# To Leave or Not to Leave: A Configurational Approach to Understanding Digital Service Users' Responses to Privacy Violations Through Secondary Use

**Research Paper**

Christina Wagner[1], Manuel Trenz[2], Chee-Wee Tan[3], and Daniel Veit[1]

[1] University of Augsburg, Chair of Information Systems and Management, Augsburg, Germany
christina.wagner@uni-a.de, daniel.veit@uni-a.de
[2] University of Goettingen, Chair of Interorganizational Information Systems, Goettingen, Germany
trenz@uni-goettingen.de
[3] The Hong Kong Polytechnic University, Management Information Systems, Hong Kong
chee-wee.tan@polyu.edu.hk

**Abstract.** Digital services increasingly collect and share user information. Accompanying this development, external secondary use of information (ESU), where an individual's information is collected for one purpose but used for a secondary purpose by an external party, is becoming a dominant privacy concern of users. This study offers valuable insights into users' perceptions of privacy violations through ESU and their resulting privacy-protective responses. Employing an abductive qualitative crisp-set approach to Qualitative Comparative Analysis (QCA) and attribution theory as a guiding meta-theory, we identify multiple configurations that lead to selected privacy-protective responses. These findings help practitioners gain clarity about how their privacy practices are perceived by their users. Theoretically, we extend attribution theory as well as prior research on privacy violations with a configurational view on ESU privacy violations.

**Keywords:** Privacy Violation; Secondary Use; Qualitative Comparative Analysis; QCA

## 1 Introduction

In digital markets, the collection and sharing of user information is becoming increasingly complex, especially with the rise of IoT, smart devices, and big data analytics. In this context, external secondary use of information (ESU), where an individual's information is collected for one purpose but used for a secondary purpose by an external party, has become a significant privacy concern for users. While in some cases, ESU might be perceived as a standard privacy practice, in others, users might perceive a privacy violation.

When users perceive a digital service's ESU practices as a privacy violation, their responses might have negative consequences for the latter–such as restricting information collection or discontinuing usage. Since digital services increasingly create value from the secondary use of information (Gerlach et al., 2015; Veit et al., 2014), retaining their customers as well as their data are necessary resources (Culnan, 2019; Grover et al., 2018). Therefore, we aim to understand two privacy-protective responses that are most relevant in this regard: Restricting information collection by the digital service while continuing usage and discontinuing usage of the digital service.

Prior research on privacy violations provides us with an understanding of the perceptions and emotional experiences related to a privacy violation (Bachura et al., 2022; Nikkhah and Grover, 2024; Zhu et al., 2023) and identifies privacy-protective responses that a user may engage in after experiencing a privacy violation (Son and Kim, 2008; Zhu and Chang, 2016).

We propose that connecting user's perceptions and emotional experiences of an ESU privacy violation with their privacy-protective responses necessitates considering the complexity inherent to this phenomenon. This complexity stems, firstly, from the involvement of various parties in ESU: an information owner (user of a digital service), an information co-owner (the digital service that is receiving the information owner's personal information), and an information consumer (an external organization that the information co-owner is sharing the information owner's personal information with). Secondly, this complexity might also be inherent to the characteristic of ESU privacy violations as being unexpected, emotion-laden experiences for information owners. Previous literature often employed a variance-based perspective on explaining individuals' perceptions of and reactions towards privacy violations (e.g., Choi et al., 2016; Keil et al., 2018; Son and Kim, 2008). Experiencing such an emotion-laden event as an ESU privacy violation might, however, not be fully explainable by linear causalities. A configurational perspective, considering interactions between different emotions and perceptions might provide insights to the phenomenon.

A theoretical framework that has been used to explain ambiguities in responsibility for privacy violations (Dunn et al., 2021; Keil et al., 2018; Syed, 2019) is attribution theory (Kelley and Michela, 1980; Weiner, 1985). We depart from classical attribution theory that focuses on explaining the process of individuals' motivations for actions on the basis of the causes that they attribute their experiences to (Weiner, 1985). Based on contempory findings on appraisal theory advocating for representing the complexity inherent to emotional events by considering dynamic and recursive interactions instead of a purely linear process (e.g., Moors et al., 2013; Yeo & Ong, 2024), we acknowledge the interdependent and equifinal nature of different elements of the attribution "process"—and interpret them as embedded in a complex, interactive cognitive interplay. Embracing a configurational view of the causes (receiving web advertisement or unsolicited contact), causal attributions (internal vs. external locus, stable vs. unstable event), emotions (anger, anxiety) and perceptions (self-efficacy, disconfirmed expectations) leading to privacy-protective responses, we emloy a set-theoretic approach of crisp-set Qualitative Comparative Analysis (csQCA) (Park et al., 2020). Thereby, we aim to gain an understanding of how different privacy-protective responses come into existence as a consequence of different combinations of characteristics of situations that are interpreted as ESU privacy violations from the perspective of an information owner, posing the research question: *What combinations of characteristics of ESU privacy violations lead to restricting information or discontinuing usage of a digital service?*

Our paper is structured as follows. First, we discuss related research on ESU privacy violations, privacy-protective responses, and provide background on attribution theory. We then present our methodological approach of csQCA. Subsequently, we present our configurational model and the results of our empirical analysis. Finally, we discuss implications for theory and practice.

## 2 Research Background and Theoretical Foundation

### 2.1 Privacy Violations Through External Secondary Use

External secondary use means that information is used for a different purpose than the one it was collected for involving access by an external party (Culnan, 1993). IS research generally found that information co-owners' practices of secondary use decrease information owners' willingness to use such services (Angst and Agarwal, 2009; Gerlach et al., 2015) and increase perceptions of privacy violations (Karwatzki et al., 2017; Sutanto et al., 2013; Zhu and Chang, 2016).

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). Prior studies can be classified in terms of the violator—be it a peer (e.g., Choi et al., 2015; Zhang et al., 2022), an outside attacker (e.g., hacking, virus attacks from outsiders) (e.g., Bachura et al., 2022; Hoehle et al., 2022; Nikkhah & Grover, 2024), or an organization that the information owner is in a relationship with (e.g., insider disclosure, sharing information with a third party) (e.g., Bansal & Zahedi, 2015; Zhu et al., 2023). ESU privacy violations fall into the latter category. Here they have been considered very broadly, as a type of privacy threats (Son and Kim, 2008), as well as with a focus on how organizations can repair trust after an ESU privacy violation (Bansal and Zahedi, 2015). Yet, none of these studies explicitly studied perceptions and responses of ESU privacy violations, considering its inherent complexity due to the involvement of multiple potential culprates.

### 2.2 Privacy-Protective Responses

Extant research considers various privacy-protective responses as an individual's reaction towards privacy violations. Son and Kim (2008) explore information owner'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 information co-owner), and complaining indirectly to third-party organizations (Son and Kim, 2008). Since then, studies explored subsets of these privacy-protective responses that information owners take towards privacy violations (Choi et al., 2016; Drake et al., 2021).

In addition to these more immediate privacy-protective responses after a privacy violation, studies explore the longer term impact on an information owner'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).

Building on the privacy-protective response of *removal* from the framework developed by Son and Kim (2008) and contextualizing it to privacy violations through ESU, we view this response more granularly by considering its longer term impact on an information owner's relationship with the violating organization: When *restricting information collection by the information co-owner while continuing usage* as a response to a perceived privacy violation through ESU, information owners restrict future information collection by the information co-owner through reducing their usage, adapting their disclosure behavior, or changing privacy settings. Further, information owners may directly delete certain information, turn off their device to avoid information tracking, or misrepresent information. When *discontinuing usage of the information co-owner*, information owners either close their account, simply stop their usage of a service, and / or switch to a different digital service.

## 2.3 Attribution Theory

Attribution theory provides a meta-theoretical framework to understand the reasons for how and why one experiences an ESU privacy violation in multidimensional and granular way. The common idea behind attribution theory is that when individuals face an experience, they strive to make sense of it by searching for causes to assign responsibility (Keil et al., 2018; Kelley and Michela, 1980; Weiner, 1985). Based on this overarching lens, we are able to delineate what characteristics of an experience lead to information owners' interpretation as an ESU privacy violation and why they subsequently react in certain ways.

The attribution process starts with an information owner's observation of an event that they associate with a potential privacy violation through ESU by an information co-owner. This experience provides the information owner with information and induces them to compare their experience with their *expectations*. On that basis, the information owner attributes causes to their experience. These causes may be viewed along three dimensions in ESU privacy violations: (1) *Locus*: Are the causes that led to the experience of the incident closer to something that the information owner did (internal) or something that the information co-owner did (external)? (2) *Controllability*: Would the information co-owner have been able to prevent the causes of the experience from the incident from happening (controllable) or were they something that happened to them without them having volitional control (uncontrollable)? And (3) s*tability*: Do the causes that led to the experience of the incident happen regularly (stable) or fluctuate over time (unstable) (Weiner, 1985)? In line with our definition of ESU privacy violations they are controllable by the information co-owner. Controllability is therefore constant, does not form part of our configurational model, and will subsequently not be discussed further. The information owner further experiences consequences at a cognitive and an affective level. At a *cognitive level,* they evaluate whether they have the ability to alter the situation through their response (Weiner 1985). *Self-*

*efficacy* refers to the extent to which information owners believe they are capable of engaging in in privacy-protective responses (Bandura, 1977; Weiner, 1985).

At the *affective level*, prior work on privacy violations found three major emotions experienced after experiencing a privacy violation: *anxiety*, *anger*, and *sadness* (Bachura et al., 2022). While anxiety and anger tend to occur more immediately, sadness occurs during retrospection at a later point in time. Since our study focuses on the more immediate experience surrounding the ESU privacy violation, we exempt sadness from our subsequent modeling. The final stage of the attribution process are the information owners' actions.

We consider *behavioral responses* in terms of the two privacy-protective responses outlined above. Generally, we expect that discontinuing usage involves external and unstable attributions, anger, high levels of self-efficacy, and a user's disconfirmed beliefs about the digital service. Regarding restricting information while continuing usage, we expect the presence of fear, stable and internal attributions, as well as the absence of self-efficacy. Despite these overall expectations, we are seek to explore how different configurations of conditions might interact with one another in unexpected ways.

## 3 Method

To gain configurational insights into how different elements of the attribution process interact with one another and produce privacy-protective responses, we rely on Qualitative Comparative Analysis (QCA). QCA is a methodology increasingly employed in IS, but only rarely in the area of individual information privacy (Mattke et al., 2021). QCA contributes by offering a configurational perspective of understanding potentially complex interdependencies between causal conditions (Mattke et al., 2021).

An abductive, qualitative, crisp-set approach (Park et al., 2020) is deemed appropriate for studying the phenomenon of perceived privacy violations through ESU. In this approach, we identify characteristics inherent to our phenomenon from qualitative data, and uncover their combined effects by means of csQCA. Hereby, observations of the phenomenon guide the identification of conditions, and attribution theory as a metatheory helps establishing an understanding of how these conditions may bring about meaningful causal recipes (Park et al., 2020). Crisp sets are deemed appropriate with qualitative data where it is difficult to determine fine-grained breakpoints (Iannacci et al., 2022).

We collected qualitative data on 57 cases by means of an online survey questionnaire containing open-ended and closed-ended questions, employing the critical incident technique (CIT) (Flanagan, 1954). Our goal was to identify incidents where information owners become aware or suspect that an information co-owner they are a customer of shared their information with an information consumer. We sent out the online survey questionnaire via a commercialized survey respondent provider to users of digital services that had experienced an ESU privacy violation. After asking paricipants to specify details of the incident, we requested them to reflect on consequences they experienced due to the incident, actions they engaged in as a response, as well as their attitudes and expectations towards the digital service and ESU in general.

Participants generally reported two types of experiences of ESU privacy violatons: (1) Receiving web advertisement, reporting for example Instagram or Google as the information co-owner; and (2) receiving unsolicited contact, receiving, for example, phone calls from a third party that one's phone provider is accused of sharing.

Engaging in first-order and second-order coding of our the qualitative data, we obtained third-order codes with attribution theory as a meta-theory (Kelley and Michela, 1980; Weiner, 1985). A detailed display of results of a preliminary qualitative analysis is part of Wagner et al. ( 2023).

Building on the guidelines for applying csQCA in the domain of IS when using quantitative (Mattke et al., 2022; Park et al., 2017) or qualitative data (Nishant and Ravishankar, 2020; Park et al., 2020), we delineate our methodological approach: First, we select conditions for our configurational model on the basis of our analysis of qualitative data. Second, we calibrate our data along these conditions. Third, we analyze truth tables for each outcome and interpret the necessary and sufficient conditions, utilizing the R "QCA" package (Duşa, 2018). Finally, we discuss these results.

## 4 Analysis

### 4.1 A Configurational View on Perceiving ESU Privacy Violations

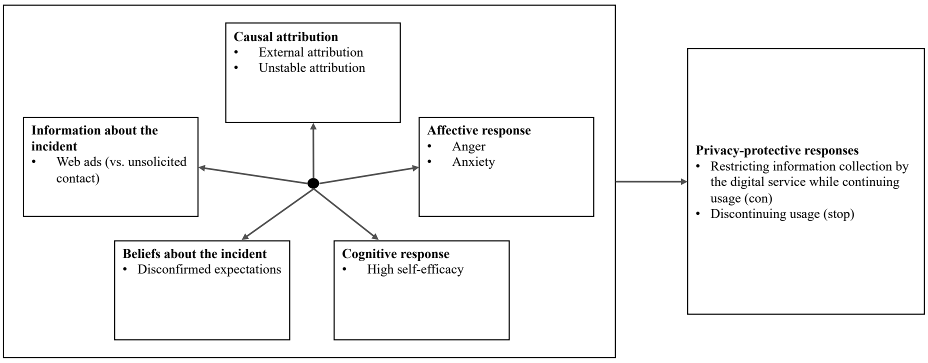
Causal attribution
• External attribution
• Unstable attribution
Information about the incident
• Web ads (vs. unsolicited contact)
Affective response
• Anger
• Anxiety
Beliefs about the incident
• Disconfirmed expectations
Cognitive response
• High self-efficacy
Privacy-protective responses
• Restricting information collection by the digital service while continuing usage (con)
• Discontinuing usage (stop)

**Figure 1.** Configurational model

Our configurational model integrates categories derived from the coding of qualitative data with respect to our configurational interpretation of attribution theory to gain a more in-depth understanding of privacy violations through ESU. Figure 1 presents our configurational model. With this configurational view, we attempt to explain how different combinations of conditional expressions produce different privacy-protective responses. Of our 57 cases, in 25 participants restrict information collection by the digital service while continuing usage and in 32 participants stop usage of the digital service.

## 4.2 Data Calibration

Calibration is a process within QCA that transforms data into sets. It is necessary to prepare these sets as input for the creation of the truth table. As discussed above, we choose to code our data into crisp sets to avoid arbitrary fine-grained breaking points (Iannacci et al., 2022). In csQCA, calibration involves determining whether a case is in the set (1) or out of the set (0) by defining an ideal case, that would signify the case as part of the set, and a nonmembership case (Basurto and Speer, 2012; Brosig et al., 2022; de Block and Vis, 2019). Table 1 provides an overview of the respective conditions, their definitions of membership, as well as illustrative examples from our qualitative data.

**Table 1.** Calibration into crisp sets

| **Condition** | **Definition of membership (1)** | **Illustrative example for membership** |
|---|---|---|
| Web ads | The participant observes targeted web advertisement. Nonmembership implies that the participant received unsolicited contact. | *"an advert appeared on my page"* (ID338, Instagram) |
| Anger | The participant feels angry, annoyed, frustrated, betrayed, or another anger-related emotion as a response to their experience. | *“I was really annoyed that someone had shared my private phone number.”* (ID 409, Amazon) |
| Anxiety | The participant feels anxious, worried, concerned, invaded, or another anxiety-related emotion as a response to their experience. | *“I started getting really worried”* (ID 333, CW Spotlight) |
| High self-efficacy | The participant displays confidence in their capability to engage in privacy-protective responses. | *“under GDPR I requested they delete all my information”* (ID 491, Paypal) |
| External attribution | The locus of causality of why the incident happened is external, i.e., someone outside is at fault. | *“thought the Facebook had scanned my search”* (ID 386, Facebook) |
| Unstable attribution | The cause of the incident fluctuates over time or is one-time. | *“Once I had provided my number I started to receive unsolicited notifications”* (ID 388, O2) |
| Disconfirmed expectations | Expectations of whether the information co-owner would engage in ESU were disconfirmed. | *“the games industry in general are usually against that kind of data misuse.”* (ID 400, Epic Games Story) |

## 4.3 Analyzing Necessary Conditions

csQCA analysis commonly begins with the analysis of necessary conditions (Mattke et al., 2022; Ortiz de Guinea and Raymond, 2020). Generally, X is a necessary condition if it is present whenever the outcome Y is present (Schneider and Wagemann, 2012). Two measures assess the degree to which a condition forms a necessary condition for an outcome in question: consistency and coverage (Schneider and Wagemann, 2012). *Consistency* is the ratio of the number of cases where X = 1 and Y = 1, and the number of cases where Y = 1. It thereby refers to the inclusion of the condition under question in the outcome under question. *Coverage* means the ratio of the number of cases where X = 1 and Y = 1, and the number of cases where X = 1. It is a measure of how relevant the necessary condition under question is for obtaining outcome Y (Duşa, 2018; Schneider and Wagemann, 2012). Thresholds for consistency and coverage established in methodological guidelines in IS literature are .9 and .6 respectively. Our results (see Table 2) show only disconfirmed expectations for discontinuing usage above the consistency threshold of .9.

**Table 2.** Necessary conditions
Consistency (coverage); Values above .9 in bold; Abbreviations explained in Figure 1

| **Outcome /Condition** | **Web ads** | **Anger** | **Anxiety** | **High self-efficacy** | **External attribution** | **Unstable attribution** | **Disconfirmed expectations** |
|---|---|---|---|---|---|---|---|
| con | .538<br>(.758) | .769<br>(.300) | .500<br>(.731) | .731<br>(.426) | .577<br>(.585) | .385<br>(.457) | .654<br>(.302) |
| stop | .176<br>(.676) | .882<br>(.360) | .265<br>(.690) | .794<br>(.491) | .412<br>(.576) | .765<br>(.593) | **.941**<br>(.396) |

## 4.4 Analyzing Sufficient Conditions

Next, we focused on identifying causal recipes that are sufficient for explaining different privacy-protective responses. We calculated truth tables for each outcome. Truth tables present in each row logically possible combinations of conditions, each listing the value of the respective outcome under analysis (Schneider and Wagemann, 2012). Next, we applied Boolean minimization to produce the conservative, parsimonious and intermediate solutions to explain each outcome. We decided to focus our analysis to the explanation of the presence of the outcome–since the absence of the outcome would signify a combination of other privacy-protective responses in effect.

Table 3 presents these results graphically, relying on the notation introduced by Ragin (2008). Black circles represent the presence, crossed-out circles the absence of a condition within the respective solution. Empty spaces present "don't care" conditions, where the condition can either be present or absent without altering the outcome. The core elements of the parsimonious solution, which are a subset of the intermediate solutions, are represented by bigger circles. Peripheral elements specific to the intermediate solution are presented by smaller circles (Ortiz de Guinea and Raymond, 2020;

Park et al., 2017). Our selection of solutions is guided by a consistency threshold of .8 (Schneider and Wagemann, 2010) and a frequency threshold of 2 (Mattke et al., 2022).

**Table 3.** Configurational results

| **Configurational element** | **Restricting information collection while continuing usage** | | | **Discontinuing usage** | | |
|---|---|---|---|---|---|---|
| | con1 | con2 | con3 | stop1 | stop2 | stop3 |
| Web ads | • | • | | ⨂ | ⨂ | • |
| Anger | | | ⊗ | • | • | • |
| Anxiety | ● | ● | ● | ⨂ | ⨂ | |
| High self-efficacy | • | | | ● | | ● |
| External attribution | ● | ● | ● | ● | ⊗ | ⊗ |
| Unstable attribution | ⨂ | ⨂ | ⨂ | ● | ● | ⊗ |
| Disconfirmed expectations | | ⨂ | ⨂ | | • | • |
| Consistency | .800 | 1.000 | 1.000 | 1.000 | .800 | 1.000 |
| Raw coverage | .160 | .120 | .120 | .156 | .125 | .062 |
| Unique coverage | .040 | .040 | .040 | .031 | .125 | .031 |
| Overall consistency | | .889 | | | .763 | |
| Overall coverage | | .400 | | | .343 | |

Our results for sufficient configurations exhibit high consistency and rather low coverage values. Overall coverage of .400 and .343 mean that the proposed paths explain 40% of the outcome restricting information collection, and 34.3% of the outcome discontinuing usage. High consistency values indicate that, among the cases exhibiting the respective combination of conditions, the vast majority also exhibit the respective outcome. Low unique coverage values for the outcome restricting information collection mean a potential overlap with causal recipes explaining other outcomes (Ragin, 2006).

## 4.5 Validating Findings

To validate our findings, we performed a variety of robustness tests as suggested by prior research. We repeated the analysis dropping and adding cases and conditions. The patterns we observe from our configurational results remain quite similar (de Block and Vis, 2019). We repeated our analysis with a consistency threshold of 1.000. The identified solutions are rather similar, however we did observe a high number of conditions as remainders, further supporting our choice of a consistency threshold at .8 (Schneider and Wagemann, 2012).

## 5 Results

For restricting information collection by the information co-owner while continuing usage, our analysis leads to three solutions explaining this privacy-protective response. Across these three solutions, we see commonalities in the presence of external attribution, the absence of unstable attribution, and the presence of anxiety. What is consistent with our expectations is the absence of unstable attribution and the presence of anxiety.

In solutions con1 and con2, stable external attributions are observed in incidents of web advertisement. con3 is valid for both incidents of receiving web advertisement and incidents of receiving unsolicited contact. con1 additionally requires the presence of high self-efficacy, con2 and con3 the absence of disconfirmed expectations. The absence of disconfirmed expectations explains the information owners' willingness for continuing usage–they expected ESU from the information co-owner, therefore they already decided in the past that they will endure this practice. Despite that, their feelings of anxiety motivate them to restrict their information sharing. A case exemplifying this configuration is ID 372 (Facebook), where the participant suspects that their "searches and verbal conversations were being recorded and the data passed to a third party advertiser", motivating them to restrict Facebook's privacy settings, while still using the service. Based on these patterns, we propose

*P1: When perceiving privacy violations through ESU, information owners engage in the privacy-protective response of restricting information collection while continuing usage, when:*

- *Attributions are stable and external, and*
- *The information owner feels anxiety, and*
- *The incident involves web advertisement, and*
- *The information owner either feels high self-efficacy or confirmed in their expectations.*

We identify three configurations that lead to the outcome discontinuing usage. stop1 and stop2 include the element of receiving unsolicited contact, whereas stop3 is valid for cases receiving web advertisement. In all three configurations, anger is present–in line with our preliminary theorizing on the single effect of anger leading to stronger privacy-protective responses.

Configurations with receiving unsolicited contact further include the absence of anxiety and the presence of unstable attribution. Attributing the incident to a one-time cause may indicate the information owner's hopes that their actions may be effective in the future–motivating the restriction of information. The rather severe nature of receiving unsolicited contact, however, combined with either high levels of self-efficacy or disconfirmed expectations, as well as the above mentioned anger, leads to the information owner's decision to stop using an information co-owner. An exemplary incident here is ID 323 (Flightright), where the participant was "inundated with overseas phone calls and unsolicited mails" after completing an application for a flight delay compensation.

This experience made them feel angry at Flightright's privacy practices so they promised to not use the service in the future to avoid any repetition of what had happened.

Discontinuing usage is also a response towards incidents of web advertisement, here combined with high self-efficacy and disconfirmed expectations and attributed to an internal stable cause. This configuration is rather surprising, as we would have associated an internal stable attribution with less of a strong response. It must be the combination of anger, high self-efficacy and disconfirmed expectations, together with a stable attribution, that enrages the information owner to such a degree that the incident, even though attributed to their own actions, leads to discontinuing the information co-owner. Similar to the above example, it might be an act of self-protection, removing themselves from the possibility of further producing incidents of privacy violations through their use of the information co-owner. Based on these patterns, we propose

*P2: When perceiving privacy violations through ESU, information owners engage in the privacy-protective response of discontinuing usage of the information co-owner, when:*

- *The information owner feels angry, and*
- *The incident involves unsolicited contact or web advertisement, and*
- *The information owner feels high levels of self-efficacy or the absence of anxiety, and*
- *The attribution is external or expectations are disconfirmed.*

## 6 Discussion

The purpose of this study is to identify, which combinations of characteristics of ESU privacy violations lead to restricting information or discontinuing usage of an information co-owner. Through csQCA analysis, we identify multiple pathways that lead to these privacy-protective responses. From these configurational outcomes, we observe some overarching trends among configurations that explain each privacy-protective response. Based on these observations, we derive propositions for attribution-theory based causal recipes that lead to different privacy-protective responses.

With this study, we contribute to prior research and theory in several ways. First, we acknowledge the inherent multiplicity of parties and we add towards understanding the characteristics of situations that information owners interpret as ESU privacy violations. We shine light on information owner perceptions of ESU privacy violations, thereby aiding a more granular understanding of this specific dimension of information owners' privacy concerns. Second, we extend applications of attribution theory in the field of IS by a configurational interpretation. Recently, it has become increasingly popular in IS research to revisit phenomena and theories through a set-theoretic angle (e.g., Böttcher et al., 2022; Maier et al., 2021; Mattke et al., 2021). We are thereby able to represent the interdependent and equifinal nature of different elements of the attribution "process"—and interpret them as embedded in a complex, interactive cognitive interplay. Third, through our set-theoretic approach, we connect an in-depth understanding of information owners' interpretations of ESU privacy violations with their subsequent privacy-protective responses. Employing CIT, we are able to collect data on actual behaviors that information owners engaged in and are able to relate those to their reported perceptions and situational characteristics–adding to prior research often focusing on vignettes or intentions to approximate actual behaviors.

Our findings on configurations of perceptions of privacy violations through ESU and resulting privacy-protective responses by information owners shine light on the causes that lead to information owners' attributions of ESU privacy violations. Organizations can thereby gain more clarity about which of their practices and activities might be perceived as such causes by their information owners. On that basis, organizations obtain a lever to prevent information owners' (mis-)attributions of their practices as ESU. In the case of correct attribution, this may include communicating any failures and altering the ways in which the organization uses and shares their customers' data and respects their customers' privacy. In the case of misattribution, this may involve strategies to more transparently display how they use their information owners' data and to communicate these practices honestly. Employing these levers may have positive consequences for organizations in their efforts for information owner retainment and loyalty, as well as for information owners, having more certainty about what is happening to their data, and based on this information being able to decide in a self-determined way how they want it to be used.

This study is not exempt from limitations. First, we engage in purposive sampling, in coherence with what is recommended for csQCA analysis, and only sample respondents that have had an experience that they interpret as an ESU privacy violation. This sampling enables us to specifically focus on privacy-protective responses of information owners who have actually experienced such a privacy violation. It might, however, overrepresent information owners dispositioned to be more privacy skeptical, and underrepresent information owners that are very unconcerned about their privacy. That said, when aiming to understand perceptions and behaviors of information owners who do perceive privacy violations through ESU, information owners that do not perceive such violations would not aid in further understanding this phenomenon. A larger-scale quantitative study could, however, provide more insights into the prevalence of information owners in the overall population who perceive experiences of ESU privacy violations. Second, individuals reporting their own subjective experiences based on their memories of these experiences are susceptible to biases and incomplete information. Information owners may therefore think that an information co-owner is engaging in ESU even when that is not true. This conceptualization is consciously chosen as perception leads to response. However, it might be interesting to consider in future research whether the information co-owner actually engages in ESU. This might also open opportunities for a multi-level study considering both information owner perceptions and responses as well as organization-level privacy behavior. Third, we consciously opted for calibration to crisp sets to avoid setting arbitrary thresholds too granular for the nature of our data. Future studies may, however, choose a fuzzy set approach, possibly enriching our approach by quantitatively measured conditions.

# 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, 339–370. https://doi.org/10.2307/20650295

Bachura, E., Valecha, R., Rui Chen, Rao, H.R., 2022. The OPM data breach: An investigation of shared emotional reactions on Twitter. MIS Quarterly 46, 881–910. https://doi.org/10.25300/MISQ/2022/15596

Bandura, A., 1977. Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review 84, 191. https://doi.org/10.1037/0033-295X.84.2.191

Bansal, G., Zahedi, F.M., 2015. Trust violation and repair: The information privacy perspective. Decision Support Systems 71, 62–77. https://doi.org/10.1016/j.dss.2015.01.009

Basurto, X., Speer, J., 2012. Structuring the calibration of qualitative data as sets for qualitative comparative analysis (QCA). Field Methods 24, 155–174. https://doi.org/10.1177/1525822X11433998

Böttcher, T.P., Weking, J., Hein, A., Böhm, M., Krcmar, H., 2022. Pathways to digital business models: The connection of sensing and seizing in business model innovation. The Journal of Strategic Information Systems 31, 101742. https://doi.org/10.1016/j.jsis.2022.101742

Brosig, C., Bley, K., Strahringer, S., Westner, M., 2022. The missing piece – Calibration of qualitative data for qualitative comparative analyses in IS research, in: Proceedings of the European Conference on Information Systems. Romania, pp. 1–16. https://aisel.aisnet.org/ecis2022_rp/37/

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, 675–694. https://doi.org/10.1287/isre.2015.0602

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, 904–933. https://doi.org/10.1080/07421222.2015.1138375

Culnan, M.J., 2019. Policy to avoid a privacy disaster. Journal of the Association for Information Systems 20, 848–856.

Culnan, M.J., 1993. "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly 17, 341–363. https://doi.org/10.2307/249775

de Block, D., Vis, B., 2019. Addressing the challenges related to transforming qualitative into quantitative data in qualitative comparative analysis. Journal of Mixed Methods Research 13, 503–535. https://doi.org/10.1177/1558689818770061

Drake, J.R., Furner, C.P., Mehta, N., 2021. Privacy policy violations: A corporate nexus of healthcare providers and social media platforms. Proceedings of the Workshop on Information Security and Privacy at the International Conference on Information Systems 1–17.

Dunn, B., Jensen, M.L., Ralston, R., 2021. Attribution of responsibility after failures within platform ecosystems. Journal of Management Information Systems 38, 546–570. https://doi.org/10.1080/07421222.2021.1912937

Dușa, A., 2018. QCA with R: A comprehensive resource. Springer, Cham.

Flanagan, J.C., 1954. The critical incident technique. Psychological Bulletin 51, 327–358. https://doi.org/10.1037/h0061470

Gao, W., Wang, H., Jiang, N., 2022. The impact of data vulnerability in online health communities: An institutional assurance perspective. Front. Psychol. 13, 1–12. https://doi.org/10.3389/fpsyg.2022.908309

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, 33–43. https://doi.org/10.1016/j.jsis.2014.09.001

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, 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, 13–42.

Hoehle, H., Venkatesh, V., Brown, S.A., Tepper, B.J., Kude, T., 2022. Impact of customer compensation strategies on outcomes and the mediating role of justice perceptions: A longitudinal study of Target's data breach. MIS Quarterly 46, 299–340. https://doi.org/10.25300/MISQ/2022/14740

Iannacci, F., Simeonova, B., Kawalek, P., 2022. Investigating the determinants of inter-organizational information sharing within criminal justice: A context-mechanism-outcome approach. Journal of Information Technology 37, 188–208. https://doi.org/10.1177/02683962211013826

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, 369–400. https://doi.org/10.1080/07421222.2017.1334467

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, 818–848. https://doi.org/10.1111/isj.12168

Kelley, H.H., Michela, J.L., 1980. Attribution theory and research. Annual Review of Psychology 31, 457–501. https://doi.org/10.1146/annurev.ps.31.020180.002325

Maier, C., Laumer, S., Joseph, D., Mattke, J., Weitzel, T., 2021. Turnback intention: An analysis of the drivers of IT professionals' intentions to return to a former employer. MIS Quarterly 45, 1777–1806. https://doi.org/10.25300/MISQ/2021/16033

Mattke, J., Maier, C., Weitzel, T., Gerow, J., Thatcher, J., 2022. Qualitative comparative analysis (QCA) in information systems research: Status quo, guidelines, and future directions. Communications of the Association for Information Systems 50. https://doi.org/10.17705/1CAIS.05008

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, 1493–1517. https://doi.org/10.1108/INTR-09-2020-0529

Moors, A., Ellsworth, P.C., Scherer, K.R., Frijda, N.H., 2013. Appraisal theories of emotion: State of the art and future development. Emotion Review 5, 119–124. https://doi.org/10.1177/1754073912468165

Nikkhah, H.R., Grover, V., 2024. Strategizing responses to data breaches: A multi-method study of organizational responsibility and effective communication with stakeholders. Journal of Management Information Systems 41, 1042–1077. https://doi.org/10.1080/07421222.2024.2415774

Nishant, R., Ravishankar, M.N., 2020. QCA and the harnessing of unstructured qualitative data. Information Systems Journal 30, 845–865. https://doi.org/10.1111/isj.12281

Ortiz de Guinea, A., Raymond, L., 2020. Enabling innovation in the face of uncertainty through IT ambidexterity: A fuzzy set qualitative comparative analysis of industrial service SMEs. International Journal of Information Management 50, 244–260. https://doi.org/10.1016/j.ijinfomgt.2019.05.007

Park, Y., Fiss, P.C., El Sawy, O.A., 2020. Theorizing the multiplicity of digital phenomena: The ecology of configurations, causal recipes, and guidelines for applying QCA. MIS Quarterly 44, 1493–1520. https://doi.org/10.25300/MISQ/2020/13879

Park, Y., Sawy, O.E., Fiss, P., 2017. The role of business intelligence and communication technologies in organizational agility: A configurational approach. Journal of the Association for Information Systems 18. https://doi.org/10.17705/1jais.00467

Ragin, C.C., 2008. Redesigning social inquiry: Fuzzy sets and beyond. University of Chicago Press, USA.

Ragin, C.C., 2006. Set Relations in Social Research: Evaluating Their Consistency and Coverage. Political Analysis 14, 291–310. https://doi.org/10.1093/pan/mpj019

Schneider, C.Q., Wagemann, C., 2012. Set-theoretic methods for the social sciences: A guide to qualitative comparative analysis. Cambridge University Press, Cambridge, UK.

Schneider, C.Q., Wagemann, C., 2010. Standards of good practice in qualitative comparative analysis (QCA) and fuzzy-sets. Comp Sociol 9, 397–418. https://doi.org/10.1163/156913210X12493538729793

Son, J.-Y., Kim, S.S., 2008. Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly 32, 503–529. https://doi.org/10.2307/25148854

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. MISQ 37, 1141–1164. https://doi.org/10.25300/MISQ/2013/37.4.07

Syed, R., 2019. Enterprise reputation threats on social media: A case of data breach framing. The Journal of Strategic Information Systems 28, 257–274. https://doi.org/10.1016/j.jsis.2018.12.001

Veit, D., Clemons, E., Benlian, A., Buxmann, P., Hess, T., Kundisch, D., Leimeister, J.M., Loos, P., Spann, M., 2014. Business Models – An Information Systems Research Agenda. Business & Information Systems Engineering 6, 45–53. https://doi.org/10.1007/s11576-013-0400-4

Wagner, C., Trenz, M., Tan, C.-W., Veit, D., 2023. Perceived Privacy Violations through Unauthorized Secondary Use – Diving into User' Perceptions and Responses. ECIS 2023 Research-in-Progress Papers.

Weiner, B., 1985. An attributional theory of achievement motivation and emotion. Psychological Review 92, 548–573. https://doi.org/10.1037/0033-295X.92.4.548

Yeo, G.C., Ong, D.C., 2024. Associations between cognitive appraisals and emotions: A meta-analytic review. Psychological Bulletin 150, 1440–1471. https://doi.org/10.1037/bul0000452

Zhang, N.A., Wang, C.A., Karahanna, E., Xu, Y., 2022. Peer privacy concern: conceptualization and measurement. MIS Quarterly 46, 491–529. https://doi.org/10.25300/MISQ/2022/14861

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. https://doi.org/10.1016/j.chb.2016.08.048

Zhu, Y.-Q., Kanjanamekanant, K., Chiu, Y.-T., 2023. Reconciling the personalization-privacy paradox: Exploring privacy boundaries in online personalized advertising. JAIS 24, 294–316. https://doi.org/10.17705/1jais.00775