosure) in period 1 and $b = 0$ ($b = 1$) denotes no data breach (data breach) in period 1. Then we denote the strategy of subject i by $s_i = \{s_{i,1}, s_{i,2,0,0}, s_{i,2,0,1}, s_{i,2,1,0}, s_{i,2,1,1}\}$, where the five arguments are the disclosure probabilities in the five information sets described above. In this treatment, subjects behave according to the following proposition

Proposition 2.

1. For all i with $\tau_i = 1$ $s_i = \{1, x, , y, 1, 1\} x, y \in [0, 1]$ **(**full disclosure**).**
2. For all i with $\tau_i = -1$ there exist values $d'' > d'$ such that:
   (a) if $d \leq d'$ then $s_i = \{0, 0, 0, w, x\}$ $w, x \in [0, 1]$ if $d \leq d'$, **(**no disclosure)
   (b) if $d \geq d''$ then $s_i = \{1, y, z, 1, 1\}$ $y, z \in [0, 1]$ if $d \geq d''$ **(**full disclosure)
   (c) if $d' < d < d''$ then$s_i = \{x_1, x_2, x_3, x_4, , x_5\}$, $x_1, x_2, x_3, x_4, , x \in [0, 1], x_1 + x_2 + x_3 > 0, x_1 + x_4 +, x_5 < 3$ (partial disclosure).

Proof. *Part 1.* The result for individuals with $\tau_i = 1$ directly follows by the consideration that their expected utility is increasing in the probability of the privacy shock. It is directly verifiable that $s_i = \{1, x, , y, 1, 1\}$ is maximizing the probability of privacy shock for any value of x. Then in the following we will use that $s_i = \{1, x, , y, 1, 1\}$ $\forall$ i s.t. $\tau_i = 1$.

Part 2. Then we can focus our attention on individuals with $\tau_i = -1$. We compute their incentives to sell information in the second period. We consider two cases: *a)* a privacy breach has occurred and *b)* no privacy breach has occurred. By $u^e(0, 1)$ and $u^e(1, 1)$ we denote the expected utilities deriving from disclosing the personal information in period 2 after, respectively, no disclosure and disclosure in period 1. By $u^e(0, 0)$ and $u^e(1, 0)$ we denote the expected

utility deriving from no disclosing the personal information in period 2 after, respectively, no disclosure and disclosure in period 1.

i) Suppose a strategy profile $\hat{s}$ and that individual i disclosed her personal information in period 1. If she receives the message "*a privacy breach has occurred*" she knows that a privacy shock can happen to the *personal information* revealed in period 1 by probability $\frac{1}{2}$. Then $u^e(1,1) = 2d - \frac{1+\frac{1}{2}}{2}\beta + \frac{1-\frac{1}{2}}{2}(2b^e_{i,\hat{s}} - 1)\beta$ and $u^e(1,0) = d - \frac{1}{2}\beta + \frac{1}{2}(2b^e_{i,\hat{s}} - 1)\beta$. Agent i will disclose if and only if $u^e(1,1) - u^e(1,0) = d - \frac{1}{2}\beta b^e_{i,\hat{s}} \geq 0$. If she receives the message *'no privacy breach has occurred'* he knows that a privacy shock cannot happen to the *personal information* revealed in period 1. Then $u(1,1) = 2d - \frac{\pi}{2}\beta + (1 - \frac{\pi}{2})(2b_{i,\hat{s}} - 1)\beta$ and $u(1,0) = d + (2b_{i,\hat{s}} - 1)\beta$. Agent i will disclose if and only if $u^e(1,1) - u^e(0,1) = d - \frac{1}{2}\beta b^e_{i,\hat{s}} \geq 0$.

ii) Suppose a strategy profile $\hat{s}$ and that individual i did not disclose her information in period 1. After any message her expected utility from disclosure in period 2 is $u^e(0,1) = d - \frac{1}{4}\beta + \left(1 - \frac{1}{4}\right)(2b^e_{i,\hat{s}} - 1)\beta$, while the expected utility from no disclosure in period 2 is $u^e(0,0) = (2b^e_{i\hat{s}} - 1)\beta$. Agent i will disclose if and only if $u^e(0,1) - u^e(0,0) = d - \pi\beta b^e_{i,\hat{s}} \geq 0$.

Note that if $d \geq d'' = \beta\frac{1}{2}b^e_{i,1}$the disclosure is preferred in all cases in period 2 while $d \leq \beta\frac{1}{2}b^e_{i,0} = d''$ implies that in period 2 no disclosure is preferred in all cases.

Case (a). Suppose that $d \leq \beta\frac{1}{2}b^e_{i,0} = d''$. It implies that in period 2 no disclosure is preferred in all cases. Assume a strategy profile $\hat{s}$ characterized by some level of disclosure in period 1, i.e. $s_{i,1} \in (0,1)$and no disclosure in period 2. The expected utility from disclosing in period 1 is $d - \frac{1}{4}\beta + \left(1 - \frac{1}{4}\right)(2b^e_i - 1)\beta$ while that from no disclosing im period 1 is $(2b^e_i - 1)\beta$. Then *personal information* will be disclosed in period 1 if and only if the difference between these utilities is positive, i.e. $d - \frac{1}{2}b^e_{i,\hat{s}}\beta \geq 0$. By initial assumption ($d \leq \beta\frac{1}{2}b^e_{i,0}$) and the consideration $b^e_{i,\hat{s}} > b^e_{i,0}$ this inequality is not satisfied. Directly follows that an equilibrium strategy has to imply no disclosure in both periods.

Case (b). Suppose $d \geq d'' = \beta\frac{1}{2}b^e_{i,1}$. It implies that in period 2 the *personal information* will be disclosed. Assume a strategy profile $\hat{s}$ characterized by some level of disclosure in period 1, i.e. $s_{i,1} \in (0,1)$and full disclosure in period 2. The expected utility from disclosing in period 1 is $2d - \frac{1}{2}\beta + \left(1 - \frac{1}{2}\right)(2b^e_{i,\hat{s}} - 1)\beta$ while that from no disclosing im period 1 is $d - \frac{1}{4}\beta + \left(1 - \frac{1}{4}\right)(2b^e_{i,\hat{s}} - 1)\beta$. *Personal information* will be disclosed in period 1 if and only if the difference between these utilities is positive, i.e. $d - \frac{1}{2}b^e_{i,\hat{s}}\beta \geq 0$. Given the initial assumption ($d \geq \beta\frac{1}{2}b^e_{i,1}$) and the consideration $b^e_{i,\hat{s}} < b^e_{i,1}$this inequality is strictly satisfied. Directly follows that an equilibrium strategy has to imply full disclosure in both periods.

Case (c). Suppose $d' < d < d''$. A strategy profile $\hat{s}$ where $s_i = \{1, y, z, 1, 1\}$ $y, z \in [0,1]$ for all i with $\tau_i = -1$ cannot be an equilibrium. Indeed, by assumption $d < d'' = \frac{1}{2}\beta b^e_{i,1}$ and the previous considerations, there is an incentive to not disclose. A strategy profile $\hat{s}$ where $s_i = \{0, 0, 0, y, z\}$ $y, z \in [0,1]$ for all i with $\tau_i = -1$ cannot be an equilibrium. Indeed, by assumption $d > d' = \frac{1}{2}\beta b^e_{i,0}$ and the previous considerations, there is an incentive to disclose.QED.

DIW BERLIN

Dear Participant,

on behalf of DIW Berlin, welcome. **Please read these instructions carefully through, because they contain important information about today's experiment.**

Scientific background: You take part in a scientific experiment, which is carried out by DIW Berlin. We use the results for scientific publications. Participation in the experiment is voluntary. Please take a moment for the present instructions. If you have any questions, please notify the experimenters by hand signal. Do not ask your neighbor.

Duration of the experiment: The entire experiment is expected to last 50 minutes. The session begins with a short entry questionnaire, and a lottery, which is followed by the experiment. The session is concluded with an exit questionnaire.

Procedure of the experiment: The experiment begins after the entry questionnaire and the lottery. As the first task in the experiment you will take a logical test that is similar to an intelligence test. After the test you will be informed about your test result. You may use the test result in a purchase transaction in order to reduce the price of a good that is offered to you for sale. This will be explained in detail below.

Test: The logical test consists of 22 questions for which you have 17 minutes (or 1040 seconds). For each correct answer you earn 0.30 Euro, 6.60 Euros at maximum. There are no deductions for wrong answers. You can divide the 17 minutes in the test freely and you may change decisions by pressing the ‚Back'-button. Please pay attention to the time remaining, it is shown at the top right – of your screen in the form of seconds. You conclude the test by pressing the "End test"-button.

After the test, each participant is **personally** and **confidentially** informed about his/her test result on the screen. You will then have the opportunity to use your test result for a price reduction of the offered good (which is a voucher).

Purchase transaction: You will now assume the role of a consumer. Your transaction partner is a company that is computerized. Each period, you meet **one company** that offers you a good for purchase. The good is a voucher of the **store Dussmann at Friedrichstrasse station in Berlin**. You may use the voucher to buy books, CDs or DVDs or other items offered. This item can be used to purchase books, CDs or DVDs, or other things. The voucher has a real monetary value of 4 Euros. This is referred to in the experiment as "your valuation."

Participation Instructions

Periods: The experiment has **two periods** in which you are offered a voucher by the company. As mentioned, the real monetary value is 4 Euros, the company offers you the voucher for the price of 3 Euros. The price remains constant. In each period, you will additionally get the chance to reduce the price of the voucher. You can receive a discount of € 2 at the company, if you disclose your name to the company. This will automatically also transfer your test result to the company. In this case you can obtain the voucher for a price of 1 Euro. Also, the discount remains constant.

If you claim the price reduction, please enter your first and last name truthfully and completely. Then press **ENTER** on the **keyboard** (this is also explained on the screen) in order to save your name for this transaction. If you do not press enter, no payments can be made.

Again, in the purchase transaction you have the following options:

- You can buy the voucher at full price at which the company offers it (3 Euros), without disclosing your name
- You may purchase the voucher at 1 Euro (the discount is 2 Euros) if you disclose name and test result – please safe your name for the purchase as explained
- You may not purchase any voucher.

Data breach: Every company has 50 percent chance that a data breach occurs. With a data breach, there is the **possibility** that you will be named at the end of the experiment and your test result is announced to the other participants. In the announcement, the experimenter will read your name and your test result out. The likelihood of data breach is 50 percent and remains the same in the individual periods. The data breach only may affect you, if you have disclosed your personal data, i.e. if you have given your name and test results of the company for a price reduction.

Please note that your name and test result is only publicly announced if there is **a coincidence of exactly three events**:

1. You purchase a voucher with a price reduction, for which you have disclosed you data and
2. the company is hit by a data breach and
3. exactly that period is randomly drawn by the experimenter at the end of the experiment

So if you have given your name to get the price reduction, this must **NOT AUTOMATICALLY** mean that your name and your test result will be read publicly. Only if the experimentalist draws just that very period and a data breach has happened, it will result in a public announcement. For better understanding, here are three examples:

Period 1	Period 2	Random draw	Announcement of name and test result
Situation 1			
• Purchase of voucher with price reduction • No data breach	• Purchase of voucher with price reduction • Data breach	Period 2	Announcement
Situation 2			
• Purchase of voucher with price reduction • No data breach	• Purchase of voucher with price reduction • Data breach	Period 1	No announcement
Situation 3			
• Purchase of voucher with-out price reduction • Data breach	• Purchase of voucher with price reduction • Data breach	Period 1	No announcement

During both periods, you will not be informed whether a data breach has occurred in the company or not. Whether your data were compromised by random draw, you will only learn at the end of the experiment, at the time when you are informed about your total payment.

[Note to the reviewers: this paragraph is exchanged in Treatment B for: After each period you will be informed whether a data breach in the company has occurred or not. The company **informs all participants, regardless of whether they have disclosed data or not**. Whether your data were further compromised by random draw (in the case that you have disclosed data), you will learn at the end of the experiment, once you are informed of the total payment.]

Participation fees and payment: At the end of the experiment you will be informed about your total payment. Please fill in your name and the total payment into the present receipt. The experimenters will briefly walk around and check whether you have entered the correct amount. Moreover, your name will be checked based on a photo or student ID. Please present your ID for checking. If you have given an incorrect name, there will be no payment.

The person who has won the lottery shall also note the amount on the receipt.

You get 6 Euros participation fee. In the test, 6.6 Euro can be earned. Moreover, you may acquire two coupons with the real monetary value of 8 Euro. If you buy with discount, you need to pay 1 Euro for each (i.e. 2 Euros for two vouchers). If you purchase without discount you pay 3 Euros each (6 Euros for two vouchers). If you are drawn as the winner of the lottery, you will also obtain the payment of the lottery. If you do not buy vouchers, you will only receive the cash payment (i.e. the payment earned in the test and the participation fee).

In the case your data have been compromised, your name and your test result is announced, but they will be deleted immediately after the experiment and they will not be used for data analysis or another purpose.

After completion of the experiment, there is an exit questionnaire. Following this, the payment is made. Please wait until we make the payments. You are paid in cash and in vouchers depending on whether you have purchased the latter.

The present experiment thus consists of the following stages:

1. Preparation: You read the instructions. The computer in front of you will then guide you through the experiment.

2. Entry questionnaire: Please first complete the entry questionnaire.

3. Lottery: Here you are faced with 11 decision situations in which you have to make one choice (either LEFT or RIGHT). This will be explained in greater detail on the screen.

4. Experiment: After that the computer guides you through the logical test. It involves questions similar to those used in an intelligence test – however, it is not a full-scaled intelligence test. Such test normally last for 1,5 hours and encompass far more questions. After the test you meet one company per period, which offers you a voucher. Finally, put the total payment on the receipt.

5. Exit questionnaire: After all participants have completed the final questionnaire, the experiment is finished.

6. Payment: After you have answered the exit questionnaire, we will announce the names and test results of the persons that have been affected by a privacy breach and the random draw. After that the payments will be issued.

Regulations: Please understand that electronic devices are not permitted during the present experiment. Please turn off them off now and stow cell phones or similar devices in your pocket or backpack before we begin the session. Please read the instructions given on the screen carefully.

Please remain seated at your place throughout the experiment, even when you finish earlier than your neighbors. You may encounter inherent waiting times during the experiment, we therefore ask for your patience.

If you disturb the course of the experiment, talk loudly or use an electronic device, we will ask you to leave the experiment without payment.

Participation Instructions

On behalf of DIW Berlin, once again a big thank-you for participating in today's experiment. Please fill now the following declaration of consent, which we need for our files:

DIW Berlin, Abt. Wettbewerb und Verbraucher

Mohrenstraße 58
10117 Berlin

Fr. Jentzsch: njentzsch@diw.de
+49 30 89789 234

I understand that my participation is voluntary and I may cancel it at any time without notice of a reason. I understand that my data will be made anonymous after the conclusion of the experiment and after payment. The above description of the research project I have read and I hereby agree to participate.

Name: .....

Date: ..... Signatur: .....

Should you at present have any questions, please call an experimenter by hand-sign. Otherwise, please switch now the screen on, and concompany that you are ready to begin the experiment.

Table 1: NOTIFICATION IMPLEMENTATION

SUBJECT ACTION IN THE 1ST PERIOD	1ST PERIOD EVENT	TYPE OF MESSAGE AFTER 1ST PERIOD
No-Notification Treatment		
Did not buy a voucher	No data breach	No message
	Data breach	No message
Bought a voucher anonymously	No data breach	No message
	Data breach	No message
Bought a voucher with data disclosure	No data breach	No message
	Data breach	No message
Notification Treatment		
Did not buy a voucher	No data breach	No message
	Data breach	No message
Bought a voucher anonymously	No data breach	"No breach has occurred"
	Data breach	"A breach has occurred"
Bought a voucher with data disclosure	No data breach	"No breach has occurred"
	Data breach	"A breach has occurred"

Table 2: VARIABLE DESCRIPTION

Variable Name	Description	No-Notification Treatment					Notification Treatment				
		Mean	Std. Dev.	Min.	Max.	N	Mean	Std. Dev.	Min.	Max.	N
Disclosure 1st period	Dummy variable equal to 1 if the subject disclosed personal data to obtain a discount for the voucher in the first period.	0.441	0.498	0	1	127	0.455	0.500	0	1	101
Disclosure 2nd period	Dummy variable equal to 1 if the subject disclosed personal data to obtain a discount for the voucher in the second period.	0.449	0.499	0	1	127	0.485	0.502	0	1	101
Below	Dummy variable equal to 1 if the subject is below the median result of the group in the logical test in the experimental session.	0.433	0.497	0	1	127	0.426	0.497	0	1	101
1st period Purchase	Dummy variable equal to 1 if the subject bought a voucher in the first period without disclosing the personal data.	0.016	0.125	0	1	127	0.010	0.100	0	1	101
2st period Purchase	Dummy variable equal to 1 if the subject bought a voucher in the second period without disclosing the personal data.	0.016	0.125	0	1	127	0.020	0.140	0	1	101
Breach Message	Dummy equal to 1 if the subject received the message "A breach has occurred" in the treatment session.	-	-	-	-	127	0.178	0.385	0	1	101
No-breach Message	Dummy equal to 1 if the subject received the message "No breach has occurred" in the treatment session.	-	-	-	-	127	0.287	0.455	0	1	101

Table 3: Probability of Information Disclosure by Treatment and Test ResulT in Period 1

D1, D2,...,D4 are dummy variables equal to 1 when the conditions in the parentheses () are met. The variable treatment is equal to one if the notification procedure is implemented and 0 otherwise. The variable below is equal to 1 if the individual is below the median result of the group, and 0 otherwise (see also Table (2)). For example, D1 is equal to 1 if the individual belongs to the No Notification treatment (i.e., treatment=0) and is above the median (i.e., below=0). The reported descriptives represent the average of disclosure in period 1 over dummies: it corresponds to the probability of observing an individual who discloses the information in each category.

	Probability of Disclosure in Period 1
D1 (i.e. treatment=0 & below=0)	0.542
D2 (i.e. treatment=0 & below=1)	0.309
D3 (i.e. treatment=1 & below=0)	0.603
D4 (i.e. treatment=1 & below=1)	0.256
Total observations	228

Table 4: Differences in Probability of Disclosure between Treatments and Test Results in Period 1

The table reports the differences in the average probability of disclosing the information in period 1 across the different categories identified in Table (3). The variable treatment is equal to 1 if the notification procedure is implemented, and 0 otherwise. The variable below is equal to 1 if the individual is below the median result of the group, and 0 otherwise (see also Table (2)).

	Difference	TTEST	PRTEST	Mann-Whitney
1) Differences between treatment=1 & treatment=0 when Below=0 (i.e. D3- D1)	0.062	0.242	0.240	0.481
2) Differences between treatment=1 & treatment=0 when Below=1 (i.e. D4-D2)	-0.053	0.283	0.281	0.564
1) Differences between types (i.e. Below=1 vs Below=0) when treatment=0 (i.e. D2-D1)	**-0.232**	**0.005**	**0.005**	**0.009**
2) Differences between types (i.e. Below=1 vs Below=0) when treatment=1 (i.e. D4-D3)	**-0.348**	**0.000**	**0.001**	**0.001**

Table 5: DESCRIPTIVES

D5, D6, ,...,D14 are dummy variables equal to 1 when the conditions in the parentheses () are met. Disclosure in period 2 is a dummy variable equal to 1, if the individual revealed his personal information in the second period. The variable treatment is equal to 1 if the notification procedure is implemented, and 0 otherwise. The variable below is equal to 1 if the individual is below the median result of the group, and 0 otherwise. The variable buy is equal to 1 when the individual bought a voucher in the first period, and 0 otherwise (see also Table (2)). For example, D5 is equal to 1, if the individual belongs to the No-notification treatment (i.e. treatment=0), did not buy a voucher in the first period (i.e. buy=0) and is above the median (i.e. below=0). The reported descriptives represent the average of disclosure in period 2 over dummies: it corresponds to the probability of observing an individual who disclose the information in each of the categories.

	PROBABILITY OF DISCLOSURE IN PERIOD 2
D5 (i.e. treatment=0 & buy=0 & below=0)	0.145
D6 (i.e. treatment=0 & buy=1 & below=0)	0.949
D7 (i.e. treatment=0 & buy=0 & below=1)	0.083
D8 (i.e. treatment=0 & buy=1 & below=1)	0.842
D9 (i.e. treatment=1 & buy=0 & below=0)	0.174
D10 (i.e. treatment=1 & buy=0 & below=1)	0.097
D11 (i.e. treatment=1 & buy=1 & below=0 & breach message =1)	0.933
D12 (i.e. treatment=1 & buy=1 & below=0 & no breach message=1)	1
D13 (i.e. treatment=1 & buy=1 & below=1 & breach message =1)	0.333
D14 (i.e. treatment=1 & buy=1 & below=1 & no breach message=1)	0.778
Total observations	228

Table 6: PROBABILITY OF DISCLOSING IN PERIOD 2: MEAN COMPARISONS

The table reports the differences in the average probability of disclosing the information in period 2 across the different categories identified in Table (5).

	Between Treatment			
	Difference	TTEST	PRTEST	Mann-Whitney
1) Breach Message when Below=0 (i.e. D11-D6)	-0.015	0.415	0.413	0.827
2) Breach Message when Below=1 (i.e. D13-D8)	-0.509	**0.027**	**0.025**	**0.056**
3) No-breach Message when Below=0 (i.e. D12-D6)[a]	0.051	0.156	0.151	0.307
4) No-breach Message when Below=1 (i.e. D14-D8)	-0.064	0.346	0.339	0.684
	Within Treatment			
	Difference	TTEST	PRTEST	Mann-Whitney
5) Breach Message vs No Breach Message when Below=0 (i.e. D11-D12)	-0.067	0.127	0.121	0.248
6) Breach Message vs No Breach Message when Below=1 (i.e. D13-D14)	-0.444	**0.094**	**0.079**	0.176
Below=1 vs Below=0 when Breach Message is given (i.e. D13-D11)	-0.600	**0.004**	**0.006**	**0.013**
Below=1 vs Below=0 when No-breach Message is given (i.e. D12-D14)	-0.222	**0.015**	**0.014**	**0.032**