

My Data is Mine - Users' Handling of Personal Data in Everyday Life

Sven Bock¹

Abstract: This experimental study is about investigating users' handling of personal data and their awareness of data collection. A deception experiment was designed to let the subjects believe that they are participating in a decision-making experiment. Only after the experiment, they were informed about the actual aim of examining their behaviour towards their personal data. Before the deception experiment either a printed or a digital version of the terms and conditions was handed out. The reading time and the willingness to accept the terms and conditions were measured in order to find significant differences. For the deception, a program was implemented which simultaneously presents two terms including sensitive data like religious and political orientations. The subject should choose the favoured term. Afterwards, subjects were asked whether and to what extent they agree to hand out their collected data to third parties in exchange for financial gain. After the experiment the participants were asked about their usual behaviour regarding their personal data.

Keywords: Terms and conditions, Privacy, Transparency, End user license agreement, Personal data, Data collection.

1 Introduction

“I accept”. These are the words you get confronted with at the end of each online transaction. It does not matter if it is the purchase of a physical item or an application. In any case the agreement is demanded by the declaration of consent. Often those terms are extensive and complicated written in legal language, so that very few users understand them. End users are usually unaware of the extent to which their data and rights are being used and the consequences of having them handed out. Especially nowadays in the era of technology, in which 86% of all households own a computer 58% of the german-speaking population a smartphone and 26% of them a tablet, the subject of data protection and data security should be highly valued.

Companies spend a lot effort collecting and analysing users' data. The high value of the data could be explained by the fact that the market is becoming more and more saturated and the companies strive for the one-to-one marketing with additional information about the costumer behaviour [Ba00]. Various concepts and techniques are increasing the efficiency and enable targeted marketing strategies and sales programs. The goal is to influence the people's consumer behaviour so that they acquire products promoted by the company. In addition to consumer behaviour, personality profiles are created which, among other things, allow an assessment of the creditworthiness. A survey in the US found that

75% of the population believe they have lost control over their personal information and thus are seeing themselves as “glass consumers” which are vulnerable to manipulations by companies and felt that companies manage too much personal information. A similar attitude is shown regarding privacy toward state authorities, as for an example a survey in Germany showed [Ku]. With an increasing amount of data and analysis possibilities in the hand of companies and state authorities, an increasing amount of monitoring and control of individuals is possible. This development is boosted by global players like Alphabet Inc., Amazon and Facebook which are omnipresent. It is assumed that the ownership of a mobile phone is always associated with the disclosure of information to large corporations which allows them to create a detailed profile of the customers. Goal of this empirical study is to examine if people are aware of handing out their data and how serious this problem is perceived. In the next step a solution should be found to make people more sensible with handing out private data.

2 Current state of research

The time when mobile phones were only used for verbal communication is long gone. Because of the faster mobile data connection smartphones and tablets are preferably used to receive information and services, such using emails, social networks, financial and health services, and other services [St]. This results in an increasing number of applications on the market offering various services. It is questionable how safe it is for someone to move through this mobile and digital world. Previous incidents have revealed numerous vulnerabilities in commonly known applications [Ki] as well as attacks from malicious software. Therefore, a secure mobile environment is currently not given. There is a large number of risks in the field of mobile devices, which concerns malware as well as the theft of confidential information and the reading of text messages. Thus, data security and privacy are a major concern for businesses and mobile end users [JS12]. Despite the popularity of smartphones, there are reasons to believe that due to concerns about security and privacy, the full potential of mobile devices is not being exploited by the users. A recent study found that 60% of smartphone users are concerned about financial and personal security risks in mobile payments [Ch12].

While end users often claim that data privacy is important for them, their actual behaviour towards sharing data and rights or installing applications is permissive. However, some studies show that privacy plays a relevant role in the installation decision. Users would always choose the applications with better privacy policies if functionality is not compromised [Go05]. The difference between the intention to protect private data and the actual permissive behaviour of individuals is known as the Private Paradox. This paradox is often explained with the Private Calculus, meaning that individuals perform a cost-benefit calculation in a situation where they can disclosure private data in order to gain compensation. This approach has been expanded by Acquisti and others to include factors such as incomplete information and the desire for instant gratification. In doing so it was transformed from a rational based explanation towards an explanation based on behavioural science [ABL15].

Terms and conditions are clear indicators for security and privacy level. Few users pay attention to these agreements before installing an application. Although, surprisingly, 60% of end users say that they consider the shared rights “sometimes” or “always”. Even though, the shared rights are classified as fairly unimportant. These findings suggest that end users rely more on reviews and recommendations than on the difficult-to-understand conditions of security and privacy [Ch12]. In general, end users are unaware of the serious impacts of confirming a dialogue box in economic, social and legal terms. Considerable attention and cognitive effort would be needed to respond appropriately to those dialogues. Both are often absent because the user usually gets into this situation while he wants to do another primary task which has to be interrupted.

3 Research Question

Goal of this study is to determine if people are aware of handing out their data and how serious this problem is perceived. Furthermore the thesis is eliciting the value people assign to their private data. The study focuses on the field of mobile devices, because of their increasing importance. Following hypothesis were postulated:

H1: Although users claim that data protection is important to them, their actual indifferent behaviour regarding data protection is caused by undiscerned consequences. There are three distinguishable parts in this hypothesis:

H 1.1: Users report that it is important to protect their data but do not behave accordingly.

H 1.2: Users are not aware of the consequences while handing out their data and rights.

H 1.3: Their indifferent behaviour regarding data protection is caused by undiscerned consequences.

Hypothesis 1.1: This hypothesis is based on the privacy paradox which claims that intend and behaviour regarding data privacy differ. On one side people were revealing that data security and data protection are highly relevant for them and for their choice of online shops. Especially the transparency of the terms and conditions has a high importance. On the other side they are permissively handing out their data for getting a better service [Kö15].

Hypothesis 1.2: Studies showed that end-users do not read contracts. This phenomenon extends from paper-contracts to CTAs [BMWT09]. Plaut and Bartlett examined individual reasons for not reading contracts, among them are length and complexity of the contract [PBI12]. Based on this behaviour it can be assumed that end-users are uncertain about the consequences of handing out personal data.

Hypothesis 1.3: This hypothesis builds a causal connection between H 1.1. and H 1.2.: The indifferent behaviour is caused by being unaware of the consequences of handing of private data. This is based on Mischels delay-of-gratification paradigm which shows that people tend to favour short-term over long-term benefits even though the long-term benefits are more substantial [Mi10]. In this case the short-term benefit is the functions of an application while the long-term benefit is the maintenance of privacy.

H2: The users are handing out their information for a low compensation.

Hypothesis 2: A study of Staiano et. al. showed that people are willing to sell their data for a low compensation regardless of their socio financial background [St14].

4 Experimental Setup and Design

An experiment was designed consisting of six steps which are illustrated in Fig. 1. One important consideration during the development was the response behaviour of the subjects regarding data protection which was assumed to be given according to social expectations. Regarding this, a deception experiment setup has been chosen as the goal was to examine the actual behaviour and not the pretended opinion. The subjects were made to believe that they are participating in a decision-making experiment. Actually, a closer look has been taken on the behaviour towards the release of personal data in exchange of financial offsets.

In the decision-making experiment the user had to choose between two opposing terms for 450 times. The chosen terms included private issues such as political and religious orientation. In this phase of the experiment the focus was put on the users' behaviour towards the agreement procedure of the terms and conditions to participate on the experiment. The terms of this agreement were designed exaggerated, so while reading the subjects could be aware that they were handing out all their rights and information. One example is that the terms and conditions included a permission to hand out personal data without any beforehand approval. The sample was divided into two groups. One group got the agreement presented in paper form while the other group got it in digital form as a click-through agreement. For both groups the users' reading time for the agreement was measured.

After completing the decision-making experiment, the subjects were told that their data would be of interest to other institutions as well. Six groups of universities and companies were presented to them. The subject should decide whether and to whom the data should be passed. For choosing not to pass the data at all the lowest financial compensation was promised. Users were offered a higher financial compensation if they choose to share their data with more institutions. This was followed by a short interview including seven questions for examining if the testee noticed something strange and aiming to get subjective impressions about handing out the data. The interview was followed by a questionnaire with 22 questions, inquiring the subjects' usual behavior while installing new mobile applications. Furthermore the participants were asked about which data they think is handed out by the application and the assumed financial value of their personal data. In addition to the present experiment, the questionnaire was also used as an online survey. Aim is to examine if there is a significant difference between the two samples, especially since the people that participated in the experiment had just been in a situation in which they had been confronted with their handling of private data.

At the end it was revealed to the participants that they took part in a deception experiment. Also all participants received the same financial compensation, regardless of their choice of data transfer. The experimental design was accepted by the Ethics committee

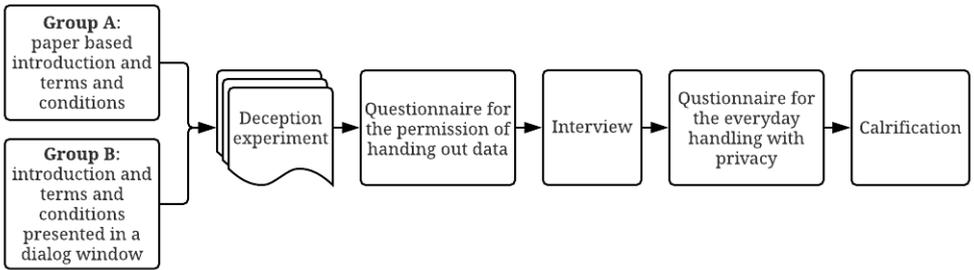


Fig. 1: Chronological process of the study.

after implementing some improvements. 51 participants were recruited using the online test person portal from the Technical University of Berlin, from which 20 of them were male. The average age was 31.27 years (SD 10.22; range: 18-64 years).

5 Results

While a thorough analysis of the data is still ongoing, a first descriptive evaluation shows that all participants ($N = 51$) signed the agreement. The mean reading time for the agreement in paper form was: $M = 58.29s$, $SD = 53.25s$ and for the digital form: $M = 51.79s$, $SD = 52.47s$. The agreement contained 833 words while the average reading speed is about 250 words per minute. This points out that the agreement has not been read completely regarding the average reading time.

On the other hand, in the questionnaire the participants pointed out that the protection of their private data is highly valued. On an eleven-staged rating scale (0 lowest, 10 highest value) more than 23% had chosen the highest value. Also 86% of the participants had chosen to share their data with the highest amount of institutions, for the highest financial gain, followed by 10% for the second highest compensation only 4% took the option not to share their data at all. At the end of the experiment, it was observed that the testees invested a lot more time in reading the clarification in contrast to the agreement before.

6 Conclusion

The rough analysis of the presented experiment has already indicated that people show a paradoxical behaviour regarding the value of their data and the actual treatment of them. This points out that the issue is a very interesting field of research and that the data of the experiment should be deeper analysed, especially regarding the increasing number of mobile device users. The next step is to find a solution for educating mobile device users and to make them more sensitive with handing out their data to prevent them of being transparent consumers.

References

- [ABL15] Acquisti, Alessandro; Brandimarte, Laura; Loewenstein, George: Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.
- [Ba00] Baeriswyl, Bruno: Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut. *Recht der Datenverarbeitung*, 1:6–11, 2000.
- [BMWT09] Bakows, Y; Marotta-Wurgler, F; Trossen, DR: Does anyone read the fine print. A test of the informed minority hypothesis using clickstream data. *New York University School of Law Working Paper*, 2009.
- [Ch12] Chin, Erika; Felt, Adrienne Porter; Sekar, Vyas; Wagner, David: Measuring user confidence in smartphone security and privacy. In: *Proceedings of the eighth symposium on usable privacy and security*. ACM, p. 1, 2012.
- [Go05] Good, Nathaniel; Dhamija, Rachna; Grossklags, Jens; Thaw, David; Aronowitz, Steven; Mulligan, Deirdre; Konstan, Joseph: Stopping spyware at the gate: a user study of privacy, notice and spyware. In: *Proceedings of the 2005 symposium on Usable privacy and security*. ACM, pp. 43–52, 2005.
- [JS12] Jain, Anurag Kumar; Shanbhag, Devendra: Addressing security and privacy risks in mobile applications. *IT Professional*, 14(5):28–33, 2012.
- [Ki] King, R.: ViaForencis: Netflix, Foursquare Apps Leave Sensitive Data Vulnerable. *ZDNet.com*, 2011.
- [Kö15] Köln, IFH: , Perspektiven für den Datenschutz in Europa aus der Sicht der Verbraucher und des (elektronischen) Handels, 2015.
- [Ku] Kurz, Constanze: Eco - Verband der Internetwirtschaft e.V., Umfrage zur Vorratsdatenspeicherung im Juni 2015. <https://netzpolitik.org/2015/umfragen-zur-vorratsdatenspeicherung-klare-mehrheit-gegen-wiedereinfuehrung/> Accessed: 25/11/2017.
- [Mi10] Mischel, Walter; Ayduk, Ozlem; Berman, Marc G; Casey, BJ; Gotlib, Ian H; Jonides, John; Kross, Ethan; Teslovich, Theresa; Wilson, Nicole L; Zayas, Vivian et al.: ‘Willpower’ over the life span: decomposing self-regulation. *Social cognitive and affective neuroscience*, 6(2):252–256, 2010.
- [PBI12] Plaut, Victoria C; Bartlett III, Robert P: Blind consent? A social psychological investigation of non-readership of click-through agreements. *Law and human behavior*, 36(4):293, 2012.
- [St] Statistisches Bundesamt. Anteil der privaten Haushalte in Deutschland mit einem Computer im Zeitraum 1998 bis 2015 (Stand: 1. Quartal 2015). <http://de.statista.com/statistik/daten/studie/2596/umfrage/ausstattungsgrad-privater-haushalte-mit-einem-pc-seit-1998/>. Accessed: 25/11/2017.
- [St14] Staiano, Jacopo; Oliver, Nuria; Lepri, Bruno; de Oliveira, Rodrigo; Caraviello, Michele; Sebe, Nicu: Money walks: a human-centric study on the economics of personal mobile data. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, pp. 583–594, 2014.