5-2-2023

PERCEIVED PRIVACY VIOLATIONS THROUGH UNAUTHORIZED SECONDARY USE – DIVING INTO USERS' PERCEPTIONS AND RESPONSES

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

Manuel Trenz
University of Goettingen, trenz@uni-goettingen.de

Chee-Wee Tan Professor
Copenhagen Business School, ct.digi@cbs.dk

Daniel Veit
University of Augsburg, daniel.veit@uni-a.de

PERCEIVED PRIVACY VIOLATIONS THROUGH UNAUTHORIZED SECONDARY USE – DIVING INTO USERS' PERCEPTIONS AND RESPONSES

Research in Progress

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

Manuel Trenz, University of Goettingen, Goettingen, Germany, trenz@uni-goettingen.de

Chee-Wee Tan, Copenhagen Business School, Copenhagen, Denmark, ct.digi@cbs.dk

Daniel Veit, University of Augsburg, Augsburg, Germany, daniel.veit@uni-a.de

Abstract

We see more and more incidents where users' 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 such external unauthorized secondary use (EUSU) is perceived as a privacy violation and what consequences such a perception entails. Employing the Critical Incident Technique (CIT), we inductively derive characteristics of real-world incidents of perceived privacy violations through EUSU and users' perceptions and responses thereto. We present preliminary results of our qualitative data analysis as well as potential contributions of this research-in-progress study. As a next step, we plan to relate characteristics with responses through Qualitative Comparative Analysis (QCA).

Keywords: Privacy Violations, External Unauthorized Secondary Use, External Parties, Critical Incident Technique.

1 Introduction

Information privacy research has started to study *external unauthorized secondary use of information* (EUSU) thirty years ago (Culnan, 1993; Smith et al., 1996) – as an individual's concern that their information is collected for one purpose, but then used for another purpose through disclosing it to an external party (Smith et al., 1996). Since then, consumer perceptions and sensitivities towards organizations collecting and using their information have changed (Hann et al., 2007). One reason is that developments in our digital economy have made the gravity of such data uses much more salient. More user data is collected through online activities – with the trend rising due to developments of the Internet of Things, connected cars, voice input, or other smart devices (Cichy et al., 2021). At the same time, new business models and services such as big data analytics and behavioural 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). With these developments, EUSU has been increasingly regulated. The General Data Protection Regulation (GDPR) requires users' consent to the sharing of personal information collected by a digital service they use for specific purposes. Anonymized data sets are, however, exempt from such regulations (GDPR., 2018).

Digital services may legally engage in external secondary uses of user information in anonymized ways or on the basis of legal consent – however, users might not be aware of the sharing or of having given consent – perceiving it as unauthorized. 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). While digital services want 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).

Prior research has used the term privacy violations in a variety of scopes and with different foci. We understand *perceived privacy violations through EUSU* 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 did not authorize. We 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. We define digital services as services that are delivered digitally and are highly dependent on access to user information to create and deliver value for their users (e.g., mobile applications, digital platforms, or electronic marketplaces) (Karwatzki et al., 2022). Further, we focus on privacy violations that are attributed as intentional by a digital service, which can be either stable or unstable.

Recent research delved into specific relationships between selected characteristics of perceived privacy violations through EUSU and individuals' responses thereto through deductive approaches (Drake et al., 2021; Keil et al., 2018). We want to pick up this in today's digital economy widespread conduct of digital services engaging in EUSU – and take one step back to understand this phenomenon and related ramifications for the user through an exploratory lens. Through this exploratory lens we uncover the immediate situation surrounding the discovery of EUSU by a user. 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 behaviourally. 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 plan to 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 section 2 provides a theoretical background of relevant Information Systems (IS) literature. Thereafter, we lay out our methodological process in section 3, providing details on our data collection. In section 4, we present the preliminary results of the qualitative analysis of our data collection up to this point. We end with a short discussion of these results as well as the next steps planned in this research project in section 5.

2 Theoretical Background

In the following we provide background on prior research on unauthorized secondary use, privacy violations, and responses to privacy violations in IS literature.

2.1 Unauthorized secondary use

Generally, secondary information use refers to practices where information is collected for one purpose, but then used for a different purpose (Culnan, 1993). Secondary use can be legal and perceived by the consumer as appropriate, however it can also be perceived as a privacy violation when it occurs in an unauthorized way (Culnan, 1993). Secondary use has been theorized on as a dimension of privacy concerns (Smith et al., 1996), as well as a privacy concept on its own (Culnan, 1993).

Culnan (1993) investigates consumers' general attitudes towards secondary use (authorized or unauthorized) for the purpose of direct marketing and distinguishes between several dimensions of secondary use. First, she distinguishes between different data processing activities: acquisition, use, and transfer of customer information (Culnan, 1993; Gerlach et al., 2015). Second, in the domain of direct marketing, secondary use can relate to different types of information associated with different customer relationships. Information can either stem from transactions with existing customers, it can extend to external information about existing customers, or it can relate to information about prospective customers (Culnan, 1993).

Smith et al. (1996) theorize on dimensions of individuals' concerns about organizational information practices. These dimensions include two types of unauthorized secondary use of personal information: internal unauthorized secondary use and external unauthorized secondary use. They define internal unauthorized secondary use as "information […] collected from individuals for one purpose but […] used for another, secondary purpose without authorization from the individuals" (Smith et al., 1996, p. 171). These concerns are exacerbated when such information is disclosed to an external party. External unauthorized secondary use (EUSU) is defined as the "concern that information is collected for one purpose but is used for another, secondary purpose after disclosure to an external party (not the collecting organization)" (Smith et al., 1996, p. 172). We subsequently focus on EUSU as defined by Smith and colleagues (1996), relating to Culnan's (1993) data processing activity of transferring customer information to external parties.

Since these foundational studies, IS research delved into the effect of EUSU, either as a dimension of privacy concerns or as a distinct factor of a privacy disclosure on a user's privacy decision. It is generally found to decrease the willingness to use services that engage in such information uses (Angst and Agarwal, 2009; Gerlach et al., 2015). One exception is the study by Buckman and colleagues (2019), who largely observe null effects of secondary use of information when studied in combination with other common privacy disclosure factors (Buckman et al., 2019). Also personalized advertisement can be perceived by users as EUSU that increases perceptions of privacy violations and impacts use (Karwatzki et al., 2017; Sutanto et al., 2013; Zhu and Chang, 2016). Marketing research delved into the practice of supplementing customer information with data from other companies (Daviet et al., 2022; Schneider et al., 2017), as well as the effect of privacy breaches that occur due to such information sharing practices (Kelly et al., 2017).

With these different angles on and instantiations of EUSU, it becomes difficult to abstract a common theoretical understanding of the relationship between perceptions users have of EUSU and the consequences that result for them and subsequently for organizations engaging in such privacy practices. Our study contributes to alleviating this unclarity by delineating the boundaries of perceptions of privacy violations through EUSU as well as exploring effects of such perceptions.

2.2 Privacy violations

Generally, privacy violations occur, when organizations collect, store, manipulate, or share an individual's personal information without that individual's knowledge thereof (Hann et al., 2007). Whether such an activity, however, is perceived as a privacy violation, depends on the individual (Hann et al., 2007).

Privacy violations can be classified along the attribution of their causes (Weiner, 1985). On the one hand, they can be intentional, where the digital service's wrongdoing is attributed to acting purposefully (Keil et al., 2018). 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 violation is sometimes used synonymously with the term privacy breach. 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, third 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). As indicated in the introduction, we focus on privacy violations.

Privacy violations by digital services are considered from a variety of angles and contexts in IS research. In an organizational setting, research focuses on understanding perceptions and consequences of privacy violations (Choi et al., 2016; Drake et al., 2021; Keil et al., 2018), and evaluates strategies for organizations to prevent privacy violations and thereby mitigate users' concerns (Culnan, 2019; Hann et al., 2007). Yet another angle is the consideration of compliance with privacy rules (Wall et al., 2016) and privacy policies (Culnan, 2019; Drake et al., 2021). In addition to the organizational setting, privacy violations in the context of social media can also involve another individual responsible for intruding someone's privacy (Choi et al., 2015; Ozdemir et al., 2017; Zhang et al., 2022). Zhang and colleagues (2022) conceptualize peer privacy concern to understand this phenomenon further.

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. Many consider data misuse more generally (Choi et al., 2016; Culnan, 2019; Hann et al., 2007). Privacy violations that result specifically from EUSU have been considered by Keil and colleagues (2018) and Drake and colleagues (2021) in the context of health information through experimental methods. These studies take the privacy violation, however, as a given.

As indicated above, our study contributes by exploring the boundaries of when EUSU is perceived as a privacy violation. This is achieved by exploring perceptions, reactions, and consequences of the immediate privacy violation situation that result from a user becoming aware of EUSU.

2.3 Responses to privacy violations

In this section, we distinguish between first-order responses to privacy violations that aim at protecting one's privacy immediately after a privacy violation, and second-order responses that impact a user's relationship with the violating organization long term.

First-order responses to privacy violations are termed as privacy protective responses in prior research. Son and Kim (2008) explore user's privacy protective responses towards privacy threats in general terms. They classify these responses into refusal, misrepresentation, removal, negative word-of-mouth, complaining directly to online companies (i.e., the digital service), and complaining indirectly to third-party organizations (Son and Kim, 2008). Since then, studies gained a more fine-grained understanding towards subsets of these privacy protective responses that users take as a response to privacy violations. Choi and colleagues (2016) consider negative word-of-mouth as a privacy protective response towards firms' recovery behaviours after privacy breaches (Choi et al., 2016). Drake and colleagues (2021) focus on negative word-of-mouth and legal actions as a response to privacy policy violations related to health information (Drake et al., 2021). In an organization-internal context, Keil and colleagues (2018) explore whistleblowing of employees as a potential outcome after an organization's privacy violation (Keil et al., 2018).

While these studies gain a more fine-grained understanding towards the antecedents of these specific privacy-protective responses across a variety of contexts, the quantitative nature of these studies limits their openness towards additional responses that may not be included as a dependent variable in their studies. We want to explore whether privacy violations through EUSU result in privacy protective responses that are captured by the categorization by Son and Kim (2008), which of those privacy protective responses are more prevalent than others, and how these different privacy protective responses relate to other situational characteristics of a privacy violation through EUSU.

In addition to these more immediate privacy protective responses after a privacy violation, studies explore the longer term impact on a user's relationship with the violating organization through (dis-) continuance intentions (Drake et al., 2021; Gao et al., 2022; Zhu and Chang, 2016) and switching intentions (Choi et al., 2016). While these studies find that privacy violations overall affect these intentions, they do not consider users' actual responses of continuing to use the violating organization. Through the methodological approach of CIT, our study is able to explore such outcomes.

3 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.

In the domain of IS, critical incidents refer to "an IS product or service experience that a user considers to be unusually positive or negative" (Salo and Frank, 2017, p. 5). The technique allows respondents to describe post-incident behaviours related to IS use in their own words (Kari et al., 2020; Meuter et al., 2000). It has been successfully applied by prior studies in the IS domain, especially in the study of IS continuance (Kari et al., 2020; Salo and Frank, 2017; Serenko and Turel, 2010).

CIT presents a method for focusing on important user experiences, providing contextualized experiences about actual events, and inferring links between experiences and behaviours (Kari et al., 2020; Meuter et al., 2000). It thereby aids researchers in examining real life experiences instead of hypothetical scenarios (Flanagan, 1954; Kari et al., 2020), contributing to both a study's rigor and relevance (Serenko and Turel, 2010).

Guided by the steps proposed by Flanagan (1954) and Tan and colleagues (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 from their memory. We pose open-ended questions to elicit details on the situation, feelings, activities, opinions, and consequences to the incident. We also pose closed-ended questions on demographics. (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 analyse the qualitative data collected on incidents with the objective of establishing a classification of their characteristics. We employ qualitative coding techniques, inspired by Gioia and colleagues (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 and triangulated with existing research, until theoretical saturation is reached.

4 Preliminary Results of Qualitative Data Analysis

We conducted our data collection in September and October 2022 via Prolific Academic, collecting 35 valid cases of critical incidents reported by users of digital services from the United Kingdom. In the introduction to our questionnaire, we asked participants to only participate if they have experienced such an incident where they were aware or suspected that a digital service engages in information sharing with external parties in a way that they had not authorized. Our sample consisted of 24 female participants, 11 were male. The majority of participants (16) fell within the age group of 30- to 39-year-olds, followed by 20- to 29-year-olds (8). Most participants (18) held a university degree from an undergraduate programme.

Cognitive appraisal theory (Folkman et al., 1986; Smith and Lazarus, 1993) provides us with a general procedural framework which aids the identification of third-order codes from first- and second-order codes. Cognitive appraisal theory explains individuals' responses towards stressful encounters and proposes that the cognitive appraisal of such an encounter occurs in two steps of appraisal, primary appraisal (i.e., evaluating the potential threat posed from the encounter) and secondary appraisal (i.e., evaluating means to cope with that threat) (Folkman et al., 1986). Within these two steps of appraisal, primary appraisal refers to the assessment of the relevance of the threat for the individual, as well as the congruence of the consequences of the threat with the individuals' goals (Smith and Lazarus, 1993).

With regard to perceived privacy violations through EUSU, this refers to the assessment of consequences experienced through the perceived EUSU, as well as any attitudes towards EUSU and the digital service that the experience is evaluated against. Secondary appraisal refers to an assessment of who is accountable for the encounter, as well as an evaluation of different means of coping with its consequences (Smith and Lazarus, 1993). Applied to the phenomenon under study, we identify different attributions of causes that produce the user's perception of a privacy violation through EUSU. Lastly, cognitive appraisal leads to the outcome of either engaging in problem-focused or emotion-focused coping responses (Smith and Lazarus, 1993). For perceived privacy violations through EUSU, such responses include either emotional responses, problem-focused responses that are directed inwardly or towards the external, and emotion-focused responses that aim at handling the emotional responses one experiences without directly increasing privacy protection. Table 1 shows an overview of the results from our qualitative analysis of incidents of perceived privacy violations through EUSU.

Third-Order Codes	**Second-Order Codes**	**Illustrative Example of First-Order Code and Quotation**
Encounter: Observable consequence	• Phishing • 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)
Primary appraisal: General dispositions towards EUSU	• 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)
Primary appraisal: Attitudes towards the digital service	• Enjoying the digital service • Not trusting the digital service • Disconfirmed expectations • Confirmed expectations	Did not expect such behaviour from digital service: "Annoyed at such a reputable company for doing that. I didn't expect it from them. I was disappointed." (ID342, EE)
Primary appraisal: Appraisal of EUSU in this incident	• Contradicts with benefit of service • Feeling overserved • Perceives benefits from EUSU • (…)	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)
Primary appraisal: Appraisal of consequences due to incident	• Manipulation • Potentially dangerous • Time and effort • Inconvenience • (…)	Finds that Facebook altering their political views is very manipulative: "Facebook should not be able to share data that can influence my political views in the long run as this is very manipulative." (ID366, Facebook)
Secondary appraisal: Cause attribution	• Internal • External • Legitimate • Illegitimate	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” (ID347, Facebook)
Secondary appraisal: Cause attribution base	• Recognizing information • Hearsay • Timing • Instinct	Recognized digital service as the responsible as they use separate emails for different purposes: “this was a specific email that I only use for travel arrangements and affairs” (ID323, Flightright)
Appraisal outcome: Affect	• Incident triggered angry feelings • Incident triggered anxious feelings • Losing trust in the digital service	Feels worried: “it is worrying because I can't even feel safe having a conversation in my own home” (ID371, Facebook)
Appraisal outcome: 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)
Appraisal outcome: Internal rectification actions	• Eliminating underlying causes • Information restriction with the digital service • Information restriction outside of the digital service • Being more aware of privacy • (…)	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)
Appraisal outcome: Emotion-focused coping	• Inaction • Positive reinterpretation • Mental disengagement	Did not take any actions to preserve their privacy after the incident: “I haven't taken any actions” (ID343, Google)

Table 1. Overview of Coding.

5 Discussion

Responding to our first research question – when and why users perceive digital services sharing their information with external parties as a privacy violation – our preliminary findings, as presented in Table 1, show the variety of encounters that can provoke a user’s perception of a privacy violation through EUSU. The appraisal of these encounters consists of dispositional attitudes towards EUSU and towards the digital service, as well as towards the specific experience of EUSU, and of its consequences in the particular incident reported. The boundaries around the perceptual nature of these privacy violations are mainly captured by the way users attribute causes to their inference of EUSU from their encounter.

Our second research question – how do users respond to such perceived privacy violations – is answered by the appraisal outcomes identified in the coding scheme. These responses range from emotions (e.g., feeling angry or anxious), to emotion-focused coping (e.g., mental disengagement or inaction), to rectification actions that are either directed internally towards the user themselves or externally towards the digital service, external parties, or the public.

These results give a first indication that most users perceive EUSU quite negatively. Many users underline the negative consequences they experience from the incident (e.g., manipulation, potentially dangerous, inconvenience, …), their negative perceptions towards the digital service that their experience produces (most participants indicate a shift towards a more negative attitude and a loss of trust in the digital service after the incident), as well as generally negative dispositions towards the practice of digital services engaging in EUSU (most participants indicate not accepting or tolerating this practice).

At the same time, users' responses are mainly directed towards changing their own behaviour, not the behaviour of the digital service responsible. In our data, the majority of responses are classified as internal rectification actions or emotion-focused coping. Very few participants named an external rectification action as their reaction to their encounter of a privacy violation through EUSU.

5.1 Potential contributions

This study is expected to contribute to theorizing on privacy violations due to EUSU. More specifically, it shall (1) describe and delineate the boundaries of perceptions of EUSU as privacy violations, (2) identify perceptions and responses that follow such an attribution within the immediate privacy violation situation, (3) uncover the multiplicity of factors that lead to the unfolding and harnessing of perceptions of privacy violations through EUSU, and (4) provide evidence for how experiences with EUSU influence actual user behaviour.

Our findings may help digital services further understand the conditions under which users perceive their engagement in EUSU as a privacy violation. This understanding can aid them in strengthening communication with their users regarding how they use their information, and potentially in adapting information uses they engage in to avoid negative perceptions of their service by their users, or even losing them as customers.

5.2 Limitations

We do see limitations of our study in the application of CIT as a methodology. First, individuals reporting their own subjective experiences based on their memories of these experiences are susceptible to biases and incomplete information. A user's perception of a digital service is, however, largely based on how they remember and perceive experiences with that digital service, biased and incomplete or not.

Second, this methodology enables us to capture individuals' actual changes of usage of a digital service they experience a privacy violation through EUSU with – which even though self-reported is less prone to misrepresentation, as it refers to the current moment.

Third, due to the wide variety of contexts that EUSU is recognized in, perceptions and responses might be very different for these distinct contexts. Consequentially, an abstraction of factors throughout these contexts might be difficult to achieve.

Lastly, users may think that organizations are engaging in EUSU even when a digital service is not doing so, or not doing so in an unauthorized way. This makes studying perceived privacy violations due to EUSU difficult to conceptually differentiate from perceived privacy violations that do not result from EUSU. However, as perception leads to users' responses, we find our focus on perceived privacy violations through EUSU appropriate.

5.3 Next steps

As a next step, we want to further refine and extend our presented qualitative data collection and 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). It is increasingly employed in recent IS studies to understand phenomena from a configurational perspective, adding to qualitative and variance-based approaches (Mattke et al., 2021). We apply QCA to understand how different situational configurations where users perceive privacy violations through EUSU relate to users' privacy protective responses.

References

Angst, C. M., Agarwal, R. (2009). "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion." *MIS Quarterly,* 33 (2), 339–370.

Buckman, J. R., Bockstedt, J. C., Hashim, M. J. (2019). "Relative Privacy Valuations Under Varying Disclosure Characteristics." *Information Systems Research,* 30 (2), 375–388.

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

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

Cichy, P., Salge, T. O., Kohli, R. (2021). "Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars." *MIS Quarterly*, 45 (4), 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), 341–363.

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

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

Daviet, R., Nave, G., Wind, J. (2022). "Genetic Data: Potential Uses and Misuses in Marketing." *Journal of Marketing,* 86 (1), 7–26.

Drake, J. R., Furner, C. P., Mehta, N. (2021). "Privacy Policy Violations: A Corporate Nexus of Healthcare Providers and Social Media Platforms." *WISP 2021 Proceedings*, 1–17.

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

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., Gruen, R. J. (1986). "Dynamics of a Stressful Encounter: Cognitive Appraisal, Coping, and Encounter Outcomes." *Journal of Personality and Social Psychology,* 50 (5), 992–1003.

Gao, W., Wang, H., Jiang, N. (2022). "The Impact of Data Vulnerability in Online Health Communities: An Institutional Assurance Perspective." *Frontiers in Psychology*, 13, 1–12.

GDPR (2018). General Data Protection Regulation (GDPR). *2016/679*. URL: https://gdpr.eu/tag/gdpr/ (visited on 11/16/2022).

Gerlach, J., Eling, N., Wessels, N., 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), 548–575.

Gerlach, J., Widjaja, T., Buxmann, P. (2015). "Handle with Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior." *The Journal of Strategic Information Systems*, 24 (1), 33–43.

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

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

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., Png, I. P. L. (2007). "Overcoming Online Information Privacy

Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems*, 24 (2), 13–42.

Kari, T., Salo, M., Frank, L. (2020). "Role of Situational Context in Use Continuance after Critical Exergaming Incidents." *Information Systems Journal*, 30 (3), 596–633.

Karwatzki, S., Dytynko, O., Trenz, M., Veit, D. (2017). "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization." *Journal of Management Information Systems*, 34 (2), 369–400.

Karwatzki, S., Trenz, M., Veit, D. (2022). "The Multidimensional Nature of Privacy Risks: Conceptualisation, Measurement and Implications for Digital Services." *Information Systems Journal*, 1–32.

Keil, M., Park, E. H., 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), 818–848.

Kelly, L., Kerr, G., Drennan, J. (2017). "Privacy concerns on social networking sites: a longitudinal study." *Journal of Marketing Management*, 33 (17/18), 1465–1489.

Kurtz, C., Semmann, M., Schulz, W. (2018). "Towards a Framework for Information Privacy in Complex Service Ecosystems." *ICIS 2018 Proceedings*, 1–9.

Mattke, J., Maier, C., Weitzel, T., Thatcher, J. B. (2021). "Qualitative Comparative Analysis in the Information Systems Discipline: A Literature Review and Methodological Recommendations." *Internet Research*, 31 (5), 1493–1517.

Meuter, M. L., Ostrom, A. L., Roundtree, R. I., Bitner, M. J. (2000). "Self-Service Technologies: Understanding Customer Satisfaction with Technology-Based Service Encounters." *Journal of Marketing*, 64 (3), 50–64.

Ozdemir, Z. D., Smith, H. J., 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), 642–660.

Ragin, C. C. (1987). *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*. University of California Press, Berkeley, CA, USA. URL: (visited on 6/13/2022).

Salo, M., Frank, L. (2017). "User Behaviours After Critical Mobile Application Incidents: The Relationship with Situational Context." *Information Systems Journal*, 27 (1), 5–30.

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., Yu, Y. (2017). "Protecting Customer Privacy when Marketing with Second-Party Data." *International Journal of Research in Marketing*, 34 (3), 593–603.

Serenko, A., Turel, O. (2010). "Rigor and Relevance: The Application of The Critical Incident Technique to Investigate Email Usage." *Journal of Organizational Computing and Electronic Commerce*, 20 (2), 182–207.

Smith, C. A., Lazarus, R. S. (1993). "Appraisal Components, Core Relational Themes, and the Emotions." *Cognition & Emotion*, 7 (3–4), 233–269.

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

Son, J.-Y., Kim, S. S. (2008). "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model." *MIS Quarterly*, 32 (3), 503–529.

Statista (2021). Google: Advertising Revenue 2021. *Statista*. URL: https://www.statista.com/statistics/266249/advertising-revenue-of-google/ (visited on 9/29/2022).

Sutanto, J., Palme, E., Tan, C.-H., Phang, C. W. (2013). "Addressing the Personalization-Privacy

Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users." *MIS Quarterly*, 37 (4), 1141–1164.

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

Wall, J. D., Lowry, P. B., 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), 39–76.

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

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

Zhu, Y.-Q., Chang, J.-H. (2016). "The Key Role of Relevance in Personalized Advertisement: Examining its Impact on Perceptions of Privacy Invasion, Self-Awareness, and Continuous Use Intentions." *Computers in Human Behavior*, 65, 442–447.