Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2022 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-11-2022

Perceived privacy violations through information sharing with external parties – Diving into user perceptions and reactions

Christina Wagner
University of Augsburg, christina.wagner@uni-a.de

Manuel Trenz
University of Goettingen

Chee-Wee Tan
Copenhagen Business School

Daniel Veit
University of Augsburg

Follow this and additional works at: https://aisel.aisnet.org/wisp2022

Recommended Citation

Wagner, Christina; Trenz, Manuel; Tan, Chee-Wee; and Veit, Daniel, "Perceived privacy violations through information sharing with external parties – Diving into user perceptions and reactions" (2022). *WISP 2022 Proceedings*. 6.
https://aisel.aisnet.org/wisp2022/6

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Perceived Privacy Violations through Information Sharing with External Parties – Diving into User Perceptions and Reactions

Christina Wagner[1]
University of Augsburg,
Augsburg, Germany

Manuel Trenz
University of Goettingen,
Goettingen, Germany

Chee-Wee Tan
Copenhagen Business School,
Copenhagen, Denmark

Daniel Veit
University of Augsburg,
Augsburg, Germany

ABSTRACT

We see more and more incidents where user information collected by digital services is shared with external parties. Users becoming aware of such information (mis-)uses may perceive a privacy violation. In this study, we want to understand when, why, and how the sharing of information with external parties is perceived as a privacy violation and what consequences such a perception entails. Employing the Critical Incident Technique (CIT) as a methodology, we inductively derive characteristics of real-world incidents of perceived privacy violations due to the sharing of information with external parties and users' perceptions and reactions thereto. We present preliminary results of our first qualitative data analysis as well subsequent steps to advance this research in progress.

Keywords: Privacy Violation, Data Misuse, Unauthorized Secondary Use, External Parties, Critical Incident Technique, Qualitative Analysis

INTRODUCTION

We see signs of increasing data sharing across organizations. More and more user data is collected through online activities – with the trend rising due to developments of the Internet of Things (IoT), connected cars, voice input, or other smart devices (Cichy et al. 2021). At the same

[1] Corresponding author. christina.wagner@uni-a.de +49 821 598 4409

time, new business models and services such as big data analytics and behavioral advertising pose more possibilities of creating value from such data (Culnan 2019; Grover et al. 2018). Google's ad revenue, for example, amounted to 209.49 billion U.S. dollars in 2021 (Statista 2021). While digital services need to leverage the value inherent to user data to remain competitive, they need to make sure to protect their users' privacy to retain them (Gerlach et al. 2019).

Inherent to such data uses is the combination of data originally collected for different purposes and from different sources (Culnan 2019). From the perspective of fair information practices, digital services shall only disclose to external parties personal information collected about their users for purposes that the user has given their consent to (Culnan 2019). Similarly, the General Data Protection Regulation (GDPR) requires users' consent to the sharing of personal information by a digital service they use for specific purposes. Anonymized data sets are, however, exempt from such regulations (GDPR 2018).

Digital services may therefore legally share user information with external parties in anonymized ways or on the basis of legal consent – however, users might not be aware of the sharing or of having given consent. Some digital services may also share user information in illegitimate ways. Either way, when digital services engage in such sharing activities and a user finds out about it, they might perceive it as something they have not consented to or do not want to be done with their data (i.e., a privacy violation). Recent (e.g, Cambridge Analytica (Kurtz et al. 2018)) as well as more distant history (e.g., Lotus Marketplace: Households (Culnan 1993)) have shown a variety of cases where the sharing of user information with external parties led to a public outcry. Consequentially, users may discontinue using a digital service, engage in legal actions, or spread negative word-of-mouth (Choi et al. 2016; Drake et al. 2021).

Prior research has used the term privacy violations in a variety of scopes and with different foci. We understand perceived privacy violations as a user suspecting or being aware that a digital service they have used shares information collected about them with external parties in a way the user thinks they have not authorized. We further specifically consider the digital service – rather than the external party that the information may be shared with – as the main actor within the perceived privacy violation.

Prior research identified the organizational practice of unauthorized secondary external use as a dimension of privacy concerns (Smith et al. 1996). More recent studies delved into specific relationships between characteristics of perceived privacy violations therefrom and individuals' responses thereto experimentally (Drake et al. 2021; Keil et al. 2018). We want to pick up this in today's digital economy widespread conduct of digital services sharing user information with external parties – and take one step back to understand this phenomenon and related ramifications for the user through an exploratory lens. We aim to understand when, why, and how exactly such conduct of digital services is suspected, perceived, and what consequences it entails – both attitudinally, as well as behaviorally. To guide this understanding, we pose the research questions: *When and why do users perceive digital services sharing their information with external parties as a privacy violation? How do users respond to such perceived privacy violations?*

Employing the methodological approach of the Critical Incident Technique (CIT), we gain inductively derived insights on characteristics of perceived privacy violations and customers' responses thereto. We combine that with a configurational approach of matching those experiences with their resulting intentions of continuing to use the respective digital service through Qualitative Comparative Analysis (QCA).

The upcoming sections will provide an overview on the background on privacy violations in IS literature. Thereafter, we will lay out our methodological process and provide details on our data collection. Finally, we will present the preliminary results of the qualitative analysis of our data collection up to this point. We will end with a short discussion of these results as well as the next steps planned in this research project.

THEORETICAL BACKGROUND ON PRIVACY VIOLATIONS

We will provide a short overview and synthesis of prior IS research on privacy violations and related concepts. Generally, privacy violations occur, “when an organization, in its efforts to pursue the organization’s objectives, collects, stores, manipulates, or transmits personal information unbeknownst to the individual" (Hann et al. 2007, p. 15). They can be classified along the attribution of their causes (Weiner 1985). On the one hand, they can be intentional, where the “cause of the wrongdoing can be attributed to the purposive action” (Keil et al. 2018, p. 821) of the digital service. Examples for such intentional violations include insider theft, selling, or sharing user information with external parties (Choi et al. 2016). On the other hand, privacy violations can be unintentional. Here, causes of wrongdoing lie outside of the purposive action of the digital service. Privacy violations can further be stable or unstable (Keil et al. 2018). Stable means privacy violations that are continuous and do no change over time (e.g., ongoing sharing of user information with external parties). Unstable means a one-time event that is subject to change (e.g., user information is shared with an external party by means of a one-time transaction) (Keil et al. 2018). The term privacy violations is sometimes used synonymously with the term privacy breaches. More often, however, privacy violations describe intentional causes (Drake et al. 2021; Keil et al. 2018; Zhang et al. 2022), whereas privacy breaches refer to its unintentional sibling as "unauthorized access to personal information,

resulting from a variety of security incidents including hackers breaking into systems or networks, external parties accessing personal information on lost laptops or other mobile devices, or organizations failing to dispose of personal information securely." (Culnan and Williams 2009, p. 675). We specifically focus on privacy violations that are attributed as intentional by a digital service, which can be either stable or unstable.

Privacy violations by digital services have been considered from a variety of angles and contexts in IS research. Some research has focused on understanding perceptions and consequences of privacy violations (Choi et al. 2016; Drake et al. 2021; Keil et al. 2018). Others suggested or evaluated strategies to prevent privacy violations for organizations and thereby mitigate users' concerns (Culnan 2019; Hann et al. 2007). Yet another angle is to consider compliance with privacy rules (Wall et al. 2016) and privacy policies (Culnan 2019; Drake et al. 2021). These studies have mostly been situated in the realm of health information, as well as more broadly in online organizations.

In addition to the organizational setting, privacy violations in online settings (mainly in the context of social media) can also involve another individual responsible for intruding someone's online privacy (Choi et al. 2015; Ozdemir et al. 2017; Zhang et al. 2022).

Finally, studies on privacy violations may or may not focus on the sharing of information with external parties as a reason for the privacy violation – they may also consider data misuse more generally (Culnan 2019; Hann et al. 2007). We however, as defined previously, focus specifically on privacy violations in terms of a digital service sharing information they collect about a user with external parties. Such privacy violations have been considered by Keil et al. (2018) in a healthcare and Drake et al. (2021) in a social media context through experimental methods. Potential differences between perceptions of privacy violations related to information

sharing with external parties as compared to other types of privacy violations motivate our research endeavor to further understand perceptions of the former through exploratory means.

METHODOLOGY

In line with the exploratory nature of our study, we follow the approach of CIT (Flanagan 1954) to identify incidents where users become aware or suspect that a digital service they use shared their information with external parties. Guided by the steps proposed by Flanagan (1954) and Tan et al. (2016), we build an online survey questionnaire containing both open-ended and closed-ended questions: (1) We specify the aim of the study and provide clear explanations of the incidents we are looking for. (2) We ask participants to report the most recent incident they experienced that relates to our specification so that they may recall it most accurately. We pose open-ended questions to elicit details on the situation, feelings, activities, opinions, and consequences to the incident. We then pose closed-ended questions on continuance intentions based on established scales in prior IS research (Bhattacherjee 2001). (3) We select respondents based on their familiarity with the incident – meaning only participants able to recall an incident as described are able to participate in the questionnaire. (4) We analyze the qualitative data collected on incidents with the objective of establishing a classification of their characteristics. We employ qualitative coding techniques, inspired by (Gioia et al. 2013), to guide our qualitative data analysis. (5) To avoid biases in our categorization of incidents and effects thereof, we conduct an iterative approach to data collection. With each iteration, categories are refined, triangulated with existing research, until theoretical saturation is reached.

PRELIMINARY RESULTS OF QUALITATIVE DATA ANALYSIS

We conducted our first rounds of data collection in September 2022 via Prolific Academic, collecting 25 valid cases of critical incidents reported by users of digital services

from the United Kingdom. Table 1 shows an overview of the results from our qualitative analysis classifying those incidents.

Table 1. Overview of coding

Third-Order Codes	Second-Order Codes	Illustrative Example of First-Order Code and Quotation
Observable consequence	• Phishing • Spam • Advertisement • Receiving unwanted contact • Someone else receiving unwanted contact	Received a lot of spam email the week following the incident: "I received a lot of spam emails for week following this" (ID333, CV Spotlight)
Cause attribution to incident	• Internal attribution • External attribution • Legitimate • Illegitimate • Isolated • Recurring	Incident happened because of clicking on an advertisement: "if I do click on an ad via Facebook, Google and other social media platforms will then share more of those items or similar with me when I visit those sites." (ID347, Facebook)
Base for certainty of cause attribution	• Recognizing information • Hearsay • Timing • Instinct	Recognized digital service as the responsible as they use separate emails for different purposes: "I use specific email addresses for certain things to keep business and personal activities separate and this was a specific email that I only use for travel arrangements and affairs" (ID323, Flightright)
General dispositions towards information sharing with external parties	• Accepting as a common practice • Not accepting as is • Tolerating • Not accepting at all • No opinion	Thinks that digital services in general engaging in unauthorized information sharing is something that happens more than we like: "I think this probably happens more than we would like and more than we realise." (ID374, Facebook)
Feelings triggered through the incident	• Incident triggered angry feelings • Incident triggered anxious feelings	Feels worried: "it is worrying because I can't even feel safe having a conversation in my own home" (ID371, Facebook)
Perceptions of the incident	• Incident not wanted • Incident perceived neutrally or apathetically • Incident perceived positively	Finds that they are capable themselves searching for products and do not need help from targeted advertisement: "I am perfectly capable of searching for the products I need and do not need emails to help." (ID373, Facebook)

Confirmed vs. disconfirmed expectations	• Disconfirmed expectations / being negatively surprised • Confirmed expectations	Did not expect such behavior from digital service: "Annoyed at such a reputable company for doing that. I didn't expect it from them. I was disappointed." (ID342, EE)
External rectification actions	• Complaining at digital service • Complaining externally • Negative Word-of-Mouth • Gathering evidence	Made a formal complaint at digital service after the incident but digital service denied having shared the information: "I made a formal complaint and they still denied it." (ID358, eBay)
Internal rectification actions	• Ignoring consequences • Handling consequences • Information restriction / removal with the digital service • Information restriction / removal outside of the digital service • (…)	Stopped a certain job as a consequence of information being shared too many times: "I have also stopped doing the job now as my details have been sent on and used too many times" (ID321, Unsure)

Our preliminary findings give a first indication that most users perceive information sharing with external parties by a digital service they have used quite negatively. At the same time, most of the actions they take are directed towards changing their own behavior, not the behavior of the digital service responsible.

OUTLOOK

As a next step, we want to further refine our presented qualitative data analysis. Subsequently, we plan to employ QCA. QCA is a methodology based on set analytic approaches that enables the analysis of complex causal conditions (Ragin 1987). We apply QCA to understand how different configurations of our inductively derived characteristics of perceived privacy violations through digital services sharing information with external parties relate to the user's intention to continue using that digital service. In consistency with our iterative approach described above, depending on the outcome of the QCA, we will continue with the next iteration of data collection.

REFERENCES

Bhattacherjee, A. 2001. "Understanding Information Systems Continuance: An Expectation-Confirmation Model," *MIS Quarterly* (25:3), pp. 351–370.

Choi, B. C. F., Jiang, Z. J., Xiao, B., and Kim, S. S. 2015. "Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding," *Information Systems Research* (26:4), pp. 675–694.

Choi, B. C. F., Kim, S. S., and Jiang, Z. J. 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904–933.

Cichy, P., Salge, T. O., and Kohli, R. 2021. "Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars," *MIS Quarterly* (45:4), pp. 1863–1891.

Culnan, M. J. 1993. "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341–363.

Culnan, M. J. 2019. "Policy to Avoid a Privacy Disaster," *Journal of the Association for Information Systems* (20:6), pp. 848–856.

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and Tjx Data Breaches," *MIS Quarterly* (33:4), pp. 673–687.

Drake, J. R., Furner, C. P., and Mehta, N. 2021. "Privacy Policy Violations: A Corporate Nexus of Healthcare Providers and Social Media Platforms," *WISP 2021 Proceedings*, p. 17.

Flanagan, J. C. 1954. "The Critical Incident Technique," *Psychological Bulletin* (51:4), pp. 327–358.

GDPR 2018. "General Data Protection Regulation (GDPR)," in *2016/679*.

Gerlach, J., Eling, N., Wessels, N., and Buxmann, P. 2019. "Flamingos on a Slackline: Companies' Challenges of Balancing the Competing Demands of Handling Customer Information and Privacy," *Information Systems Journal* (29:2), pp. 548–575.

Gioia, D. A., Corley, K. G., and Hamilton, A. L. 2013. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), pp. 15–31.

Grover, V., Chiang, R. H. L., Liang, T.-P., and Zhang, D. 2018. "Creating Strategic Business Value from Big Data Analytics: A Research Framework," *Journal of Management Information Systems* (35:2), pp. 388–423.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13–42.

Keil, M., Park, E. H., and Ramesh, B. 2018. "Violations of Health Information Privacy: The Role of Attributions and Anticipated Regret in Shaping Whistle-Blowing Intentions," *Information Systems Journal* (28:5), pp. 818–848.

Kurtz, C., Semmann, M., and Schulz, W. 2018. "Towards a Framework for Information Privacy in Complex Service Ecosystems," *ICIS 2018 Proceedings*.

Ozdemir, Z. D., Smith, H. J., and Benamati, J. H. 2017. "Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study," *European Journal of Information Systems* (26:6), pp. 642–660.

Ragin, C. C. 1987. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*, Berkeley, CA, USA: University of California Press.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196.

Statista 2021. *Google: Advertising Revenue 2021*. in *Statista* Retrieved 29. September, 2022, from https://www.statista.com/statistics/266249/advertising-revenue-of-google/.

Tan, C.-W., Benbasat, I., and Cenfetelli, R. T. 2016. "An Exploratory Study of the Formation and Impact of Electronic Service Failures," *MIS Quarterly* (40:1), pp. 1-A31.

Wall, J. D., Lowry, P. B., and Barlow, J. B. 2016. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association for Information Systems* (17:1), pp. 39–76.

Weiner, B. 1985. "An Attributional Theory of Achievement Motivation and Emotion," *Psychological Review* (92), pp. 548–573.

Zhang, N. (Andy), Wang, C. (Alex), Karahanna, E., and Xu, Y. 2022. "Peer Privacy Concern: Conceptualization and Measurement," *MIS Quarterly* (46:1), pp. 491–529.