Who is responsible for customers' privacy? Effects of first versus third party handling of privacy contracts on continuance intentions

BAYERL, Petra Saskia <http://orcid.org/0000-0001-6113-9688> and JACOBS, Gabriele

Technological Forecasting & Social Change 185 (2022) 122039

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

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

Who is responsible for customers' privacy? Effects of first versus third party handling of privacy contracts on continuance intentions

Petra Saskia Bayerl [a,*], Gabriele Jacobs [b]

[a] CENTRIC, Sheffield Hallam University, 20 Furnival Street, Sheffield S1 2NU, UK
[b] Erasmus University College, Erasmus University Rotterdam, Nieuwemarkt 1A, 3011HP Rotterdam, The Netherlands

ARTICLE INFO

Keywords:
Information privacy
Continuance intentions
Psychological contract
Privacy contract
e-commerce
Third party

ABSTRACT

E-commerce data management has become an extensive network of interrelated players that links companies providing goods or services (first parties) with companies that analyse, manage or otherwise use customers' data (third parties). In consequence, privacy is now the combined responsibility of first and third parties. We introduce the concept of *privacy contract* to investigate the effect of first versus third party privacy handling on customer reactions, including privacy contract fulfilment versus privacy contract breach. An online experiment with 296 participants confirmed that differences in privacy contract handling affects continuance intentions. This link is mediated through perceived contract fulfilment and feelings of violation. Although first party actions led to somewhat stronger reactions, both first and third party privacy contract (mis)handling affected continuance intentions and cognitive and affective reactions. Our findings demonstrate that individuals make little distinction between first and third party responsibilities, indicating that privacy contracts extend beyond the original relationship between customer and online retailer. It further demonstrates that privacy contracts offer a strong theoretical framework to understand customer reactions across different privacy situations. Conceptually, our study shifts privacy from a dualistic towards a network perspective of subjectively held privacy obligations, offering important pointers to guide organizations' privacy management.

1. Introduction

Privacy concerns are an important reason for customers to refrain from using online services or from purchasing goods online (Cho et al., 2006; Hsu and Lin, 2016; Yin et al., 2015). Actual privacy infringements can have even more severe consequences, ranging from a company's loss of reputation and loss of customers to its eventual demise. This fact is illustrated by well-publicized privacy violations such as Cambridge Analytica which used Facebook data for the manipulation of the 2016 US elections. The revelations led to a global call to delete Facebook accounts, whereas Cambridge Analytica itself announced its closure barely two months later (BBC, 2018; Hsu, 2018). Such scandals demonstrate that the adequate handling of customer data is of vital importance for the long-term viability of online businesses — and they further show that problematic privacy behaviours of one company can negatively affect the reputation and fate of others (Martin et al., 2017).

This effect is important to understand, as nowadays data and information management has become an extensive network of interrelated players that link companies from which customers receive goods or services (i.e., first parties) with other companies that analyse, manage, sell on or otherwise use customers' data (i.e., third parties) (Akter and Wamba, 2016). In the context of e-commerce, for instance, a customer who buys a product online engages in a network of interrelated business services, where the purchase of a pair of trousers, books or toys via a business-to-consumer online platform generally involves also the product provider, the delivery service and the financial transaction service provider. Such transactions are often further surrounded by companies that provide data analytics to optimize logistics, supply chains, prizing or marketing (Akter and Wamba, 2016). As another example, location-based mobile advertisement relies on a complex network of advertising agencies, mobile providers and brands as well as the platforms that deliver such ads to individuals while they browse other content online (e.g., Lin et al., 2016). Privacy is therefore seldom the task of only one company. Rather this *networked nature of privacy management* results in multiple and often complex relationships that connect individuals, first and third parties in the collection and (re)use

* Corresponding author.
E-mail addresses: p.s.bayerl@shu.ac.uk (P.S. Bayerl), jacobs@euc.eur.nl (G. Jacobs).

https://doi.org/10.1016/j.techfore.2022.122039
Received 29 September 2020; Received in revised form 28 February 2022; Accepted 10 September 2022
Available online 10 October 2022

of personal data and that create a network of privacy obligations as well as interlinked privacy expectations.

However, so far past research has focused primarily on privacy handling by first parties with little reference to the role of other linked parties involved. It further focused largely on the consequences when first parties mishandle customers' privacy, that is on the negative side of privacy handling (e.g., Chih et al., 2017; Fang and Chiu, 2014; Hsieh, 2012; Malhotra et al., 2017). This ignores two core features of the complex landscape of data management, namely the important role that third parties play in the management and control of personal data as well as the effect when companies *fulfil* their privacy obligations (i.e., the positive side of handling privacy). We argue that to fully understand the complex nature of privacy in todays' data management landscape and its impact on individuals' reactions, a broader view on privacy handling situations is needed that takes into account its networked nature across multiple companies.

Privacy laws around the world, like the European Union's General Data Protection Regulation (GDPR) introduced in 2018, acknowledge the increased connectivity and third party collection of data by stressing that companies need to take care of the associated risks and compliance obligations related to privacy and data security (Hintze, 2018). A common distinction made is between the *data controller* (typically the first party) who "determines the purposes and means of the processing of personal data" (GDPR Article 4(7)) and the *data processor* (typically the third party) "who processes personal data on behalf of the controller" (GDPR Article 4(8)). Given the high impact that violations of privacy can have on citizens, privacy laws have specified the obligations of controllers and processors and have also enhanced the sanctions that can come with violations. These changes in the playing field require companies to engage in serious risk assessments for both – the data controllers and data processors – in the understanding that "you are only as strong as your weakest link" (Pantlin et al., 2018). It is therefore important for companies to understand the dynamics between customer reactions to privacy handling across the supply chain. In fact, understanding customer reactions can be considered an important part of today's risk management for companies active in online sales or services.

Our study addresses this topic by investigating how various forms of privacy handling by first and third parties shape individuals' willingness to remain customers of an online retailer. We chose an online retail context, as this is a situation with often complex first and third party relations (Akter and Wamba, 2016) and high levels of personal (including sensitive) data being collected (e.g., bank details and home address, but also potentially intimate data such as political or sexual orientation through type of purchases or online services). It is further a context most Internet users will be highly familiar with (e.g., in 2021, 89% of individuals in the Netherlands and 91% in Denmark bought goods or services online) (Eurostat, 2021). We position our investigation within the framework of psychological contract theory (Rousseau, 1989, 1995), as psychological contracts allow to study privacy expectations explicitly as a relational construct. Within this framework we investigate the impact of a company' status as direct provider of products or services (i.e., first party) versus as third party without direct links to the customer. We moreover compare successful versus failed privacy handling to create insights into reactions across the full spectrum of privacy handling situations.

In the following sections we outline the theoretical background of our study followed by a description of the methodology and results. Our findings carry important implications for a more nuanced understanding of privacy as a network of (subjective) privacy obligations, which will be discussed in theoretical and practical terms at the end of the paper.

1.1. Customer privacy as psychological contract

Privacy in an e-commerce context refers to the assurance that personal information provided as part of commercial transactions remains secure and that access to this information is only possible by the people or organizations to which the customer grants this right. This view of online privacy is based on the concept of *information privacy* (Dinev et al., 2013; Smith et al., 2011), which denotes the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7).

This definition already highlights the fact that information privacy is a relational construct (Guo et al., 2017) in that it assumes a link between the person the data belongs to and a person or entity for which a right to this data has been granted by the data owner. Privacy in this view involves two parties that are linked by an exchange of information, together with the right of the data owner to determine who, how and why another party may have access to it. In an e-commerce context, this exchange forms the foundation for any transaction between customers and online retailers.

There are two perspectives on what forms the basis of privacy agreements. The first perspective focuses on legal obligations. These are governed by laws such as consumer rights and privacy regulations and provide the formal, enforceable basis of customer–company relations. Legal obligations tend to be explicitly codified in privacy statements and may also be signalled through privacy seals placed on retailers' websites (Bansal et al., 2015). However, privacy regulations can cover the quickly changing technological reality only to a certain extent and often stay ambiguous (e.g., can innovations in hacking attacks compel third parties to analyse customer data provided by first parties in order to identify and tackle emerging threats?). Also, as the context of e-commerce shows, the notion of *data owner* and *data controller* is frequently complex. For instance, when an attorney (i.e., third party) hired by a company (first party) examines personal data, this attorney controls the data, but does not own them (Hintze, 2018). The concepts of *data control* and *data processing* are also not always clearly distinct. One example is when data processors exert some data control by determining purpose and means of processing personal data when taking decisions about their IT infrastructure or in defence of potential hacker attacks (Hintze, 2018). Another instance arises if both, data owner and data controller, can take the initiative to put a data-processing agreement in place or to overfulfill privacy compliance terms in order to distinguish themselves in the market (Pantlin et al., 2018). Thus, legal regulations leave some unclarity in the field of third party obligations.

The second perspective, which is the focus of our study, views privacy in terms of subjective expectations about rights and responsibilities. This view is grounded in psychological contract theory (Rousseau, 1989, 1995), which describes individual's personal interpretation of obligations for each party involved. More precisely, psychological contracts are defined as "an individual's beliefs about the terms and conditions of a reciprocal exchange agreement between that person and another party" (Robinson, 1996, p. 575). In the context of privacy obligations, we refer to psychological contracts as *privacy contracts*.

That it is possible – and useful – to differentiate legal and psychological perspectives is demonstrated by observations that a legal contract that allows the (re-)use of data only partly attenuates perceptions of privacy breaches. As Mamonov and Benbunan-Fich (2015) demonstrate, individuals can perceive the capturing of personal information as a privacy breach even if this action is covered by a legal agreement. Hence, even if something may be legally possible, customers may still feel that a certain data practice violates their personal understanding of what is acceptable. This illustrates that psychological privacy contracts tend to exist next to and often independent of actual or written legal obligations and that psychological contracts have a powerful impact on individual reactions. Understanding the subjective perspective of customers is especially relevant for online companies, as customers may

sanction their privacy handling independent of a company's compliance with legal obligations.

Considering privacy agreements within the framework of psychological contract theory offers several benefits: Firstly, it explicitly addresses the relational nature of information privacy by framing privacy as subjectively held expectations about the mutual obligations when data sharing agreements are entered into. This allows to focus on the personal meaning and relevance of privacy independent of the question whether privacy was safeguarded or infringed in actual terms. Conceptualizing privacy as psychological contract thus provides the theoretical foundation to understand the frequent disparities in perspectives between actors about what constitutes permissible actions or obligations with respect to customer data.

Psychological contract theory further draws our attention to the possibility of negative as well as positive contract handling, in that it is possible to both breach and fulfil contracts. Contract breaches are usually the ones that make the headlines and have also been the focus of past research about online privacy. Malhotra et al. (2017), for instance, found that perceived violations of obligations reduced customers' intentions to reuse retailers' websites, while other studies demonstrated that privacy breaches lowered intentions to continue buying from an online market (Pavlou and Gefen, 2005), decreased the amount spent on online purchases (Janakiraman et al., 2018) or lead to a decrease in stock market performance of companies short- and long-term (Rasoulian et al., 2021).

However, studies in the field of employee–employer relationships, in which psychological contract theory was first developed (Robinson, 1996; Rousseau, 1995), provides evidence for the relevance also of psychological contract fulfilment. Analysing diary entries of employees, Conway et al. (2011) for instance found that fulfilling or even exceeding perceived obligations increased positive emotions such as feeling cared for and self-worth. In the privacy literature, this positive end of the spectrum has so far found little attention. This is problematic as it severely limits our understanding of consequences across the diversity of possible privacy handling obligations — and thus also our possibility to guide companies in how to manage their privacy obligations and customer relations with a view to supporting the long-term viability of their business.

1.2. Privacy contracts and continuance intentions

The long-term viability of businesses is linked to the willingness of customers to keep returning for their products or services, i.e., their customers' *continuance intentions* (Castaneda et al., 2017). Compared to the intention to purchase a particular item (in preference to another item or none), continuance intentions thus capture individuals' general willingness to return to a company (or to abandon it) and are thus a strong, general measure of a company's viability. While assessing individual product purchases can provide a good indication of the attractiveness of a company's offers and its bottom-line, a drop in continuance intentions can signal the actual demise of company and have therefore become one of the most common indicators to capture success in e-commerce (Kawaf and Tagg, 2012; Malhotra et al., 2017). The importance of continuance intentions is especially high in an online context, where customers can usually switch quickly and easily between a large number of companies that provide similar services.

Given the importance of online privacy for continuance intentions (e.g., Aslam et al., 2020; Malhotra et al., 2017; Rasoulian et al., 2021; Yin et al., 2015), it may surprise little that past studies provide a convincing link between online companies' mishandling of privacy and customers' reduced continuance intentions, i.e., the negative impact of mishandling privacy obligations by first parties (e.g., Fang and Chiu, 2014; Hsieh, 2012). Mamonov and Koufaris (2014), for instance, demonstrated that perceptions of a privacy breach by smartphone users increased their intentions to terminate their contract with the provider. Comparing two types of psychological contract breaches experienced by customers of an online auction website, Fang and Chiu (2014) further demonstrated that experiences of contract breach led to negative word-of-mouth and e-boycotts due to mediating experiences of anger, while feelings of dissatisfaction served as mediator for intentions to switch to another seller. Janakiraman et al. (2018) observed that data breach announcements reduced customer spending in warehouses and resulted in a move to alternative, unbreached channels to shop from this company (e.g., from online shopping to a physical store). The latter is especially problematic for retailers that only operate online and cannot offer alternative channels and may thus lose customers to other companies.

Privacy contract handling also has a positive side, namely when privacy promises are fulfilled. Contract fulfilment happens when an organization is seen to stick to its promises or even exceeds the promises made (Conway and Briner, 2002). Few studies so far have considered the effects of fulfilling privacy contract obligations. An exception is a study by Flavian and Guinaliu (2006) who found that the perceived security of handling personal data resulted in more trust in and higher loyalty to a retailer's website. Indirect indications of a possible positive link between privacy contract fulfilment and customer reactions are studies that found that customers are willing to pay a premium for goods or services if online shops offer better privacy protection. Letting participants decide between purchases from vendors with low versus high privacy ratings, Tsai et al. (2011), for instance, found that customers preferred purchases from sites that promised better privacy. Participants were even willing to pay more for the same product, if the vendor had a higher privacy rating. Gurumurthy and Kockelman (2020) made similar observations in the context of self-driving vehicles, where more privacy conscious individuals indicated a higher willingness to pay for masking the locations they had driven to. Consumers thus seem to value adequate handling of privacy and are not only willing to pay more to purchase at such retailers but also show greater e-loyalty to privacy conscious companies.

Taken together, this evidence suggests that continuance intentions are differentially affected by perceptions of either the positive handling of a privacy contract (i.e., privacy contract fulfilment) or the negative handling of a privacy contract (i.e., privacy contract breach).

Studies in customer data vulnerability and effects on customer behaviour usually assume a cognitive path (e.g., trust) and an affective path (e.g. emotional violation) (Martin et al., 2017). The same is true for psychological contract theory indicating basic psychological processes of sense-making. The cognitive path covers the rational evaluation of the situation in which the behaviour of the other party needs to be interpreted as relevant to the psychological contract for a reaction to occur. This is captured in the definition of a psychological contract breach as the "subjective experience" that another party "has failed to fulfil adequately the promised obligations of the psychological contract" (Robinson, 1996, p. 576). The cognitive path also helps to understand situations in which an actual breach or fulfilment may have occurred but that did not lead to a reaction, e.g., because a person did not notice it or because the breach/fulfilment was not important enough to be perceived as a relevant event. It can also explain situations that are (objectively) unrelated to the psychological contract but are interpreted in its contexts (e.g., a data sharing practice that is legally allowed but still considered as unacceptable). The cognitive path thus mediates between psychological contract handling situations and individuals' reactions to them, as without this cognitive connection no relationship between the two will exist.

The second mediator in psychological contract theory is the affective path, which focuses on the emotional impact of psychological contract handling. This is based on the observation that psychological contract breaches often leave their victims feeling violated, angry and disappointed (Robinson and Morrison, 2000), while contract fulfilments can improve positive emotions such as surprise and self-worth (e.g., Conway et al., 2011). Transferred to the context of privacy, this means that both cognitions and emotions will determine how

individuals react to perceived privacy contract (mis)handling (Zhao et al., 2007), and that both aspects need to be taken into account when investigating customers' continuance intentions in the aftermath of privacy breach or fulfilment information.

In the context of e-commerce, we can transfer above observations to the link between privacy contract handling and continuance intentions, leading to the expectation that privacy contract breach – mediated cognitively through perceived lack of fulfilment and affectively through feelings of contract violation – will reduce continuance intentions, while privacy contract fulfilment – again mediated through both the cognitive and affective paths – will increase continuance intentions. This can be formulated into two hypotheses, namely that continuance intentions are higher in cases of privacy contract fulfilment than in cases of privacy contract breach and that these effects are mediated through the degree of breach/fulfilment perceptions (cognitive path) and feelings of (non)violation (affective path).

H1: Situations of privacy contract fulfilment will be linked to higher continuance intentions than situations of privacy contract breach.

H2: The relationship between privacy contract handling and continuance intentions is mediated by breach/fulfilment perceptions and feelings of violation.

1.3. Party responsible for privacy contract handling

Psychological contracts are usually conceptualized as an agreement between an individual and the organization this individual is linked to (Robinson, 1996; Robinson and Morrison, 2000). In an e-commerce context, *individual* refers to the online customer, while *organization* refers to the platform or company that customers share their information with to obtain services or goods. Hence, in the first instance a privacy contract is an obligation between a customer and the company.

In reality, however, most online stores and platforms work with third parties (e.g., for customer analytics, marketing or logistics; Akter and Wamba, 2016). Customers are generally aware of this fact and know – or can at least strongly assume – that information about their profile and online purchases travels beyond the company they make their purchase from. Also, customers seem to increasingly accept the networked nature of privacy management, such as targeted advertising in exchange for the free service of a website (Schumann et al., 2014). Still, the *unauthorized* third party access remains one of the major concerns of online consumers when shopping online (Miyazaki and Fernandez, 2001). Also, knowing that an online shop shares personal information with external parties seems to increase the perceived risk of shopping from such a store and in consequence decrease purchase intentions (Jai et al., 2013). Such observations are a clear indication that concerns about third parties impact customer reactions towards first parties that use their services and thus emphasize the importance to consider the networked nature of privacy.

The question is whether the difference in status as first versus third party affects the perception of responsibility for privacy contract handling, i.e., whether third parties are held to account in the same way as first parties even though they are not directly linked with the customers whose data they access and process. To our knowledge no studies have so far investigated this question directly in the context of online privacy. However, research in organizations on psychological contracts in multi-agency relationships can give some direction, as it suggests that the psychological contracts individuals form with disparate entities differ in their nature and thus effect. *Multi-agency relationships* refer to situations in which an employee forms a relationship not only with their direct employer but also with other linked entities and in consequence develops separate and distinct psychological contracts with each of the entities (e.g., Claes, 2005; Lapalme et al., 2011). Dawson et al. (2014) investigated this situation for consultants that become part a 'triangular relationship' between the consulting firm as employer, the client firm they work with and themselves. Studying how psychological contract breach by one organization impacts on the psychological contract with the second organization, the authors found that breaches, regardless by which organization, led to feelings of violation and fewer positive behaviours, and that negative reactions 'spilled over', in that breaches by one company also led to negative reactions to the other. However, they also found that effects differed depending on whether the psychological contract breach was caused by the consultancy firm (i.e., the employer), rather than the client, indicating that the employing organization received more severe reactions.

Explanations for the differences in reactions towards both organizations despite causing the same event (i.e., psychological contract breach) lay in the different interpretations of the events. Psychological contracts are specific in the sense that they are formed in particular situations towards specific actors and thus encode individualized expectations and obligations towards the other party. The nature of the relationship between an individual and an organization thus determines how the psychological reaction takes form (e.g., in terms of its scope, stability, time frame, tangibility; Parks et al., 1998). The more severe reactions towards an employing organization compared to a client organization can thus be explained by the fact that psychological contracts with the former tend to be broader, more clearly defined and based on longer-term commitments resulting in stronger emotional and behavioural responses (Alcover et al., 2016; Dawson et al., 2014).

While the situation between employees in multi-agency relationships and that of customers of online companies may not be directly comparable, the underlying psychological mechanisms of psychological contract formation remain transferable. Customers, confronted with first and third parties handling their personal data, will form privacy expectations and thus psychological privacy contracts with both parties. However, customers will likely perceive their main relationship to be with the online retailer (i.e., first party), as they give their data in the context of an economic exchange directly only to this organization. The online retailer will thus carry the main responsibility for ensuring the adequate handling of customers' data. Given this primary responsibility, it can be expected that the psychological contract with this first party will be more clearly defined, more explicit and endowed with stronger privacy obligations. The act of actively providing information to an online platform or retailer will further have an effect on the salience of privacy obligations towards this organization creating stronger and more vivid privacy contracts than with third parties that receive customers' data only indirectly and hidden from view.

Taken together, this evidence suggests that customers will react to information about the positive or negative privacy contract handling of first parties more strongly than to information about third parties. Thus, while we expect that privacy contract handling (either in the positive sense of fulfilment or in the negative sense of breach) by both first and third parties will affect continuance intentions, we hypothesize that these reactions will be stronger for privacy contract handling by the first party compared to the third party. These stronger reactions will find their expression also in the mediating factors (perceptions of breach and feelings of violation), leading to the following two hypotheses:

H3a: Breaches by the first party will lead to lower continuance intentions, while fulfilment by the first party will lead to higher continuance intentions compared to third party breach or fulfilment, respectively.

H3b: Breaches by a first party will lead to higher perceived privacy breach and higher feelings of violation, while fulfilment by the first party will lead to lower perceived privacy breach and lower feelings of violation compared to third party breach or fulfilment, respectively.

1.4. Intentionality of privacy contract mishandling

A considerable part of privacy incidents is not due to purposeful actions of a retailer but due to actions of others. In a highly informative study on data breaches in the USA between 2005–2015, Posey

et al. (2017) identified 4500 privacy incidents involving personally identifiable information, of which most were caused by actions from outsiders (e.g., hacks or identity/credit card theft). Rasoulian et al. (2021) came to a similar insight in a review of literature on data breaches: only the minority of reported breaches was caused intentionally by someone within the company, while the majority of data breaches was either caused by outsiders (theft, hacker attacks) or by accidents (technical error, accidental disclosure, misplaced data sources or improper disposal). Privacy breaches are thus not always the intentional action of a company but are often the result of accidents or actions by others. We refer to such incidents as *unintentional privacy breaches* to differentiate them from *intentional privacy breaches*: while in the case of unintentional breaches a company becomes a victim of others' actions, in intentional breaches the company itself pursues actions that violate privacy obligations (e.g., by selling customer data despite promises not to do so). Past research on psychological contracts have focused primarily on intentional breaches (e.g., Chih et al., 2017; Fang and Chiu, 2014; Malhotra et al., 2017; Pavlou and Gefen, 2005), while research on online privacy seems to have focused primarily on unintentional ones (e.g., Carre et al., 2018; Janakiraman et al., 2018; Posey et al., 2017; Rasoulian et al., 2021). In this study, we aim to understand both situations, that is, apart from the question of whether customers perceive a privacy breach to have occurred, we also consider whether the intentionality of the breach affects reactions.

Past research in organizations has shown that negative reactions are much more severe, if individuals hold the organization responsible for the breach (e.g., Conway and Briner, 2002; Robinson and Morrison, 2000; Rousseau, 1995). Janakiraman et al. (2018) studied the result of unintentional privacy breaches in a direct way by comparing customer behaviours before and after a data breach announcement due to hacking. In contrast to findings from research on other psychological contract violations, customers did not abandon the retailer but simply moved to other purchasing channels. The fact that the incident was due to hacking may have been perceived as attenuating circumstance. Similar to the attribution of a contract breach to a 'misunderstanding' (Robinson and Morrison, 2000), the perception that the first party was 'not at fault' may thus reduce negative reactions. Moreover, two studies in the area of supply-chain management revealed that the internal attribution of a contract breach (i.e., unwillingness to deliver on obligations despite being able to) led to lower order quantities than if the breach was attributed to external factors (i.e., due to circumstances beyond the company's control) (Eckerd et al., 2013, 2016). These studies were conducted in a business-to-business (B2B) context and not with respect to privacy but they suggest that the differentiation between intentional versus unintentional breaches affect customer reactions in important ways. In the context of customer privacy, we thus expect that intentional privacy contract breaches lower continuance intentions more than situations in which privacy contract breaches happen unintentionally.

H4: Intentional first party privacy contract breach will be linked to lower continuance intentions than unintentional contract breach.

2. Methods

2.1. Study approach

The controlled investigation of privacy contracts in real life is challenging, as the creation of privacy breaches for academic purposes is problematic on ethical and legal grounds. We therefore used an online experiment using experimental vignette methodology (EVM) to compare privacy contract handling situations. EVM presents participants "with carefully constructed and realistic scenarios" (Aguinis and Bradley, 2014, p. 352) to allow experimental realism and the controlled manipulation of independent variables, thus ensuring internal and external validity. Scenarios are a common method to investigate privacy violations (cp. Siponen and Vance, 2014) and can provide a realistic and powerful approach to investigate phenomena that are not easily studied in real life (Aguinis and Bradley, 2014). To ensure realism and relevance, we followed the guidelines developed by Aguinis and Bradley (2014) and Siponen and Vance (2014) including the creation of a realistic looking website to increase immersion, manipulations based on actual news items as well as providing specific examples of violations and fulfilment.[1]

The core experiment was a 2x2 design, comparing type of contract handling (breach versus fulfilment, testing H1) and party responsible for the contract handling (first versus third party, testing H2 and H3). We added two additional conditions, an unintentional breach condition (testing H4) and a control condition, leading to a total of six experimental conditions. The control condition was added to allow a comparison between situations where participants received information about privacy handling (i.e., where experimental manipulations take place and should lead to the hypothesized effects) with a situation in which no information was given about privacy handling and thus no experimental manipulation took place. The latter control condition allows to establish whether the experimental manipulations do have an effect on participants' reactions as well as how large the effect of the experimental manipulations are compared to a neutral situation. To ensure the controlled comparison across manipulations, each participant only experienced one of the six conditions (between-subject design).

2.2. Sample

Participants were recruited through the online crowdsourcing platform Crowdflower. The choice for an online crowdsourcing platform was deliberate as individuals who are part of an online panel represent a diverse group of working adults, familiar with online environments and privacy settings (Behrend et al., 2011; Casler et al., 2013). Recruitment thus ensured that our participants have a high likelihood of using online services such as e-shopping and are thus able to relate to and have an understanding of the experience of online shopping increasing the realism of reactions. Comparisons with traditional samples (e.g., students, in-person convenience samples) also indicate that online samples tend to be more representative of the general population and that results are of comparable reliability (Buhrmester et al., 2011; Berinsky et al., 2012).

In total, 579 people reacted to our invitation to the experiment. Of these 257 dropped out before filling out a single item, while 22 others only filled in qualitative information in the 'registration form' (see Section 2.5). For a further two a software error meant that the experimental condition was not recorded, so that they could not be assigned. This left 298 useable surveys. This group comprised 56.3% men and 43.7% women. The sample had a good distribution across age groups with 11.8% aged 18–24, 29.2% aged 25–34, 29.5% aged 35–44, 19.1% ages 45–55 and 10.4% 55 or older. The majority of the sample had bachelor as highest degree (43.7%), with the remaining participants distributed across high-school (29.1%), master (15.4%), professional degree (5.9%), doctorate (2.4%) and no schooling (3.1%). The majority of participants classified themselves as White (76.7%), a smaller part as Asian (13.5%) and the remainder as Hispanic (4.5%), African–American (2.8%), Indian–American (1.4%) or 'other' (1.0%). Frequency of online shopping in this sample was moderate (m = 3.38, sd = .83; 3.0 on the scale referring to 'sometimes'). Experiences with privacy invasions were rare (m = 2.22, sd = .95), while recent exposure to news about negative privacy events was moderate (m = 3.12, sd = 1.02). Participants thus did not seem to represent extremes in either their online shopping habits or their privacy experiences.

[1] In fact, the website seemed convincing enough for the panel provider Crowdflower to block access to our pages, as it thought we were using the panel to sign up participants for a real service. Access was only restored after we confirmed that the survey was run as part of an academic study.

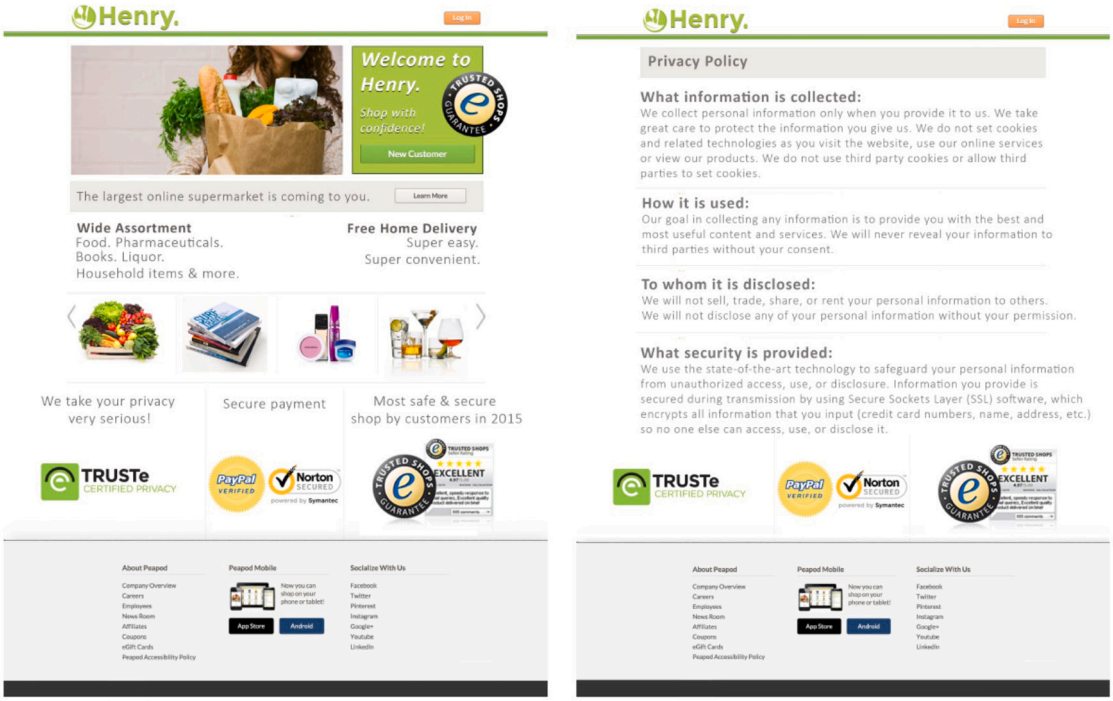


Fig. 1. Screenshots of landing page and privacy statement for the online store 'Henry'.

2.3. Variables and instruments

The dependent variable *continuance intentions* was measured with three items by Bhattacherjee (2001, e.g., "I intend to continue using the service rather than discontinue its use"). The scales for *perceived contract breach* (5 items; e.g., "Henry has broken many of its promises towards me even though I've upheld my side of the deal") and *feelings of violation* (4 items; e.g., "I feel betrayed by Henry") were adapted from Robinson and Morrison (2000). These are both global measures evaluating individuals' overall perception of the extent to which an organization has fulfilled or failed to fulfil its obligations or promises. This contrasts with composite measures that require participants to indicate fulfilment of promises with regard to a set of specific items (e.g., high pay, promotion, education). We chose a global measure, since it is challenging to develop a set of items that measure fair information practices in online settings without prior history. Moreover, global measures have shown to possess stronger relationships with outcome variables compared to composite measures (Zhao et al., 2007). The contract breach scale further comprised positively and negatively worded items, which made the scale an excellent fit for our setting with breach as well as fulfilment conditions.

Demographics were captured for gender, age (in five groups from 18 to 55+) and highest completed education (from 'no schooling' to 'doctoral degree'). Experiences with previous privacy invasions – either in person or by proxy through media – can impact the propensity to trust organizations with personal data (Bansal et al., 2010) and can thus impact the cognitive and affective reactions to privacy contract handling. We therefore included personal experiences with privacy invasions (1 item: "How frequently have you personally been victim of what you felt as an invasion of your privacy") as well as degree of media exposure (1 item: "How much have you heard or read during the last year about the use and potential misuse of information collected from the Internet") as control variables (both adapted from Malhotra et al., 2004) to ensure these potential influences can be captured. Unless otherwise indicated, all items were measured on a scale from 1:strongly disagree to 5:strongly agree. The full list of items is provided in Appendix A.

2.4. Material

The setting of our experiment was a fictious online grocery store called *Henry*. To create an immersive setting, we programmed webpages with the look and feel of a real webstore. The first page represented Henry's homepage with a short introduction to its services (Fig. 1 left). To create high privacy expectations, this text emphasized that Henry "prides itself" on being "a safe and reliable environment for the most personal of purchases". Privacy expectations were further emphasized by adding three well-known privacy and quality seals. In the introduction text, participants were further advised that Henry relies on a third party advertising agency called AdRoom for its service. We moreover constructed a privacy statement in imitation to existing privacy policies (Fig. 1 right).

For the manipulation we used a fictitious news item supposedly published by the renowned business news provider BusinessInsider. The wording was based on existing online news articles describing privacy breaches/fulfilments, while the layout replicated the formatting style, logo and colours of BusinessInsider news. An example is given in Fig. 2; for all six manipulations see Appendix B.

Before using the six news items in our experiment, we conducted a pilot-test with 40 master students to ensure that the texts of the six news items were equally easy to understand, trustworthy and credible. This step was important to ensure that the texts would not affect participants' reactions in unexpected ways simply through disparities in how easy to understand or credible the texts were perceived. A one-sample t-test demonstrated that all texts were perceived as credible, trustworthy and easy to understand (means significantly above the neutral scale point of 3; see Table 1). ANOVA analyses further revealed no significant differences amongst the six texts in the three criteria, assuring equality of texts in these three aspects. We further tested the six news items for the reactions they elicited in readers to ensure that the texts were successfully representing the three privacy handling conditions: privacy contract breach, contract fulfilment and the control situation. An ANOVA analysis showed significant differences for the perception of Henry in the necessary direction, which indicates that the texts were effective as experimental manipulations.

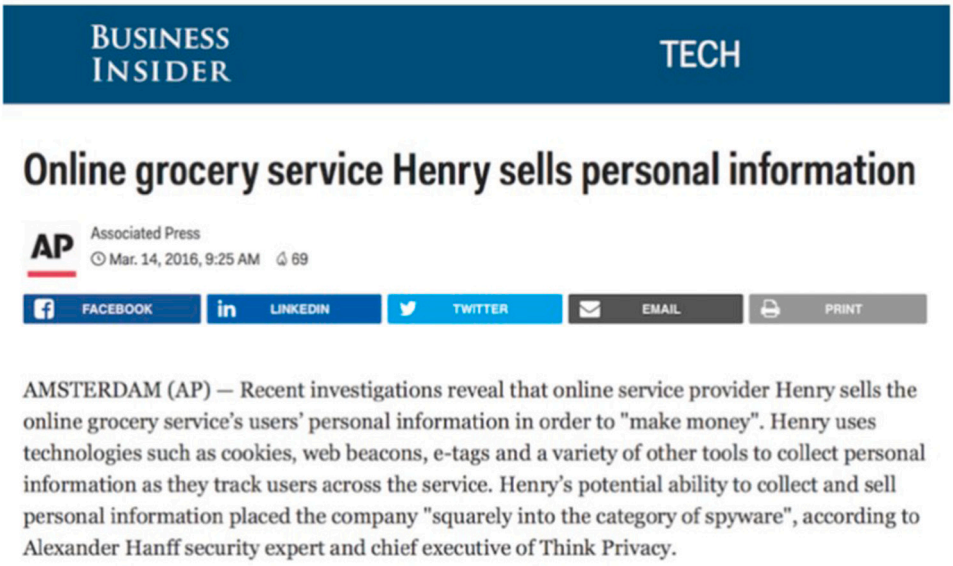


Fig. 2. Example for the experimental manipulation (intentional breach condition by first party).

Table 1
Results of pilot test for manipulations.

	Credible	Trustworthy	Easy to understand	Reaction towards Henry
Henry intentional breach	4.17	3.67	4.83	2.17
Henry unintentional breach	4.33	4.67	4.33	2.67
Henry fulfilment	3.38	3.83	4.33	4.33
AdRoom intentional breach	3.50	3.50	4.17	2.67
AdRoom fulfilment	3.60	3.80	4.20	4.00
Control	4.60	4.20	4.00	4.40
	F = 1.25 p = .31	F = 1.31 p = .29	F = .56 p = .73	F = 8.51 p<.001

2.5. Experimental procedure

After agreeing to participate in the experiment, participants were presented with a link that brought them to Henry's homepage with the introduction text. A popup then presented its privacy policy. After closing this window, participants were then invited to register as a new Henry user. Information requested on the registration form included first name, last name, gender, age, telephone number, monthly income, hobbies/interests and credit/debit card number. To reinforce Henry's privacy obligations, participants were notified that the information they provided would be kept in the strictest confidence. After registration, participants were asked to list their last ten grocery purchases to provide Henry with the opportunity to provide "better and more personalized" services. Participants were again advised that this personalization was done with the help of the third party advertising agency AdRoom. This step was added to reinforce the online shopping context and again reinforce a privacy-sensitive setting of information sharing with Henry as well as a third party. Subsequently, participants were randomly assigned to one of the six experimental conditions using the randomization feature of the survey software. The manipulation was done using a pop-up window showing the respective news item. After reading the news, participants filled in the post-exposure questionnaire capturing perceived contract fulfilment, feelings of violation, continuance intentions and demographic information. Finally, participants were debriefed about the intention of the experiment and the fictitious nature of the setting. Participants were paid $0.10US after completing the questionnaire in line with payments in comparable tasks at the time of the study. To increase survey quality (Jakobsson, 2009), participants were manually rewarded an additional $0.15US in case of proper completion (e.g., controlling for surveys with identical answers to all items).

2.6. Data preparation and analysis

Missing-value analysis (MVA) revealed that 86 participants provided incomplete surveys (28.8% partial response rate). Of these the majority were item-level missings (i.e., incomplete scales), while only 1.68% were missings for a complete scale. In handling missings, we followed the recommendations of Newman (2014). Since construct-level missings were scarce, we did not use imputation. For item-level missings we calculated scale mean values based on available information. Outlier tests using Mahalanobis distance, Cook's distances and Leverage values revealed two participants with problematic values. They were removed before further analyses retaining 296 valid answers.

A confirmatory factor analysis (R, lavaan package) revealed that negatively worded items in the perceived contract breach scale loaded only weakly on the construct (0.28). Removing the two negatively worded items and fixing errors between two violation items led to an acceptable model fit with $\chi^2(31) = 104.73, p < .001, CFI = .98, TLI = .97, RMSEA = .097(95\%CI, [.08, 1.12]), SRMR = .05$. Further analyses were thus conducted with the three positively worded contract breach items, leading to a positive orientation of the concept (i.e., privacy contract fulfilment instead of breach).

Table 2 demonstrates that all measures had adequate psychometric properties. Composite reliability (CR) and Cronbach alpha values were above .70, confirming internal consistency. Values for Average Variance Extracted (AVE) were above 0.50. Further, square root of AVE values were higher than the latent correlation values between constructs confirming discriminant validity (Fornell and Larker, 1981).

The mediation models were tested using the PROCESS macro v3.0 in SPSS (Hayes, 2018), which allows the use of multicategorical predictors. The confidence interval was set to 95% and the number of bootstrap samples to 5000.

3. Results

3.1. Testing for demographics and control variables

Age groups did not differ across any of the concepts (perceived fulfilment: $F(4, 281) = 2.43$, *ns*; feelings of violation: $F(4, 281) = 3.10$, *ns*; continuance intentions: $F(4, 281) = 2.42$, *ns*; $n = 286$). Genders did not

Table 2
Discriminant validity of constructs.

	PF	V	CI	AVE	CR	α
PF	**.95**[a]			.89	.86	.96
V	.73	**.95**		.90	.92	.97
CI	−.77	−.65	**.69**	.75	.78	.89

PF: perceived contract fulfilment; V: feelings of violation; CI: continuance intentions.
[a]Diagonal values represent square root of AVEs, the off-diagonal values correlations.

differ with respect to degree of felt violation ($m_{women} = 2.98, m_{men} = 2.92$; $t(235.69) = -.36$, ns; $n = 286$). However, women showed lower levels of perceived privacy fulfilment than men ($m_{women} = 2.55, m_{men} = 3.08$; $t(248.28) = 3.49$, $p < .01$) and lower levels of continuance intentions ($m_{women} = 2.60, m_{men} = 3.03$; $t(225.30) = 3.14$, $p < .01$), indicating that gender has a significant effect on relevant outcomes. Privacy invasion experiences were not significantly linked to both mediators and the dependent variable (perceived fulfilment: $r = .03$, ns; feelings of violation: $r = .04$, ns; continuance intentions: $r = -.04$, ns; $n = 282$), indicating that past experiences of privacy invasions did not affect reactions. Media exposure was unrelated to contract fulfilment ($r = -.10$, ns) but correlated significantly with feelings of violation ($r = .15$, $p < .05$) and continuance intentions ($r = .13$, $p < .05$; $n = 284$), indicating that media exposure affected reactions in relevant ways. As recommended by Becker (2005), we therefore included gender and media exposure as control variables in all subsequent tests of hypotheses H1-4 to account for their influence in the analyses.

3.2. Impact of responsible party and privacy contract handling

We conducted a 2 (first party versus third party) × 2 (intentional breach versus fulfilment) ANCOVA to test for the impact of party responsible depending on type of privacy contract handling. Given their significant correlations with relevant aspects, gender and media exposure were included as control variables (cp. section above).

Type of contract handling significantly influenced continuance intentions ($F(5, 171) = 21.45, p < .001, \eta_p^2 = .39$) in that privacy contract fulfilment led to higher continuance intentions than privacy contract breach, confirming hypothesis H1. Responsible party did not show a direct effect on continuance intentions ($F(1, 171) = 3.19$, ns, $\eta_p^2 = .02$). Hence, whether it was the first or third party who fulfilled or breached the privacy contract did not make a direct difference for continuance intentions. There was a significant, albeit small interaction effect, however ($F(1, 171) = 5.25, p < .05, \eta_p^2 = .03$), which showed a slightly higher effect for first party compared to third party privacy contract breach, although not for privacy contract fulfilment (see Fig. 3 top). This provides only partial support for hypothesis H3a.

Models for the cognitive and affective reactions were highly significant (perceived contract fulfilment: $F(5, 171) = 28.26, p < .001, \eta_p^2 = .45$; feelings of violation: $F(5, 171) = 27.21, p < .001, \eta_p^2 = .44$). Again we found significant main effects for privacy contract handling in the same direction, i.e., privacy contract fulfilment led to higher perceptions of contract fulfilment and lower feelings of violation than privacy contract breach (perceived contract fulfilment: $F(1, 171) = 111.21, p < .001, \eta_p^2 = .39$; feelings of violation: $F(1, 171) = 108.76, p < .001, \eta_p^2 = .39$). The main effect for responsible party remained again non-significant (perceived contract fulfilment: $F(1, 171) = 1.12$, ns, $\eta_p^2 = .01$; feelings of violation: $F(1, 171) = 0.02$, ns, $\eta_p^2 = .00$). A small interaction effect in the hypothesized directions (perceived contract fulfilment: $F(1, 171) = 9.48, p < .01, \eta_p^2 = .05$; feelings of violation: $F(1, 171) = 18.38, p < .001, \eta_p^2 = .10$) indicates that cognitive and affective reactions to privacy contract fulfilment and breach are somewhat more pronounced for the first party compared to the third party, offering again partial support for hypothesis H3b (cp. Fig. 3 middle and bottom).

We ran additional ANCOVAs comparing the four experimental conditions with the control condition to explore the effect of situations in

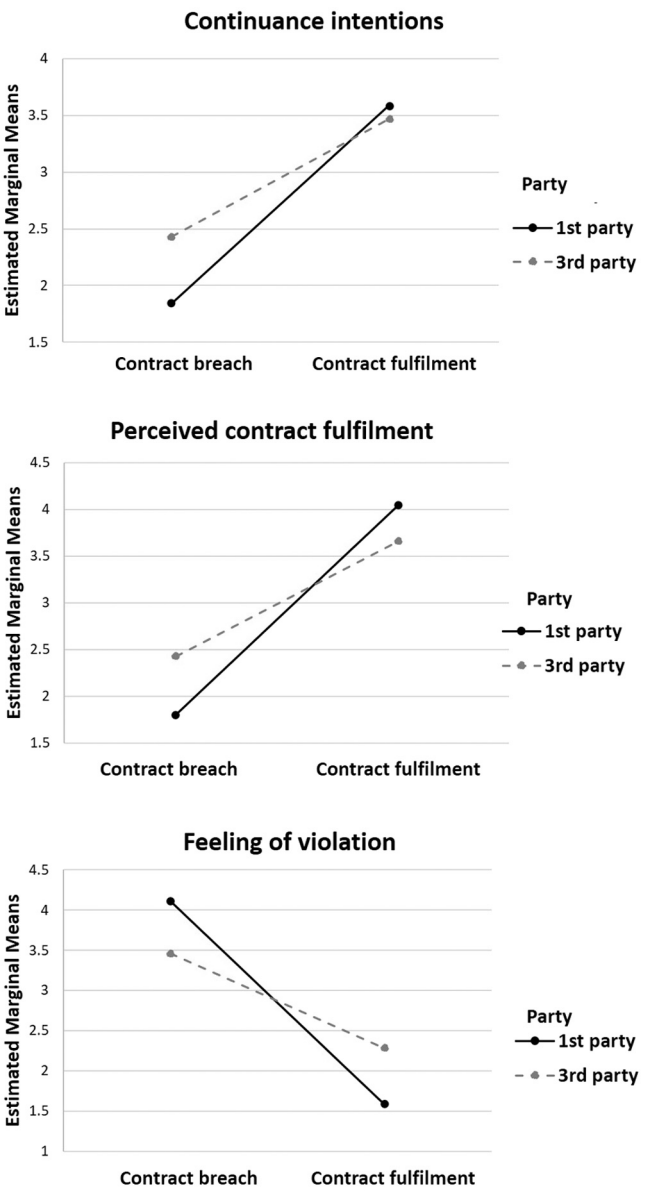


Fig. 3. Interaction between type of privacy contract handling and responsible party.

which privacy contract information (positive or negative) is revealed compared to a situation in which no information about privacy contract handling is provided (simple planned contrast with control as reference condition and gender and media exposure as control variables). Both first and third party breach led to significantly higher negative reactions on all three variables compared to the control condition (all $p < .001$). Third party contract fulfilment did not lead to significantly different reactions than the condition without privacy information (control) indicating that positive actions by the third party did not improve perceptions of Henry in a relevant way. First party privacy contract fulfilment, in contrast, led to higher perceived contract fulfilment and lower feelings of violation (both $p < .05$), although this did not translate into significantly higher continuance intentions. The means for the three variables across experimental conditions and the control condition can be found in Table 3.

3.3. Test for mediation

We conducted the mediation analysis with privacy contract handling as multi-categorical predictor (four levels: control/C, intentional

Table 3
Descriptive information across conditions.

	First party		Third party		Control
	Breach (n = 48)	Fulfilment (n = 34)	Breach (n = 50)	Fulfilment (n = 51)	(n = 50)
PF	1.76 (sd = .98)	4.04 (sd = .89)	2.33 (sd = 1.33)	3.66 (sd = .86)	3.25 (sd = 1.01)
V	4.11 (sd = .93)	1.59 (sd = .95)	3.46 (sd = 1.26)	2.28 (sd = 1.12)	2.29 (sd = 1.03)
CI	1.84 (sd = .98)	3.59 (sd = .80)	2.43 (sd = 1.09)	3.47 (sd = 1.01)	3.33 (sd = .73)

PF: perceived contract fulfilment, V: feelings of violation, CI: continuance intentions.

breach/IB, unintentional breach/UB and fulfilment/F), the two mediators perceived contract fulfilment and feelings of violation and continuance intentions as dependent variable. We again included gender and media exposure as covariates. Since the PROCESS macro only allows testing against one reference category, we ran three separate analyses to test all pairwise comparisons across the four contract handling conditions; the first with the control condition as reference category, the second with intentional privacy contract breach and the third with privacy contract fulfilment as reference.

The pairwise comparisons of contract handling conditions showed a significant effect on both mediators for all combinations. Both intentional and unintentional privacy contract breach led to significantly lower perceptions of contract fulfilment ($b_{IB \diamond C} = -1.53, p < .001; b_{UB \diamond C} = -1.11, p < .001$) and higher feelings of violation than the control condition ($b_{IB \diamond C} = 1.89, p < .001; b_{UB \diamond C} = 1.12, p < .001$). Intentional breach was also linked to more adverse reactions compared to unintentional breach (perceived contract fulfilment: $b_{IB \diamond UB} = 0.42, p < .05$; feelings of violation: $b_{IB \diamond UB} = -0.69, p < .01$) and privacy fulfilment (perceived contract fulfilment: $b_{IB \diamond F} = 2.11, p < .001$; feelings of violation: $b_{IB \diamond F} = -2.53, p < .001$). Similarly, unintentional privacy breach led to significantly more negative reactions than fulfilment or control condition (perceived contract fulfilment: $b_{F \diamond UB} = -1.69, p < .001; b_{C \diamond UB} = -1.11, p < .001$; feelings of violation: $b_{F \diamond UB} = .1.84, p < .001; b_{C \diamond UB} = 1.12, p < .001$), suggesting that even breaches without fault of the first party led to adverse cognitive and affective reactions. Overall, intentional privacy breach was linked to the highest level of adverse reactions, followed by unintentional privacy breach, no contract information (control condition) and lastly privacy fulfilment with the most positive reactions (cp. also Table 3; result tables for the three analyses are provided in the supplemental materials for space reasons).

The second part of the mediation model, testing the relationships between the two mediators and continuance intentions, was also significant (perceived contract fulfilment: $b_{PF \diamond CI} = 0.48, p < .001$; feelings of violation: $b_{V \diamond CI} = -0.30, p < .001$). Further, except for the contrast between unintentional breach versus fulfilment ($b_{IB \diamond UB} = .48, p < .05$), all direct effects between contract handling and continuance intentions were non-significant, confirming a mediation effect. These findings provide support for hypotheses H2.

3.4. Intentionality of privacy breaches by the first party

To test intentionality, we conducted an ANCOVA across the three privacy contract handling conditions by Henry plus the control condition, again adding gender and media exposure as co-variates. The overall model was highly significant with $F(5, 181) = 20.07, p < .001, \eta_p^2 = .36$, in that disparate privacy contract handling resulted in significant difference in continuance intentions ($F(3, 181) = 28.45, p < .001, \eta_p^2 = .22$). Planned contrasts with intentional privacy contract breach as reference category demonstrated that intentional breach led to significantly lower continuance intentions compared to all other conditions (i.e., unintentional privacy contract breach, privacy contract fulfilment as well as the control condition; all $p < .001$; cp. Fig. 4). These findings support hypothesis H4. Checking for controls, women showed lower continuance intentions than men, $F(1, 181) = 6.40, p < .05, \eta_p^2 = .03$, whereas media exposure showed no effect $F(1, 181) = 0.95, \eta_p^2 = .01$, *ns*.

4. Discussion

In our study we investigated individuals' reactions to first versus third party privacy handling, proposing an extended network perspective of online privacy in an e-commerce context. Although actions by the first party led to somewhat stronger reactions, both first and third party privacy contract handling led to significant differences in continuance intentions as well as mediating cognitive and affective effects, confirming our perspective of networked privacy.

More specifically, in line with previous studies (e.g., Mamonov and Koufaris, 2014; Mamonov and Benbunan-Fich, 2015), psychological privacy contract breaches reduced continuance intentions. Yet, in an extension of previous studies, we demonstrate that this reaction holds independent of whether the breach occurs by the first or third party. In a further extension of previous research, we also found effects on the positive side of privacy handling in that privacy contract fulfilment by the first party was linked to more positive cognitive and affective reactions above and beyond a situation in which no privacy handling information is available, suggesting that awareness of privacy contract fulfilment can improve perceptions of and attitudes towards the first party. Privacy contract fulfilment did not, however, translate into higher continuance intentions. Overall, results indicate that privacy contract handling is a relevant factor in determining continuance intentions and that actions by first as well as third parties impacts customer reactions.

Our findings have important implications for understanding the role of privacy in an e-commerce context. Traditionally, psychological contracts have been conceptualized as perceived obligations between two parties (Robinson, 1996; Guo et al., 2017). Our study found that actions of a linked third party affected customers' reactions to the first party — cognitively, affectively and in terms of behavioural intentions. This demonstrates that psychological contracts with respect to privacy extend beyond the original relationship between a customer and an online retailer in that third party privacy management affects this original relationship.

Conceptually, this implies that for an understanding of privacy and privacy contracts, we need to consider not only immediate relationships between customers and retailers but the whole network of obligations customers enter into. Pavlou and Gefen (2005) made a related point in the context of online marketplaces, in which contract breaches by one seller can reflect negatively on others, as they tend to be judged collectively in their role as 'online sellers' (Martin et al., 2017). Our context differs from this setting in that first and third parties are not collectives of organizations with mutually replaceable actors but identifiable and mutually dependent entities. Instead of a one-to-many relationship, which in essence still implies a dualistic view, our setting implies a multitude of inter-relations. Our study thus shifts our understanding of privacy and demonstrates that privacy management needs to be broadened from a dualistic relationship to a network of obligations with multiple linked parties.

Our study introduced the concept of psychological privacy contracts as a strong theoretical framework to investigate customer reactions in this more complex network of interrelated players. The notion of privacy contract allows the exploration of subjective meanings of parallel and interdependent privacy expectations across a wide spectrum of contract handling situations — enabling the systematic consideration

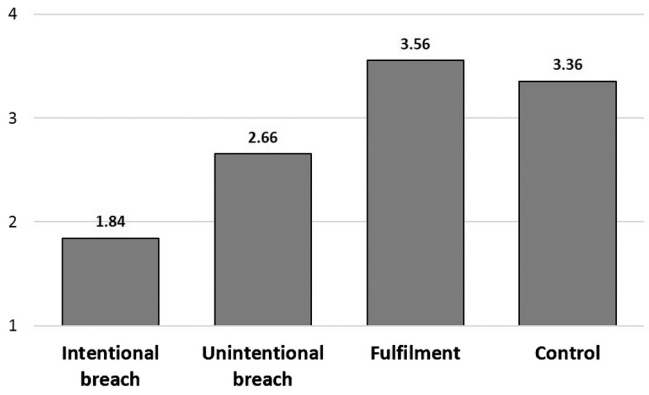


Fig. 4. Continuance intentions across privacy contract handling conditions by Henry.

along the complete range of privacy handling situations beyond the traditional focus on privacy failures. In that regard, our study is the first to consider the effects of privacy contract fulfilment as well as disparate breach conditions (including a neutral condition). Pitting this wider spectrum of privacy handling situations against each other unearthed interesting disparities in effects. First parties were punished more severely than third parties for privacy breaches but did not gain more from fulfilling privacy expectations. Also, while third party actions led to negative effects for Henry, positive actions did not profit the company. Thus, actions of the third party affected reactions on the negative spectrum of privacy contract handling (i.e., breach), but less so on the positive side. For the first party, in contrast, the explicit fulfilment of a privacy contract led to more positive cognitive and affective reactions compared to a privacy neutral situation without privacy handling information, even if this did not lead to direct gains in continuance intentions.

The missing effect on continuance intentions for privacy contract fulfilment is counter to our expectations. A possible explanation is that privacy contract fulfilment is a general expectation of customers and may thus no translate into direct increases in continuance intentions. In the same regard, customers did react in a positive way, cognitively and affectively, to privacy contract fulfilment by both the first and the third party. This suggests that privacy contract fulfilment does have a positive impact on the perception of privacy contract handling and emotions. While it may not lead to immediate behavioural intentions, customers' positive perceptions are an important factor in increasing loyalty longer term (Toufaily et al., 2013). Given that cognitive and affective reactions emerged as relevant mediators of continuance intentions, privacy contract fulfilment does make a difference and may potentially lead to compound effects for positive customer attitudes over time; a possibility which should be assessed in future studies.

We further found no link between past privacy invasions experiences and our mediators or continuance intentions, indicating that in our sample past negative privacy experiences did not affect reactions in a significant way. While this may be surprising at first glance, this is in line with other studies (e.g. Henke et al., 2018). Most anxieties about privacy violations, or so called "customer data vulnerabilities", seem to stem from fear of potential damages or feelings of violations rather than actual experiences of data misuse (Martin et al., 2017). Given that reports on data breaches are wide-spread across basically all industries and public institutions, it is likely that a ceiling effect has been reached and customers have a generalized assumption of data vulnerability. Thus, own experiences of data breach might not provide additional information in the perspective of customers, as it fits the overall expectation. In contrast, recent exposure to media news about privacy infringements did affect reactions. A possible explanation are spill-over effects (Martin et al., 2017), which lead unaffected customers who witness violations via the media to sanction privacy violations more harshly when they experience them themselves. Such sanctioning can be understood as a way of punishing selfish or irresponsible behaviour also by individuals who are not directly affected in order to strengthen norm abidance in the market place (Fehr and Fischbacher, 2004; Jordan et al., 2016). This in fact supports our psychological perspective of networked privacy in that actions by other parties affect individuals' reactions to first parties.

Our findings make important theoretical contributions by improving our understanding of processes that create perceived privacy obligations across multiple actors. Applying psychological contract theory to the online privacy context, it becomes apparent that psychological responsibility perceptions of customers follow own cognitive and emotional logics and are not necessarily aligned with legal definitions of responsibility. Thus, even though a first party might legally not be liable for the failures of their third party, customers (psychologically) do not release the first party from perceived obligations. A network perspective of privacy contracts thus seems a more realistic representation of the complexity in personal data management we encounter today. To fully understand customers' reactions to online privacy handling, we therefore need to investigate and systematically compare a larger spectrum of privacy handling situations and amongst a larger number of actors than is traditional in current privacy research.

By contrasting situations of intentional and unintentional privacy breach our study also broadens common perspectives of privacy failures as research on psychological contracts tends to focus on intentional breaches (e.g., Chih et al., 2017; Fang and Chiu, 2014; Malhotra et al., 2017; Pavlou and Gefen, 2005), while research on online privacy focuses primarily on unintentional ones (e.g., Carre et al., 2018; Janakiraman et al., 2018; Posey et al., 2017). Intentionality emerged as an important factor for influencing participants' cognitive and affective reactions as well as behavioural intentions. The intentional breach by Henry as first party led to significantly lower perceptions of contract fulfilment, stronger feelings of violation and lower continuance intentions than the unintentional breach due to hacking. This means that although both situations were perceived as psychological privacy contract breach, the intentional breach was perceived as more severe than the no-fault situation. These observations are in line with other studies, illustrating that individuals make a difference between harm caused by accident and harm caused by intent or irresponsibility (Weiner, 1985). Such attribution of responsibility to an actor heightens negative reactions and punishing intentions (cp. Janakiraman et al., 2018; Robinson and Morrison, 2000) proposing a central role of attribution processes for individuals' sense-making of privacy events. This again emphasizes the subjective nature of privacy contracts which requires a psychological and relational lens to privacy contract handling.

4.1. Limitations and future studies

The experimental setup was intended to investigate whether privacy contract handling affects individuals' reactions. This quantitative setup

is well-placed to analyse the complex impacts of different privacy handling situation, which were the focus in this study. Equally relevant would be to understand the form, nature and content of privacy contracts and how they are (qualitatively) affected by disparate first and third party actions. The experimental approach is not intended to investigate this qualitative aspects of privacy contracts; yet, subsequent studies using qualitative methods could do much to clarify the processes underlying the quantitative observations made in this study.

Our scenario focused on one specific online store. This setting allows to investigate how customers experience privacy contract handling by a single company and is realistic in the sense that privacy breaches and fulfilment are usually events linked to individual online retailers. The setting cannot, however, answer the broader question of when and why people may move to other online retailers as customers often have alternatives they can switch to (cp. Pavlou and Gefen, 2005). In the same regard, there are also platforms or online services for which genuinely few alternatives may exist (e.g., some social media platforms or governmental services). This raises the question of which strategies customers can and do employ when switching to other services after a privacy contract breach is not a viable option, and how privacy networks affect these choices. Moreover, in this setting continuance intentions are of little relevance and other behavioural consequences may need to be explored.

A network perspective on privacy contracts further allows to investigate the formation, development and nature of relationships between various parties and how they influence privacy as well as reactions to privacy fulfilment and breaches. Future studies could thus gain much by considering the underlying psychological mechanisms that cause differential reactions such as found in our study to disparate privacy contract handling situations across various responsible parties. Of special interest, as suggested by our study, may be attribution and sense-making mechanisms for understanding customer reactions to different privacy contract handling situations.

A more comprehensive perspective of the full spectrum of privacy contract handling also opens the possibility to study the combination of effects. Pavlou and Gefen (2005) demonstrated that privacy breaches led to less actual transactions four months later. Yet, given the scant attention paid to different privacy handling scenarios, we know little about how psychological privacy contract experiences combine over time and for how long positive and negative effects last. For instance, can privacy contract fulfilment help retailers recover from previous negative privacy events by a third party or could third party fulfilment act as a buffer, so that fewer customers switch to other online retailers after later failures in privacy obligations? Given the variation of reactions to fulfilment versus breach as well as different breach conditions we advocate for a more comprehensive and long-term perspective on privacy contract handling across multiple interrelated parties.

4.2. Managerial implications

Our findings also offer concrete pointers for a successful and nuanced approach to the management of privacy by organizations relying in loyalty of their online customers.

An important result of our study is the role of third parties in shaping continuance intentions. Although reactions were strongest for intentional first party privacy breaches, our study illustrates that retailers also get punished for breaches caused by third parties linked to their business. That is, companies seem to be made co-responsible for failures of the organizations they engage with. This suggests that customers make little differentiation between a first and third party in terms of perceived privacy obligations. The networked nature of privacy obligations thus increase the possibility of spillover effects when privacy breaches happen in other, linked parties. For online retailers this means that they need to develop mitigation strategies not only in case of their own shortcomings but also in case third parties mishandle psychological privacy contracts of their customers. A strategy of 'finger pointing' will not be successful, as in customers' views first parties are psychologically implicated in any wrongdoing of linked parties. This network effect also means that first parties need to react to third party breaches as intensely as if they would happen by their own organization and need to actively invest into the trustworthiness across the whole network of organizations customer data is exposed to.

In the same regard, online retailers may benefit from positive actions with respect to privacy. In fact, fulfilment of privacy contracts seems to be a successful strategy to engage privacy-conscious customers (Tsai et al., 2011). Yet, this process only works if customers are aware of the privacy contract fulfilment, as indicated by the positive difference between control and fulfilment conditions. Hence, companies should make privacy efforts and successes as visible as possible, especially if privacy protection actions may lead customers to experience them as *exceeding* privacy contract expectations. On a more cautious note, however, fulfilment needs to be more than paying lip service to customers' privacy concerns. The severe reactions in case of intentional privacy contract breach are a reminder for retailers to be honest and transparent about their data management practices. The intentional reneging of the privacy promise caused the highest level of negative emotions, and negative emotions are main drivers for punitive reactions such as negative word-of-mouth, protests or consumer boycotts (e.g., Fang and Chiu, 2014; Grappi et al., 2013; Xie et al., 2015). Our findings are a warning that customers react very sensitively to perceived deceptions of privacy promises. Hence, businesses need to ensure that their explicit and implicit privacy signals are consistent with actual practice to avoid the perception of intentional privacy contract breaches.

In our study we focused on customer–business relationships. Given the networked nature of privacy obligations demonstrated in this study, it might be relevant for online retailers to also look into business-to-business relationships. For instance, it can be advantageous for first parties to publicly sanction third parties in order to signal their own trustworthiness. Due to the often ambiguous legal situation of data ownership, such actions could add to the risk profile of third parties. An aspect that receives quite some public attention, as it can dramatically impact customers data, is the response to law enforcement requests or cooperation with other governance agencies. Governmental information discloser requests can be expressed to both, first and third parties, which makes it even more relevant for first parties as part of their due diligence to look for third parties with strong privacy commitments in the face of governmental requests (Hintze, 2018).

5. Conclusions

Our study provides a new understanding of privacy as subjective obligations that are formed and negotiated within a complex network of interrelated actors. The psychological contract perspective which underlies this view on privacy can help businesses to be more sensitive to the value of safeguarding personal data and keeping their promises around data use. Privacy contracts are not only business transactions but create relationships between their customers and themselves that are invested with interests as well as emotions. It is thus not only their personal data customers are wary about but also their relationship with the organizations they share their data with. As our study illustrates, privacy contracts represent a system of privacy obligations in which actors become co-responsible. Online retailers therefore have to manage privacy contracts, not only for themselves but also for third parties that are linked to them. Privacy contracts are subjective expectations that often remain implicit and tacit and often strongly vary across individuals (e.g., Bayerl et al., 2018; Sheehan, 2002). Making these tacit expectations explicit can be complicated but is needed to

ensure alignment of companies' practices and customer expectations and ultimately to protect the continued viability of online businesses.

CRediT authorship contribution statement

Petra Saskia Bayerl: Conceptualization, Data curation, Formal analysis, Methodology, Project administration, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. **Gabriele Jacobs:** Conceptualization, Methodology, Project administration, Supervision, Writing – review & editing.

Acknowledgement

We warmly thank Max Kleyweg for his work for this research. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Appendix A. List of items

Concept	Items	Scale
Perceived contract breach	Almost all the promises made by Henry have been kept so far. (reversed) I feel that Henry has come through in fulfilling the promises made. (reversed) Henry has done an excellent job of fulfilling its promises to me. (reversed) I have not received everything promised to me in exchange for my contributions. Henry has broken many of its promises towards me even though I have upheld my side of the deal.	1: strongly disagree…5: strongly agree
Experienced violation	I feel a great deal of anger towards Henry. I feel betrayed by Henry. I feel that Henry has violated the contract between us. I feel extremely frustrated by how I have been treated by Henry.	1: strongly disagree …5: strongly agree
Continuation intentions	I intend to continue using the service rather than discontinue its use. My intentions are to continue using this service than use any alternative means. If I could, I would like to discontinue my use of this service.	1: strongly disagree…5: strongly agree
Experience with privacy invasion	How frequently have you personally been victim of what you felt as an invasion of your privacy.	1: never…5: very frequently
Media exposure to negative news about privacy events	How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet.	1: not at all…5: very much

Appendix B. Texts used for experimental manipulation

See Scenarios 1–6.


BUSINESS INSIDER TECH

Online grocery service Henry sells personal information

AP Associated Press
Mar. 14, 2016, 9:25 AM 69

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

AMSTERDAM (AP) — Recent investigations reveal that online service provider Henry sells the online grocery service's users' personal information in order to "make money". Henry uses technologies such as cookies, web beacons, e-tags and a variety of other tools to collect personal information as they track users across the service. Henry's potential ability to collect and sell personal information placed the company "squarely into the category of spyware", according to Alexander Hanff security expert and chief executive of Think Privacy.

Scenario 1. Contract breach (intentional) by first party.


BUSINESS INSIDER TECH

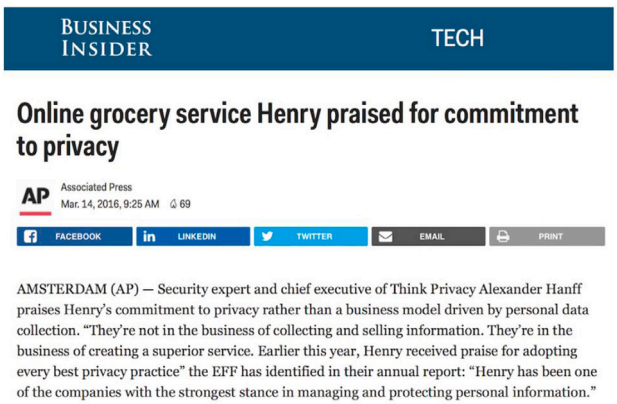
Online grocery service Henry is hacked

AP Associated Press
Mar. 14, 2016, 9:25 AM 69

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

AMSTERDAM (AP) — Henry, a service for online grocery shopping, has been hacked. An unauthorized third-party has accessed users' personal data. Despite their state-of-the art security systems and their efforts to protect their user's privacy at all cost, Henry was not able to avert this first hack attack of its kind.

Scenario 2. Contract breach (unintentional) by first party.


BUSINESS INSIDER TECH

Online grocery service Henry praised for commitment to privacy

AP Associated Press
Mar. 14, 2016, 9:25 AM 69

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

AMSTERDAM (AP) — Security expert and chief executive of Think Privacy Alexander Hanff praises Henry's commitment to privacy rather than a business model driven by personal data collection. "They're not in the business of collecting and selling information. They're in the business of creating a superior service. Earlier this year, Henry received praise for adopting every best privacy practice" the EFF has identified in their annual report: "Henry has been one of the companies with the strongest stance in managing and protecting personal information."

Scenario 3. Contract fulfilment by first party.


BUSINESS INSIDER TECH

Advertising company AdRoom accesses & sells personal information

AP Associated Press
Mar. 14, 2016, 9:25 AM 69

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

AMSTERDAM (AP) — Recent investigations reveal that advertising company AdRoom accesses and sells users' personal information from online grocery service Henry in order to "make money". AdRoom uses technologies such as cookies, web beacons, e-tags and a variety of other tools to collect personal information as they track users across the service. AdRoom's potential ability to collect and sell personal information placed the company "squarely into the category of spyware", according to Alexander Hanff security expert and chief executive of Think Privacy.

Scenario 4. Contract breach by third party.


BUSINESS INSIDER TECH

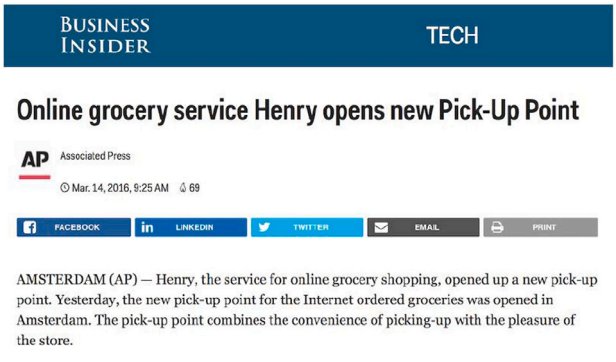
Advertising agency AdRoom praised for commitment to privacy

AP Associated Press
Mar. 14, 2016, 9:25 AM 69

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

AMSTERDAM (AP) — Security expert and chief executive of Think Privacy Alexander Hanff praises AdRoom's commitment to privacy rather than a business model driven by personal data collection. "They're not in the business of collecting and exploiting information. They're in the business of creating a superior service". Earlier this year, AdRoom received praise for adopting every best privacy practice the EFF has identified in their annual report: "AdRoom has been one of the companies with the strongest stance in respecting personal information."

Scenario 5. Contract fulfilment by third party.


BUSINESS INSIDER TECH

Online grocery service Henry opens new Pick-Up Point

AP Associated Press
Mar. 14, 2016, 9:25 AM 69

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

AMSTERDAM (AP) — Henry, the service for online grocery shopping, opened up a new pick-up point. Yesterday, the new pick-up point for the Internet ordered groceries was opened in Amsterdam. The pick-up point combines the convenience of picking-up with the pleasure of the store.

Scenario 6. Control condition.

Appendix C. Supplementary data

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.techfore.2022.122039.

References

Aguinis, H., Bradley, K., 2014. Best practice recommendations for designing and implementing experimental vignette methodology studies. Organ. Res. Methods 17 (4), 351–371.

Akter, S., Wamba, S., 2016. Big data analytics in E-commerce: A systematic review and agenda for future research. Electron. Markets 26 (2), 173–194.

Alcover, C.-M., Rico, R., Turnley, W., Bolino, M., 2016. Understanding the changing nature of psychological contracts in 21st century organizations: A multiple-foci exchange relationships approach and proposed framework. Organ. Psychol. Rev. 7 (1), 4–35.

Aslam, W., Hussain, A., Farhat, K., Arif, I., 2020. Underlying factors influencing consumers' trust and loyalty in e-commerce. Bus. Perspect. Res. 8 (2), 186–204.

Bansal, G., Zahedi, F., Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis. Support Syst. 49, 138–150.

Bansal, G., Zahedi, F., Gefen, D., 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. Eur. J. Inform. Syst. 24 (6), 624–644.

Bayerl, P.S., Fidlerova, D., Klesse, A., 2018. Changing understandings of online privacy: Profiling millennials. In: Cunnane, V., Corcoran, N. (Eds.), Proceedings of the 5th European Conference on Social Media. ECSM 2018, pp. 427–435.

BBC, 2018. Cambridge analytica: Facebook data-harvest firm to shut. BBC News online, www.bbc.co.uk/news/business-43983958.

Becker, T., 2005. Potential problems in the statistical control of variables in organizational research: A qualitative analysis with recommendations. Organ. Res. Methods 8, 274–289.

Behrend, T., Sharek, D., Meade, A., Wiebe, E., 2011. The viability of crowdsourcing for survey research. Behav. Res. 43, 800–813.

Berinsky, A., Huber, G., Lenz, G., 2012. Evaluating online labor markets for experimental research: Amazon.com's mechanical turk. Political Anal. 20 (3), 351–368.

Bhattacherjee, A., 2001. Understanding information systems continuance: An expectation-confirmation model. MIS Q. 25 (3), 351–370.

Buhrmester, M., Kwang, T., Gosling, S., 2011. Amazon's mechanical Turk: A new source of inexpensive, yet high-quality, data?Perspect. Psychol. Sci. 6 (1), 3–5.

Carre, J., Curtis, S., Jones, D., 2018. Ascribing responsibility for online security and data breaches. Manag. Audit. J. 33 (4), 436–446.

Casler, K., Bickel, L., Hackett, E., 2013. Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing. Comput. Hum. Behav. 29, 2156–2160.

Castaneda, J., Francisco, M., Luque, T., 2017. Web acceptance model (WAM): Moderating effects of user experience. Inform. Manag. 44 (4), 384–396.

Chih, W., Chiu, T., Lan, L., Fang, W., 2017. Psychological contract violation. Impact on perceived justice and behavioral intention among consumers. Int. J. Conflict Manag. 28 (1), 103–121.

Cho, C., Kang, J., Cheon, H., 2006. Online shopping hesitation. CyberPsychol. Behav. 9 (3), 262–274.

Claes, R., 2005. Organization promises in the triangular psychological contract as perceived by temporary agency workers, agencies, and client organizations. Empl. Responsib. Rights J. 17 (3), 131–142.

Conway, N., Briner, R., 2002. A daily diary study of affective responses to psychological contract breach and exceeded promises. J. Organ. Behav. 23, 287–302.

Conway, N., Guest, D., Trenberth, L., 2011. Testing the differential effects of changes in psychological contract breach and fulfillment. J. Vocat. Behav. 79 (1), 267–276.

Dawson, G., Karahanna, E., Buchholtz, A., 2014. A study of psychological contract breach spillover in multiple-agency relationships in consulting professional service firms. Organ. Sci. 25 (1), 149–170.

Dinev, T., Xu, H., Smith, J., Hart, P., 2013. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. Eur. J. Inform. Syst. 22, 295–319.

Eckerd, S., Boyer, K., Qi, Y., Eckerd, A., Hill, J., 2016. Supply chain psychological contract breach: An experimental study across national cultures. J. Supply Chain Manag. 52 (3), 68–82.

Eckerd, S., Hill, J., Boyer, K., Donohue, K., Ward, P., 2013. The relative impact of attribute, severity, and timing of psychological contract breach on behavioral and attitudinal outcomes. J. Oper. Manage. 31 (7/8), 567–578.

Eurostat, 2021. Digital economy and society statistics – households and individuals. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistic_-_households_and_individuals. (Online, Accessed 20 February 2022).

Fang, Y., Chiu, C., 2014. Exploring online double deviation effect from psychological contract violation, emotion, and power perspectives. Pacific Asia J. Assoc. Inform. Syst. 6 (1), 39–65.

Fehr, E., Fischbacher, U., 2004. Third-party punishment and social norms. Evol. Hum. Behav. 25 (2), 63–97.

Flavian, C., Guinaliu, M., 2006. Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Ind. Manag. Data Syst. 106 (5), 601–620.

Fornell, C., Larker, D., 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Mar. Res. 18 (1), 39–50.

Grappi, S., Romani, S., Bagozzi, R., 2013. Consumer response to corporate irresponsible behavior: Moral emotions and virtues. J. Bus. Res. 66, 1814–1821.

Guo, L., Gruen, T., Tang, C., 2017. Seeing relationships through the lens of psychological contracts: The structure of consumer service relationships. J. Acad. Mark. Sci. 45 (3), 357–376.

Gurumurthy, K., Kockelman, K., 2020. Modeling Americans' autonomous vehicle preferences: A focus on dynamic ride-sharing, privacy & long-distance mode choices. Technol. Forecast. Soc. Change 150, 119792.

Hayes, A., 2018. Introduction to Mediation, Moderation, and Conditional Process Analysis, second ed. Guilford, New York.

Henke, J., Joeckel, S., Dogruel, L., 2018. Processing privacy information and decision-making for smartphone apps among young German smartphone users. Behav. Inform. Technol. 37, 488–501.

Hintze, M., 2018. Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. J. Internet Law August.

Hsieh, P., 2012. Why e-return services fail: A psychological contract violation approach. Cyberpsychol. Behav. Soc. Netw. 15 (12), 655–662.

Hsu, T., 2018. For many facebook users, a 'Last Straw' that led them to quit. New York Times, https://www.nytimes.com/2018/03/21/technology/users-abandon-facebook.html.

Hsu, C., Lin, J., 2016. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. Comput. Hum. Behav. 62, 516–527.

Jai, T., Burns, L., King, N., 2013. The effect of behavioral tracking practices on consumers' shopping evaluations and repurchase intention toward trusted online retailers. Comput. Hum. Behav. 29 (3), 901–909.
Jakobsson, M., 2009. Experimenting on mechanical Turk: 5 how Tos. IT World, http://www.itworld.com/internet/76659/experimenting-mechanical-turk-5-how-tos.
Janakiraman, R., Lim, J., Rishika, R., 2018. The effect of data breach announcement on customer behavior: Evidence from a multichannel retailer. J. Marketing 82, 85–105.
Jordan, J., Hoffman, M., Bloom, P., Rand, D., 2016. Third-party punishment as a costly signal of trustworthiness. Nature 530 (7591), 473–476.
Kawaf, F., Tagg, S., 2012. Online shopping environments in fashion shopping: An SOR based review. Mark. Rev. 12 (2), 161–180.
Lapalme, M., Simard, G., Tremblay, M., 2011. The influence of psychological contract breach on temporary workers' commitment and behaviors: A multiple agency perspective. J. Bus. Psychol. 26 (3), 311–324.
Lin, T., Paragas, F., Goh, D., Bautista, J., 2016. Developing location-based mobile advertising in Singapore: A socio-technical perspective. Technol. Forecast. Soc. Change 103, 334–349.
Malhotra, N., Kim, S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Inf. Syst. Res. 15 (4), 336–355.
Malhotra, N., Sahadev, S., Purani, K., 2017. Psychological contract violation and customer intention to reuse online retailers: Exploring mediating and moderating mechanisms. J. Bus. Res. 75, 17–28.
Mamonov, S., Benbunan-Fich, R., 2015. An empirical investigation of privacy breach perceptions among smartphone application users. Comput. Hum. Behav. 49, 427–436.
Mamonov, S., Koufaris, M., 2014. The impact of perceived privacy breach on smartphone user attitudes and intention to terminate the relationship with the mobile carrier. Commun. Assoc. Inform. Syst. 34, 1157–1174.
Martin, K., Borah, A., Palmatier, R., 2017. Data privacy: Effects on customer and firm performance. J. Marketing 81 (1), 36–58.
Miyazaki, A., Fernandez, A., 2001. Consumer perceptions of privacy and security risks for online shopping. J. Consumer Affairs 35 (1), 27–44.
Newman, D., 2014. Missing data: Five practical guidelines. Organ. Res. Methods 17 (4), 372–411.
Pantlin, N., Wiseman, C., Everett, M., 2018. Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. Comput. Law Secur. Rev. 34 (4), 881–885.
Parks, J.M., Kidder, D., Gallagher, D., 1998. Fitting square pegs into round holes: Mapping the domain of contingent work arrangements onto the psychological contract. J. Organ. Behav. 19 (S1), 697–730.
Pavlou, P., Gefen, D., 2005. Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. Inf. Syst. Res. 16 (4), 331–436.
Posey, C., Raja, U., Crossler, R., Burns, A., 2017. Taking stock of organisations' protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. Eur. J. Inform. Syst. 26 (6), 585–604.
Rasoulian, S., Grégoire, Y., Legoux, R., Sénécal, S., 2021. The effects of service crises and recovery resources on market reactions: An event study analysis on data breach announcements. J. Serv. Res..
Robinson, S., 1996. Trust and breach of the psychological contract. Admin. Sci. Q. 41, 574–599.
Robinson, S., Morrison, E., 2000. The development of psychological contract breach and violation: A longitudinal study. J. Organ. Behav. 21 (5), 525–546.
Rousseau, D., 1989. New hire perceptions of their own and their employer's obligations: Study of psychological contracts. J. Organ. Behav. 11, 389–400.
Rousseau, D., 1995. Psychological Contracts in Organizations: Understanding Written and Unwritten Agreements. Sage, Newbury Park, CA.
Schumann, J., von Wangenheim, F., Groene, N., 2014. Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services. J. Mark. 78 (1), 59–75.
Sheehan, K., 2002. Toward a typology of internet users and online privacy concerns. Inform. Soc. 18 (1), 21–32.
Siponen, M., Vance, A., 2014. Guidelines for improving the contextual relevance of field surveys: The case of information security police violations. Eur. J. Inf. Syst. 23, 289–305.
Smith, H., Dinev, T., Zu, H., 2011. Information privacy research: An interdisciplinary review. MIS Q. 35 (4), 989–1015.
Toufaily, E., Ricard, L., Perrien, J., 2013. Customer loyalty to a commercial website: Descriptive meta-analysis of the empirical literature and proposal of an integrative model. J. Bus. Res. 66 (9), 1436–1447.
Tsai, J., Egelman, E., Cranor, L., Acquisti, A., 2011. The effect of online privacy information on purchasing behavior: An experimental study. Inf. Syst. Res. 22 (2), 254–268.
Weiner, B., 1985. An attributional theory of achievement motivation and emotion. Psychol. Rev. 92, 548–573.
Westin, A., 1967. Privacy and Freedom. Atheneum, New York.
Xie, C., Bagozzi, R., Gronhaug, K., 2015. The role of moral emotions and individual differences in consumer responses to corporate green and non-green actions. J. Acad. Manag. Sci. 43, 333–356.
Yin, F., Liu, M., Lin, C., 2015. Forecasting the continuance intention of social networking sites: Assessing privacy risk and usefulness of technology. Technol. Forecast. Soc. Change 99, 267–272.
Zhao, H., Wayne, S., Glibkowski, B., Bravo, J., 2007. The impact of psychological contract breach on work-related outcomes: A meta-analysis. Pers. Psychol. 60, 647–680.

Petra Saskia Bayerl is Professor for Digital Communication and Security at the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) at Sheffield Hallam University, UK.

Gabriele Jacobs is Professor of Organizational Behavior and Culture at Erasmus School of Social and Behavioral Sciences, Erasmus University Rotterdam, the Netherlands.