Journal of Economic Behavior & Organization 123 (2016) 138–148

Contents lists available at ScienceDirect

Journal of Economic Behavior & Organization

journal homepage: www.elsevier.com/locate/jebo

Disclosure of personal information under risk of privacy shocks

Francesco Feri[a], Caterina Giannetti[b], Nicola Jentzsch[c,*]

[a] Department of Economics, Royal Holloway, University of London, United Kingdom
[b] Department of Economics, University of Jena, Germany
[c] Deutsches Institut für Wirtschaftsforschung (DIW Berlin), Mohrenstrasse 58, 10117 Berlin, Germany

ARTICLE INFO

Article history:
Received 16 August 2013
Received in revised form 27 August 2015
Accepted 4 December 2015
Available online 25 December 2015

JEL classification:
D43
L14
O30

Keywords:
Privacy
Information sharing
Data protection

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.

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% 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.

* Corresponding author. Tel.: +49 030 897 89 0; fax: +49 897 89 103.
E-mail addresses: francesco.feri@rhul.ac.uk (F. Feri), caterina.giannetti@uni-jena.de (C. Giannetti), njentzsch@diw.de (N. Jentzsch).

http://dx.doi.org/10.1016/j.jebo.2015.12.001
0167-2681/

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* 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 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 private/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

[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*.

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