Reactions by actual data breach victims over time:
Evidence from Facebook's Cambridge Analytica breach

Frederic Schlackl
HEC Montreal,
Montreal H3T 2A7 Quebec, Canada frederic.schlackl@hec.ca

Florian Pethig
Department of Information Systems and Operations Management, Tilburg School of Economics and Management, Tilburg University, 5037 AB Tilburg, The Netherlands f.pethig@tilburguniversity.edu

Hartmut Hoehle
Business School, University of Mannheim,
68161 Mannheim, Germany hoehle@uni-mannheim.de

Rajiv Sabherwal
Information Systems Department, Sam M. Walton College of Business, University of Arkansas,
Fayetteville, Arkansas 72701 rsabherwal@walton.uark.edu

Abstract

Individuals react negatively to data breaches, for example, by perceiving anxiety and losing trust. Such responses are exhibited by both the actual data breach victims, whose privacy has been violated, and by individuals who may only have been potentially affected. Understanding how reactions differ across these groups can help data breach crisis management, communication, and compensation, but prior research has not examined the similarities or differences between them. Here, we exploit the publicly available breach notification of Facebook's Cambridge Analytica breach to identify effects on actual breach victims in a real-world setting. Using two waves of data collection as a quasi-natural experiment (n = 380), we find that actual breach victims show stronger initial reactions than non-victims in several outcome variables, such as continuance intention, trust, perceived psychological contract breach, feelings of violation, and online social network belongingness. These effects are heterogeneous, small, and partially independent of prior Facebook use and breach experience. In a third wave (n = 183), we find that differences between the groups disappear within six months. In a follow-up preregistered longitudinal experiment using scenarios (n = 653), we find that cognitive dissonance increases victims' post-breach attitudes, as high switching costs render leaving the platform unfeasible. However, we also find non-dissonant victims to show greater attitude regression over time, hinting at a self-perception mechanism. Our findings have implications for the literature on data breach reactions and remediation and on privacy in online social networks.

Keywords: data breach, privacy, online social network, Facebook, Cambridge Analytica

1. Introduction

Individuals react adversely to a company's data breach, showing negative emotions (Bachura et al. 2022), losing trust in the company (Bansal and Zahedi 2015), switching to competitors, or adopting more privacy-protective behaviors (Lee and Lee 2012). Prior research finds these reactions among both the general public (e.g., Bachura et al. 2022) and individuals whose data were compromised (e.g., Janakiraman et al. 2018). An individual learning about a data breach can fall into one of three distinct categories: (1) the breach could not possibly affect them (e.g., people who are not customers of the breached firm), (2) the breach could potentially affect them (e.g., customers of the breached firm), or (3) actual breach victims whose data were compromised by the breach.

Studies of real-world data breaches generally examine effects on the second group, *potential breach victims* (e.g., Goode et al. 2017; Hoehle et al. 2022), while scenario-based experiments typically focus on the third group, *actual breach victims* (e.g., Choi et al. 2016; Nikkhah and Grover 2022). Understanding how these groups differ is important. For research, it allows greater precision in theorizing and assessing the impacts of data breaches. For firms, it informs more targeted crisis communication and remedy plans. Intuitively, actual breach victims might be expected to react more strongly than potential victims, as they have genuinely experienced a privacy violation and face potential negative impacts (Pang and Vance 2025). However, strong reactions from the public (Bachura et al. 2022) and potential victims (Lee and Lee 2012) challenge this assumption, suggesting that being an actual breach victim may not be a necessary condition for adverse reactions to occur. Hence, we ask the following:

> **RQ1:** How do reactions to data breaches, in terms of changes in attitudes and behavioral intentions, differ between actual breach victims and their non-breached peers?

How individuals' reactions to data breaches change over time is also unclear. Typically, actual and potential breach victims are surveyed a few days after a breach. The few studies of long-term effects find that changes in victims' behavior are short-lived (Janakiraman et al. 2018; Agarwal et al. 2024), but the persistence of underlying attitude changes remains an open question. Do victims begrudgingly revert their behavior as their negative attitudes persist, or do their attitudes change in lockstep with their behavior? This tension has prompted calls to better understand how breach victims' perceptions evolve (Agarwal et al. 2024). Thus, we ask the following:

> **RQ2:** How persistent over time are the differences between actual breach victims and their non-breached peers in terms of their reactions to the breach?

To address the above research questions, we conducted two studies: (1) an empirical study examining the effects of Facebook's (FB) Cambridge Analytica breach notification on user reactions and (2) a longitudinal experiment investigating the underlying mechanisms driving these reactions over time. We leveraged a unique aspect of this data breach: a public website created by FB for users to check if their data had been breached. This allowed us to distinguish the effects of the breach on actual victims versus potential victims (unaffected users) using a difference-in-differences (DID) analysis. We surveyed 380 FB users before and after the breach notification became public to identify its immediate effects. To understand the effects over time, we conducted a third survey with 183 of these users six months later. To extend these results, we followed up with a longitudinal scenario-based survey experiment of 653 participants.

This article makes three contributions. First, we show that a data breach has a small-to-medium-sized effect on actual breach victims' attitudes relative to the one it has on non-victims. This nuances the current understanding of data breach effects. Second, we extend the literature on the relation between online social network (OSN) use, OSN belongingness, and privacy. We find that actual breach victims reduce their OSN belongingness irrespective of their FB use. Third, we show that beyond the effects seen in behavioral studies, the effect on attitudes is also short-lived. We find that while post-breach attitudes are shaped by cognitive dissonance, as switching costs hinder users from leaving the OSN, the observed attitude regression[1] is primarily driven by users who do not perceive cognitive dissonance, indicating a self-perception mechanism. Overall, we demonstrate the effects of a data breach on OSN users' attitudes and examine why such effects are short-lived.

2. Background

2.1. Data Breaches

A *data breach* is an incident where personal data becomes accessible to unauthorized third parties (IBM 2023), creating a privacy violation for the victims (Wright and Xie 2019). Consumers feel vulnerable when companies access their data and worse when they hear that their data has been breached (Martin et al. 2017). Consequences include loss of trust (Bansal and Zahedi 2015), negative attitudes toward the company (Wright and Xie 2019), and switching (Martin et al. 2017). Due to the prevalence of privacy violations, people often experience a sense of resignation and helplessness (Hinds et al. 2020). Such feelings, when associated with emotional exhaustion

[1] We are grateful to the senior editor for suggesting the term *attitude regression*.

and cynicism, have been dubbed *privacy fatigue* (Choi et al. 2018) and *breach fatigue* (Kwon and Johnson 2015). The extent to which this fatigue occurs and users adapt after multiple breaches is unclear. The consequences of privacy violations are often diffuse and intangible, which partly explains consumers' inaction (Acquisti et al. 2020). In breaches of financial data, many affected consumers are unlikely to ever experience identity theft or fraud. The low sensitivity of OSN data likely adds to this intangibility. While this absence of tangible economic damage causes difficulties for data breach litigation, legal scholars argue for emotional harm arising from the loss of one's data, regardless of whether it was misused (Solove and Citron 2018).

We review 21 articles on individual-level post-breach reactions and present their classification in Table 1 (coding details in Appendix A1). First, we distinguish studies by *their empirical setup* (i.e., whether they analyze a real-world data breach or use scenarios). Real-world breaches sample respondents with relevant experience, such as shopping at Target before its breach (Hoehle et al. 2022) or posting breach-related hashtags on Twitter (Bachura et al. 2022). Scenario-based studies use prompts for respondents to imagine a breach (e.g., Choi et al. 2016); their controlled nature allows for rigorous mechanism testing but may reduce ecological validity.

Table 1. Prior Literature on Post-breach Reactions and Responses

Group		Article	Context	Outcomes
Scenario-based	General public	Nofer et al. (2014)	Investment decision	Trust (−), investment (−)
		Bansal and Zahedi (2015)	Website use	Trust (−)
	Potential victims	Wright and Xie (2019)	Resp.-dependent	Attitude toward company (−)
	Actual victims	Mamonov and Koufaris (2014)	Mobile carrier	Trust (−), commitment (−), cynicism (+)
		Choi et al. (2016)	Online vendor	Justice perceptions, perceived breach, feelings of violation, WOM, switching*
		Bentley and Ma (2020)	Online vendor	Reputation, attribution of responsibility, purchase intention, WOM*
		Masuch et al. (2021)	Fitness tracker	Expectation confirmation, satisfaction, trust, loyalty, WOM*
		Nikkhah and Grover (2022)	Resp.-dependent	Expectation violation, dissatisfaction, switching behavior, WOM*
		Guo et al. (2023)	Online vendor	Anger, fear, WOM, switching*
Real-world breach	General public	Syed (2019)	Home Depot	Anger (+), disgust (+), sadness (+), fear (+)
		Bachura et al. (2022)	OPM	Anxiety, anger, sadness*
	Potential victims	Lee and Lee (2012)	Internet Auction Co	Switching (+), providing fake information (+)
		Goode et al. (2017)	Sony	Service quality, continuance intention, repurchase intention*
		Kude et al. (2017)	Target	Perceived compensation, service recovery, customer experience*
		Mikhed and Vogan (2018)	SC Dept of Revenue	Credit and fraud protection service usage (+)
		Ayaburi and Treku (2020)	Facebook	Behavioral integrity, privacy concerns, trust*
		Hoehle et al. (2021)	Home Depot	Service quality, continuance intention, repurchase intention*
		Hoehle et al. (2022)	Target	Justice perceptions, continuance intention, WOM, complaining*
	Actual victims	Janakiraman et al. (2018)	Unknown, retail	Spending (−), channel switching (+)
		Turjeman and Feinberg (2023)	Ashley Madison	Searches (−), messages (−), photo deletion (+)
		Agarwal et al. (2024)	Zomato	Digital payments (−), cash payments (+)
	This study (actual and potential victims)		Facebook	Continuance intention, trust, perceived breach, feelings of violation, OSN attitudes (anxiety, belongingness)

Notes: * Study investigates the relations between variables in a post-breach setting instead of the direct impact of the breach. + Data breach increases outcome variable. − Data breach decreases outcome variable. WOM, word of mouth; OSN, online social network; OPM, Office of Personnel Management, Resp.-dependent, respondent-dependent; SC, South Carolina.

The second dimension captures *the relationship between the studied group and the breach*. Studies of the *general public* inform respondents broadly about a breach's occurrence (e.g., Nofer et al. 2014) or sample public social media exchanges (e.g., Bachura et al. 2022). Studies of *potential breach victims* examine customers of breached companies (e.g., Target in Hoehle et al. 2022) or ask respondents to name a company they shop with and present a fictitious news article about a breach there (e.g., Wright and Xie 2019). Studies of *actual breach victims* inform respondents that their data has been breached (e.g., Choi et al. 2016) or use real-world transaction data of breached persons (e.g., Janakiraman et al. 2018). Real-world studies often use potential breach victims (7 of 12 in Table 1), as separating actual victims from potential victims is difficult. Scenario-based studies often present their subjects as actual victims (6 of 9), which is a notable difference from real-world studies. Ten articles study companies' responses (e.g., apology or compensation) to a data breach rather than the breach's direct impact. They demonstrate the effects of a company's response on outcomes such as continuance intention and trust, but the initial impact of being breached remains unclear. The reactions shown by actual breach victims include a decrease in trust, commitment, customer spending, and web activity and an increase in cynicism, content deletion, and channel switching, all of which are generally short-lived (Janakiraman et al. 2018; Turjeman and Feinberg 2023). Loss of trust and negative emotions also occur among the general public and potential breach victims (e.g., Lee and Lee 2012; Bachura et al. 2022), leaving the incremental effects on actual victims unclear.

As such, we have little knowledge of actual breach victims' attitudinal reactions. The *behavior* of actual breach victims in a real-world breach has been studied (Janakiraman et al. 2018; Turjeman and Feinberg 2023), but not the *attitudes* that precede it. Many outcomes (e.g., continuance intention, trust, and psychological responses) have only been studied for the general public or potential victims. If they differ for actual breach victims, we may need to reassess models that do not account for this. Conversely, if being an actual breach victim has no additional impact over being a potential one, firms may need to refocus their recovery efforts. We aim to close this gap by examining reactions in both attitudes and behavioral intention (see Table 1).

2.2. Privacy in Online Social Networks

Privacy is an established topic of research at the interface of economics, psychology, and information systems (IS). In general, individuals struggle to obtain their desired level of privacy online, with a stark contrast between stated preferences for privacy and observed behavior. This paradox may be explained by opaque privacy practices and biases affecting privacy decision-making (Acquisti et al. 2020; Dehling and Sunyaev 2024). Appendix A2 provides a more comprehensive review of privacy research in IS.

Privacy is also a key topic of research on OSNs, relating both to information disclosure toward other users and to users' attitudes toward OSNs and their privacy practices. While FB users have reduced their public information sharing as the OSN has matured, this has not reduced data capture by FB, its advertisers, and third-party apps (Stutzman et al. 2013). Before the Cambridge Analytica breach, triggered through a third-party app, users were generally unaware of these apps' permission and data harvesting practices (King et al. 2011). These apps allow for the harvesting of previously shared information via a user's friends, violating the user's privacy by breaching the information's contextual integrity (Hull et al. 2011). How users react to this breach of contextual integrity in an OSN environment that is already associated with latent privacy violations is unknown.

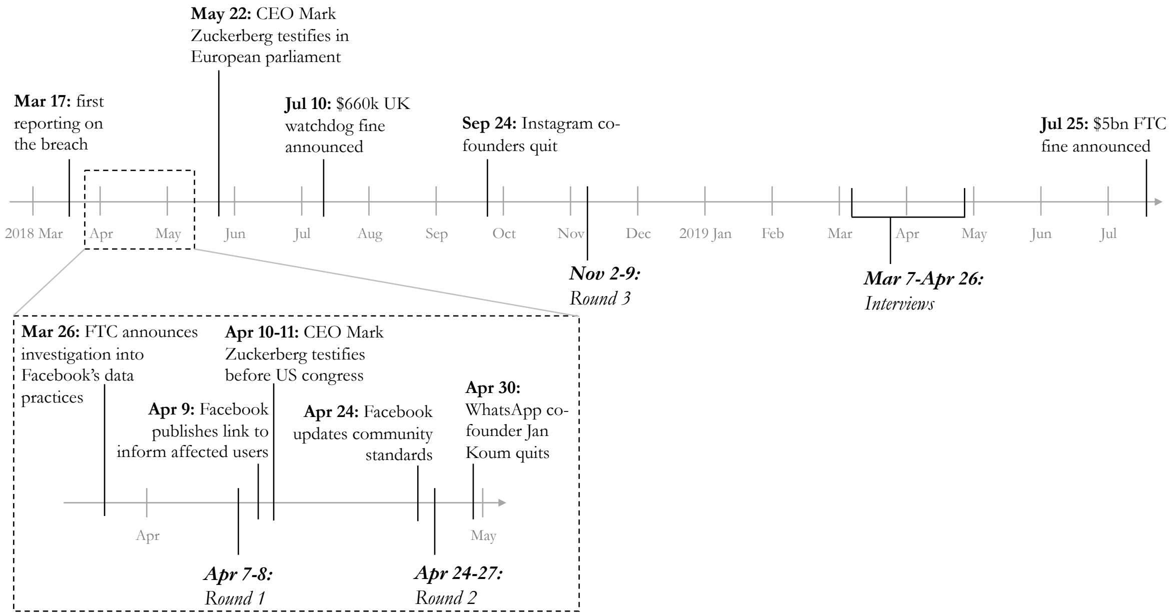
2.3. The Cambridge Analytica Breach

In 2015, researcher Aleksandr Kogan, in cooperation with the political consulting firm Cambridge Analytica, built a third-party personality quiz app for FB called *This Is Your Digital Life*. It gathered data from 270,000 FB users who logged into it, answered a survey, and provided access to their FB profile data. Clandestinely, the app also harvested the data (including usernames, profile pictures, birthdays, current cities, and page likes) of every respondent's FB friends, amassing 87 million records (Badshah 2018). From the original respondents' likes and their answers to the survey, Cambridge Analytica constructed personality profiles, which were then used for political advertising in the United States and the United Kingdom (Hern 2018).

In late 2015, FB became aware of this mass data harvesting and banned the app without notifying users. This caused a scandal in March 2018, when *The Guardian* and *The New York Times* reported on it after being contacted by a whistleblower (Cadwalladr and Graham-Harrison 2018). FB's share price fell 7% the day after the news and continued to drop for the next several months. Parliamentary and criminal investigations ensued, leading to FB being fined $5 billion by the U.S. Federal Trade Commission (Fung 2019). During the scandal, FB issued a link where all users could check if they were breached. Figure 1 shows a timeline of the scandal and our data collection. The breach's consequences for FB remain unclear. Market researchers report that FB lost

15 million users in the United States, while FB claimed continued user growth (Schroeder 2019). Empirical literature on FB users' reactions is scarce. Prior research found contradictory privacy concerns, temporarily reduced FB use, and a sense of powerlessness among users (Brown 2020; Hinds et al. 2020).

Figure 1. Timeline of the Cambridge Analytica Scandal



May 22: CEO Mark Zuckerberg testifies in European parliament
Mar 17: first reporting on the breach
Jul 10: $660k UK watchdog fine announced
Sep 24: Instagram co-founders quit
Jul 25: $5bn FTC fine announced
2018 Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
2019 Jan
Feb
Mar
Apr
May
Jun
Jul
Nov 2-9: *Round 3*
Mar 7-Apr 26: *Interviews*
Mar 26: FTC announces investigation into Facebook's data practices
Apr 10-11: CEO Mark Zuckerberg testifies before US congress
Apr 9: Facebook publishes link to inform affected users
Apr 24: Facebook updates community standards
Apr 30: WhatsApp co-founder Jan Koum quits
Apr
May
Apr 7-8: *Round 1*
Apr 24-27: *Round 2*

The Cambridge Analytica breach differs from other data breaches (see Table 2) because (a) it straddles the line between a data breach and a deliberate privacy violation, as the data were obtained from nonconsenting individuals and shared with an unauthorized party (Cambridge Analytica); (b) it was the first large-scale breach in an OSN; and (c) it spread through the OSN, causing users to inadvertently breach their FB friends.

Table 2. The Cambridge Analytica Breach Compared to Other Large Data Breaches

Breach	Year	Records breached	Type of data	Cause	Company reaction
Sony	2011	77 million PSN users	Account data	Hacker targeting web app server	Compensation, apology
Target	2013	110 million shoppers	Credit card data	Hacker targeting POS terminals	Compensation, apology
Yahoo	2016	3 billion accounts	Account data, passwords	Hacker using login cookies	Concealment, apology
Uber	2017	57 million Uber users	Account data	Hacker using credential stuffing	Concealment, apology
Equifax	2017	149 million	PII, SSN numbers	Hacker targeting web app server	Compensation, apology
Marriott	2018	383 million guests	Payment data	Hacker using remote access trojan	Compensation, apology
Facebook	2018	87 million FB users	OSN data	Abuse of permissive app accesses	Concealment, apology

Notes. Year refers to the year disclosed. Compensation excludes legal settlements. PSN, PlayStation Network; POS, point of sale; PII, personally identifiable information; SSN, social security number; OSN, online social network.

3. Outcomes of Interest

Based on prior literature on data breach victims' reactions, we examine the effects on six outcomes (see Table 3). Trust and continuance intention are two common outcome variables in studies of data breach victims (see

Table 1) and post-breach responses (Goode et al. 2017; Hoehle et al. 2022). However, only scenario-based studies examine trust (Nofer et al. 2014; Bansal and Zahedi 2015), while the impacts of a data breach on victims' and non-victims' continuance intention have not been studied. Because of breached companies' concerns about worsened customer relationships (Hoehle et al. 2022), investigating differences in potential and actual breach victims' trust and continuance intention is important. The second set of outcome variables—feelings of violation and perceived breach—is used in studies viewing data breaches as a psychological contract breach (PCB) (Choi et al. 2016; Wright and Xie 2019). Perceived breach refers to the perception of a PCB (i.e., the cognitive response to it), while feelings of violation refer to affective responses, including frustration, hostility, and anger. A data breach plausibly violates the psychological contract between an individual and the company responsible for their data, but this has only been tested in scenario-based studies. The extent to which it translates to real-world settings is unclear. Moreover, the extent to which an individual may perceive a PCB arising from being a potential breach victim, as opposed to only when their data is actually stolen, is also unclear.

Table 3. Outcomes of Interest

Construct category	**Construct**	**References**
Outcomes established for potential breach victims	Continuance intention	Goode et al. (2017); Hoehle et al. (2022)
	Trust	Nofer et al. (2014); Bansal and Zahedi (2015)
Outcomes established in scenario-based studies	Perceived breach	Choi et al. (2016)
	Feelings of violation	Choi et al. (2016)
OSN-specific outcomes	OSN belongingness	Grieve et al. (2013); James et al. (2017)
	OSN anxiety	James et al. (2017)

Note. OSN, online social network.

FB's Cambridge Analytica breach is not a traditional data breach affecting customers' financial data but an OSN breach affecting users' profile data. Thus, we also investigate two OSN-related outcome variables: OSN belongingness, defined as "feelings of social connectedness to others on an OSN" (James et al. 2017, p. 565), and OSN anxiety, which is a negative emotional response to OSN use, reflecting worry and stress. Since OSN data breaches have not yet been studied, their effects on user perceptions of the OSN are unclear. An increase in OSN anxiety signals an increase in negative feelings about FB use, and a decrease in OSN belongingness signals reduced pleasure from FB use. Whether loss of profile data affects user perceptions of social interactions on FB is unclear. Being a breach victim may lead to negative associations with the OSN, especially for users breached by a friend. Alternatively, breached users may hold negative feelings solely against FB, the company, and be unaffected in their feelings toward FB, the OSN. Thus, we examine the effects on six outcomes from prior literature: continuance intention, three broader attitudes, and OSN-related attitudes.

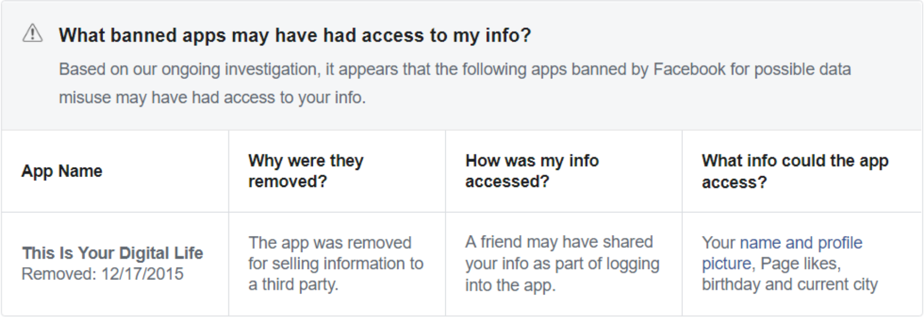
4. Methodology

To address RQ1, we conducted Study 1, a two-wave longitudinal survey leveraging a quasi-natural experiment on the effects of the Cambridge Analytica breach on actual breach victims. To address RQ2, we extended Study 1 by incorporating a third survey six months after the breach notification. To further validate the results from Study 1 and investigate the underlying mechanisms, we conducted Study 2, a longitudinal scenario experiment where we observed users' reactions to a breach notification at a fictitious OSN called *SocialNet*.

4.1. Data Collection (Study 1, Rounds 1 and 2)

In Study 1, we used Amazon Mechanical Turk (MTurk) to recruit U.S. residents who had completed at least 50 tasks with an approval rating of 90% or higher. The first survey occurred on April 7 and 8, 2018, after FB announced that it would notify users affected by the breach but before it began notifying them on April 9. The second survey was carried out after users were informed, from April 24 to 27. A push notification at the top of users' newsfeeds linked to a page stating whether they were affected by the breach (Figure 2). Through this website, all users switched from being potentially affected to being actual breach victims or non-victims.

Figure 2. Excerpt from the Facebook Breach Notification Page



⚠ **What banned apps may have had access to my info?**

Based on our ongoing investigation, it appears that the following apps banned by Facebook for possible data misuse may have had access to your info.

App Name	Why were they removed?	How was my info accessed?	What info could the app access?
This Is Your Digital Life Removed: 12/17/2015	The app was removed for selling information to a third party.	A friend may have shared your info as part of logging into the app.	Your name and profile picture, Page likes, birthday and current city

In the first survey, we recruited 580 participants, 538 of whom stated that they had an FB account and thus could potentially be affected. The survey was completed by 530 of them. We removed 29 individuals who did not correctly answer all three attention checks[2] and 6 who did not provide a correct completion code on MTurk, leading to a sample of 495 individuals to whom the second survey was provided. Among the 396 who responded, we removed 12 individuals who did not correctly answer all three attention checks and 4 who did not provide a

[2] The wording of the attention checks was based on James et al. (2017). In line with Lowry et al. (2016), we implemented additional measures to ensure the validity of online panels (Appendix B1).

correct completion code on MTurk. The remaining 380 participants were asked to visit the breach notification page[3] at the start of the second survey and confirm their breach status. They were aware of their breach status as they answered the second survey. Combining the data from both treated (i.e., breached) and non-treated (i.e., non-breached) users across the prenotification and post-notification periods allowed for a DID analysis.

To measure the outcomes, we adapted established scales, including survey items using seven-point Likert scales, from the literature (see Appendix B2). We controlled for age, gender, prior breach experience (Martin et al. 2017), and intensity of pre-period FB use—specifically, pre-period FB use frequency, hours on FB, and number of FB friends (James et al. 2017), as they might affect reactions. Following OSN research (James et al. 2017), we controlled for the Big Five personality traits (John et al. 1991) in robustness tests.

4.2. Sample Characteristics

Tables 4 and 5 provide the descriptive statistics. The final sample of 380 respondents included 49% men and 51% women. As for their ages, 19% of them were 29 or younger, 42% were 30–39, 17% were 40–49, 15% were 50–59, and 7% were 60 or older. 207 respondents had experienced prior data breaches, and 173 had not. While 104 were actual victims of the Cambridge Analytica breach, 276 were not. To ensure that our sample was representative of the wider population of U.S. FB users, we calculated the sample size required to correctly estimate the proportion of breached users. As 31.5% of U.S. FB users were affected by the breach,[4] the sample size required to obtain a 5% margin of error at a 95% confidence level was n = 332 (computed per Cochran 1977), which was below our sample of n = 380. The proportion of breached users in our sample was 27.4%, which was within 5% of the population ratio. We also performed a power analysis to assess the adequacy of the sample for detecting effects. For an error probability (α) of 0.05 and a medium effect size (f^2) of 0.15 (commonly used default values, e.g., Cohen [1988]), the sample of 380 respondents achieved a power of over 0.99. The sample was sufficiently powered to detect f^2 above 0.04 at a power of 0.80. Scale reliability (Cronbach's alpha) exceeded 0.70 for all measures. Appendix B3 provides the correlations. We used t-tests to determine whether attrition was of concern in our sample (Ployhart and Vandenberg 2010). The results in Appendix B4 show that the respondents who dropped out did not significantly differ from those who remained in the post-period.

[3] See https://www.facebook.com/help/1873665312923476 (accessed July 23, 2025).

[4] Seventy million U.S. users were affected (Badshah 2018), out of 222 million U.S. Facebook users in total (Statista 2023).

Table 4. Facebook Use Statistics (Study 1)

Number of Facebook friends		**Frequency on Facebook**		**Hours per day on Facebook**	
1–29	36	Less than once a week	25	<1 hour	175
30–99	70	Less than once a day	51	1–2 hours	132
100–299	141	Once a day	70	3–4 hours	49
300–499	70	2–5 times a day	137	5–6 hours	17
500–1,000	44	6 or more times a day	97	7–8 hours	5
>1,000	19			8–9 hours	0
				≥10 hours	2

Notes. All values are in the pre-period. Items from James et al. (2017).

Table 5. Descriptive Statistics (Study 1)

Variable	**Pre**			**Post**			**Difference (Pre vs. Post)**		
	α	Mean	SD	α	Mean	SD	b	t	p
Continuance intention	0.98	4.75	1.72	0.98	4.79	1.83	–0.04	(–0.29)	0.77
Trust	0.86	3.64	1.34	0.88	3.59	1.44	0.05	(0.48)	0.63
Perceived breach	0.92	4.66	1.61	0.92	4.36	1.78	0.30*	(2.45)	0.01
Feelings of violation	0.91	3.70	1.76	0.90	3.39	1.88	0.31*	(2.31)	0.02
OSN belongingness	0.94	4.38	1.35	0.95	4.37	1.37	0.01	(0.14)	0.89
OSN anxiety	0.84	3.49	1.67	0.89	3.62	1.81	–0.13	(–1.06)	0.29

Notes. *n* = 380 for both pre- and post-breach samples. The descriptives (means and standard deviation [SD]) of age (3.48, 1.17), gender (1.51, 0.50), prior breach (1.46, 0.50), FB friends (3.19, 1.28), FB frequency (3.61, 1.19), and FB hours (1.82, 0.99) are not reported here, as they were only measured in the pre-survey. All these variables are individual single-item measures, so their reliabilities (α) cannot be computed. α, inter-item reliability; OSN, online social network; FB, Facebook.
* p < 0.05; ** p < 0.01; *** p < 0.001.

Figure 3 displays the means and 95% confidence intervals for breach victims and non-victims in the pre- and post-periods. For trust, continuance intention, and OSN belongingness, the victims' post-period means decrease between 2.9% and 6.1%. For perceived breach and violation, the victims' means are nearly unchanged, whereas the non-victims' means drop by 9.9% and 11.4%, respectively. This could indicate that the scandal around the data breach was already salient in the pre-period, increasing perceived breach and violation. During the two weeks between our survey rounds, the breach may have become less salient, with saliency rising again for the victims after they realized that they had been breached.

5. RQ1: Attitude Changes of Actual Breach Victims (Study 1)

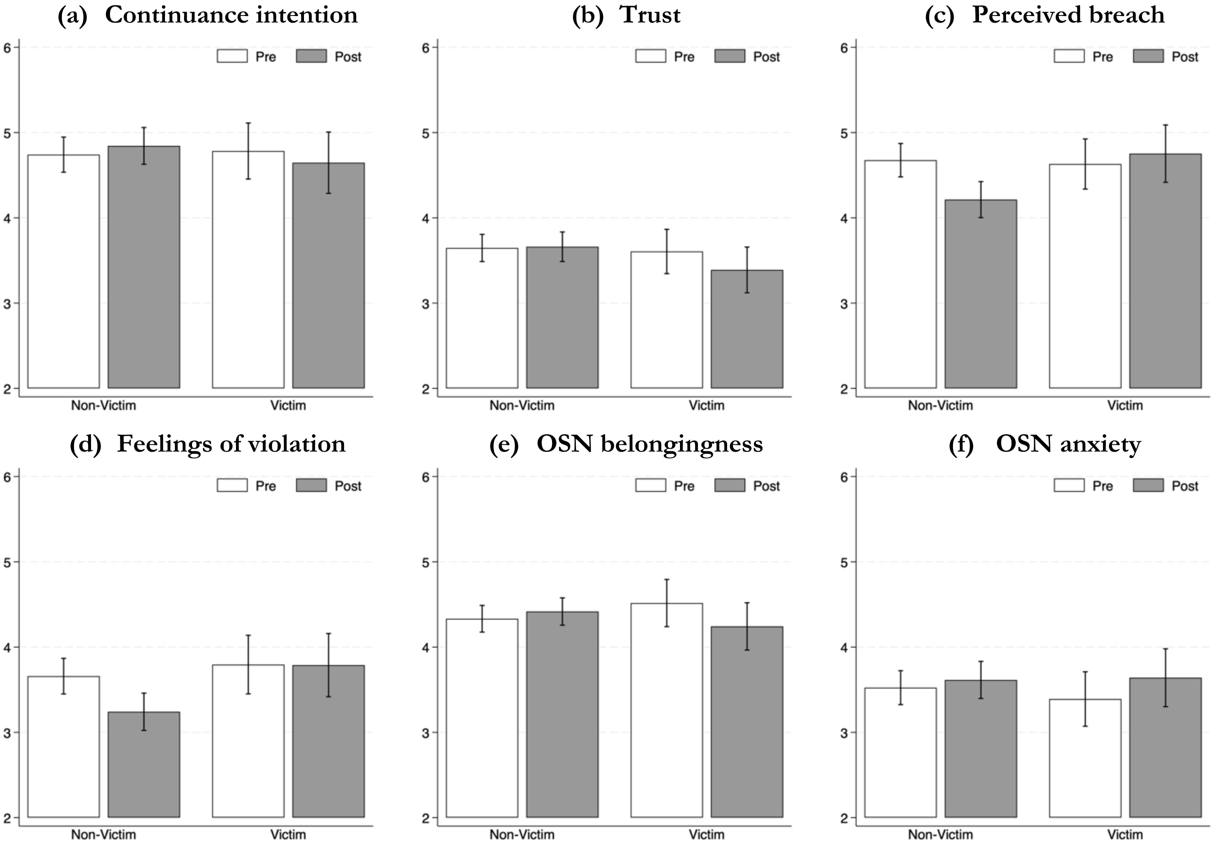
5.1. Analysis and Results

We use ordinary least squares (OLS), with robust standard errors clustered on the respondent level, to estimate our results and a canonical DID model to assess the effects of receiving the breach notification:

$$y_{it} = \beta_0 + \beta_1 Post_t + \beta_2 Victim_i + \beta_3 (Post_t \times Victim_i) + \gamma_1 X_i \qquad (1)$$

Here, *y* variously denotes each outcome variable for respondent *i* at time *t*. *Post* is the time dummy, equaling 1 in the second survey. *Victim* is the treatment dummy, equaling 1 for actual breach victims. *Post* × *Victim* is the DID term (i.e., the marginal effect of being an actual breach victim after receiving the notification).

Figure 3. The Six Outcome Variables Before and After the Breach Notification (Study 1)



(a) Continuance intention **(b) Trust** **(c) Perceived breach**

(d) Feelings of violation **(e) OSN belongingness** **(f) OSN anxiety**

X is individual respondent characteristics (fixed at the pre-period). Table 6 shows the results. The odd columns present the baseline specification, regressing the outcome variables on *Victim*, *Post,* and the DID term. Relative to their peers who heard about the Cambridge Analytica breach but were not victimized, breach victims show significantly different changes in all outcome variables, except OSN anxiety. The even-column results, which add control variables, are consistent. Actual breach victims show greater post-period increases in perceived PCB ($p < 0.001$) and feelings of violation ($p = 0.003$) and greater decreases in continuance intention ($p = 0.03$), trust ($p = 0.03$), and OSN belongingness ($p = 0.002$). The last row in Table 6 presents the standardized effect sizes (Cohen's *d*). The results show smaller effect sizes than in scenario-based studies, suggesting that real-world breaches induce more subtle reactions (Appendix B5).

The period indicator *Post* has negative effects on feelings of violation ($p < 0.001$) and perceived breach ($p < 0.001$). These results are consistent with the descriptive statistics showing a decline in perceived breach and feelings of violation from pre- to post-period, suggesting the incident became less salient.

Furthermore, *Victim* is associated with increased feelings of violation (p = 0.04) and decreased trust (p = 0.02) and continuance intention (p = 0.03). These effects, absent in the baseline models without control variables, may be attributed to correlations between the FB use variables and *Victim*. Because the victims were exposed to the Cambridge Analytica breach via their FB friends, pretreatment differences in FB use exist between victims and non-victims. We explore this further in the next section.

5.2. Validation and Robustness

5.2.1. Pretreatment Differences

The key identifying assumption of a DID model is common trends for the treatment and control groups. Since we cannot establish parallel trends with only two survey rounds, we rely on descriptive similarity. Because the data breach happened to friends of the *This Is Your Digital Life* survey respondents, treatment assignment is likely not entirely random. A single survey-taking friend was sufficient for an FB user to be breached, putting users with more friends at higher risk. Thus, actual breach victims should have, on average, more friends than non-victims do. Because of the association of the number of friends with other variables (Appendix B3), victims and non-victims may differ across more variables.

To examine what affects victim status, we regress *Victim* on all pre-period variables in a logistic regression and OLS (Table 7). In a second model, we also include the Big Five personality traits, which Cambridge Analytica used for targeting (Hern 2018). As predicted, the number of FB friends is the most significant factor in both models. Across all models, the number of FB friends is by far the most significant factor for being breached. In OLS, it is the only significant variable. The coefficients indicate that a move toward the next-highest friend category (e.g., from 100–299 to 300–499) increases the chance of being a victim by 7%.

5.2.2. Matching

We further reduce possible bias via matching. In the first configuration, we construct sampling weights by matching victims to non-victims using their number of FB friends in the pre-period. In a second configuration, we match using the number of FB friends, FB use frequency, and gender.[5] We use weighted regression based on the matching covariates. Appendix B6 presents the results, which parallel those for the unmatched sample.

[5] Since our variables are categorical, they are insufficiently granular to use k2k matching of victims to non-victims. For each victim, multiple non-victims with the same category value of FB friends exist. Instead, we calculate weights using the *cem* package in Stata.

Table 6. Effects of Being an Actual Data Breach Victim (Study 1)

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post	0.10†	0.10†	0.01	0.01	−0.46***	−0.46***	−0.42***	−0.42***	0.08	0.08	0.09	0.09
	(0.06)	(0.06)	(0.06)	(0.06)	(0.08)	(0.08)	(0.08)	(0.08)	(0.06)	(0.06)	(0.06)	(0.06)
Victim	0.04	−0.38*	−0.04	−0.36*	−0.04	0.26	0.14	0.41*	0.18	−0.09	−0.13	0.16
	(0.20)	(0.17)	(0.15)	(0.14)	(0.18)	(0.17)	(0.20)	(0.19)	(0.16)	(0.16)	(0.19)	(0.19)
Victim × Post	−0.24*	−0.24*	−0.23*	−0.23*	0.58***	0.58***	0.41**	0.41**	−0.36**	−0.36**	0.16	0.16
	(0.11)	(0.11)	(0.10)	(0.10)	(0.16)	(0.16)	(0.14)	(0.14)	(0.12)	(0.12)	(0.13)	(0.13)
Age		0.10		0.09		0.02		−0.19*		0.13*		-0.11
		(0.07)		(0.06)		(0.07)		(0.08)		(0.05)		(0.07)
Gender		−0.04		−0.09		0.02		−0.12		−0.12		0.28
		(0.17)		(0.13)		(0.16)		(0.19)		(0.13)		(0.17)
Prior breach		0.16		0.30*		−0.28†		−0.33†		0.06		−0.31†
		(0.16)		(0.13)		(0.15)		(0.17)		(0.12)		(0.16)
FB friends		0.09		0.18**		−0.15*		−0.10		0.11*		−0.13†
		(0.07)		(0.05)		(0.07)		(0.08)		(0.06)		(0.08)
FB frequency		0.57***		0.21**		−0.22*		−0.29**		0.31***		−0.44***
		(0.09)		(0.07)		(0.09)		(0.10)		(0.07)		(0.09)
FB hours		0.18*		0.25**		−0.23*		−0.11		0.16†		−0.05
		(0.08)		(0.07)		(0.09)		(0.10)		(0.09)		(0.09)
Constant	4.74***	1.65***	3.65***	1.33***	4.68***	6.61***	3.66***	6.46***	4.33***	2.31***	3.52***	5.96***
	(0.10)	(0.50)	(0.08)	(0.39)	(0.10)	(0.47)	(0.11)	(0.52)	(0.08)	(0.38)	(0.10)	(0.50)
N	760	760	760	760	760	760	760	760	760	760	760	760
R^2	0.001	0.222	0.004	0.170	0.018	0.122	0.016	0.106	0.003	0.151	0.002	0.133
Cohen's *d*	−0.14		−0.17		0.36		0.23		−0.27		0.10	

Notes. Post is a dummy variable for the second survey round, and *Victim* is a dummy variable for individuals who stated that they were breached in the Cambridge Analytica breach in the second data collection round. Robust standard errors clustered by respondent are in parentheses. We explain the calculation of the effect size (Cohen's *d*) in Online Appendix H. We interpret the effect sizes of 0.15, 0.36, and 0.65 as small, medium, and large, respectively (Lovakov and Agadullina 2021). Based on these thresholds, we interpret one effect size as medium (perceived breach), three as small (trust, violation, and OSN belongingness), and two as very small (continuance intention and OSN anxiety). OSN, online social network; FB, Facebook; Base, baseline specification; Ctrl, control variables.

† $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Table 7. Variables Influencing Victimization by the Data Breach (Study 1)

	Logit				OLS			
	β	SE	β	SE	β	SE	β	SE
OSN anxiety	−0.13	(0.13)	−0.14	(0.13)	−0.02	(0.02)	−0.02	(0.02)
OSN belongingness	0.01	(0.13)	0.02	(0.14)	−0.00	(0.02)	0.00	(0.02)
Feelings of violation	0.15	(0.14)	0.16	(0.14)	0.03	(0.02)	0.03	(0.03)
Perceived breach	−0.08	(0.14)	−0.07	(0.14)	−0.01	(0.02)	−0.01	(0.02)
Trust	−0.18	(0.16)	−0.19	(0.16)	−0.03	(0.03)	−0.03	(0.03)
Continuance intention	−0.09	(0.12)	−0.09	(0.13)	−0.01	(0.02)	−0.01	(0.02)
Age	0.11	(0.11)	0.10	(0.12)	0.02	(0.02)	0.02	(0.02)
Gender	0.45†	(0.26)	0.42	(0.28)	0.08	(0.05)	0.07	(0.05)
Prior breach	0.09	(0.25)	0.08	(0.25)	0.02	(0.04)	0.02	(0.05)
FB friends	0.39***	(0.12)	0.38**	(0.12)	0.07***	(0.02)	0.07**	(0.02)
FB frequency	0.26*	(0.14)	0.25†	(0.14)	0.04	(0.02)	0.03	(0.02)
FB hours	0.12	(0.15)	0.13	(0.15)	0.03	(0.03)	0.03	(0.03)
Openness			−0.26	(0.18)			−0.04	(0.03)
Conscientiousness			0.01	(0.24)			−0.01	(0.04)
Extraversion			0.14	(0.14)			0.02	(0.03)
Agreeableness			−0.06	(0.22)			−0.01	(0.04)
Neuroticism			0.04	(0.18)			0.00	(0.03)
Constant	−3.35**	(1.42)	−2.64	(1.96)	−0.10	(0.24)	0.06	(0.33)
R^2					0.095		0.101	

Notes. n = 380 in all models. β, regression coefficient; SE, robust standard errors shown in parentheses; OSN, online social network; FB, Facebook.
† $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

5.2.3. Self-Selection Among Breached Users

As described above, the Cambridge Analytica breach has two types of victims: a small group of people who logged into the app themselves and a larger group breached via a friend. As the first group technically consented to share their data with the app, we repeat our main model with only the respondents who were breached through friends (77 breach victims). In this model, the effect on continuance intention disappears, while the other effects are consistent. This indicates that users who had logged into the app themselves primarily drive the decrease in continuance intention. Appendix B7 presents these results.

5.3. Heterogeneity Analysis

Next, to understand the role of the OSN and breach contexts, we examine how two individual attributes related to the OSN and the breach—FB use intensity and prior breach experience—affect reactions to the breach.

5.3.1. Low vs. High-intensity Users

We split the FB use intensity variables according to the pre-period median.[6] High-intensity users may be more emotionally invested in FB, which may trigger stronger responses. By contrast, low-intensity users may not

[6] For brevity, we only show the split analysis for FB hours. The consistent FB frequency table can be found in Appendix B8.

sufficiently care about FB and their data to show any meaningful reaction. The results of the split sample analysis (Table 8, Panel A) only partially support this intuition. High-intensity users exhibit a decrease in continuance intention and trust, but low-intensity users do not. However, for perceived breach, violation, and OSN belongingness, both high and low-intensity users show reactions to being breached. Thus, the shock of learning that one's data has been breached appears to be mostly independent of the extent of previous FB use.

5.3.2. Prior Breach Experience

Repeated data breaches can cause breach fatigue, suggesting that prior breach experience may reduce users' concerns about subsequent incidents (Kwon and Johnson 2015; Choi et al. 2018). This is particularly relevant in the OSN context, as the data breached by Cambridge Analytica were relatively non-sensitive. Panel B in Table 8 shows the models for users with and without prior breach experience. For all attitudes (except OSN anxiety, which shows no consistent difference between actual and potential victims), previously breached users show similar or stronger reactions than previously non-breached users. This indicates that privacy and breach fatigue do not reduce users' reactions to being breached; FB users are not accustomed to privacy violations. The negative effect on attitudes seems to be somewhat universal. However, only users without prior breach experience show a decrease in continuance intention. This implies that previously breached users may have reconciled with data breaches with respect to their FB use, are unlikely to stop using FB, and correctly self-assess this.

Table 8. Heterogeneity of Effects across Facebook Use and Prior Breach Experience (Study 1)

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	Panel A: Number of hours on Facebook											
	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Victim × Post	−0.15	−0.29†	−0.16	−0.30*	0.62*	0.57*	0.40*	0.41*	−0.36†	−0.35*	0.30	0.06
	(0.17)	(0.15)	(0.15)	(0.14)	(0.24)	(0.22)	(0.20)	(0.19)	(0.21)	(0.14)	(0.22)	(0.16)
N	350	410	350	410	350	410	350	410	350	410	350	410
R^2	0.199	0.111	0.084	0.145	0.094	0.109	0.109	0.085	0.145	0.073	0.170	0.066
	Panel B: Prior breach experience											
	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Victim × Post	−0.30*	−0.17	−0.21	−0.26†	0.46*	0.73**	0.35†	0.48*	−0.41*	−0.30†	0.26	0.04
	(0.14)	(0.18)	(0.14)	(0.15)	(0.21)	(0.26)	(0.18)	(0.21)	(0.17)	(0.16)	(0.17)	(0.18)
N	414	346	414	346	414	346	414	346	414	346	414	346
R^2	0.280	0.196	0.187	0.153	0.166	0.092	0.107	0.116	0.193	0.169	0.149	0.169

Notes. Post is a dummy variable for the second survey round, and *Victim* is a dummy variable for individuals breached in the Cambridge Analytica breach in the second survey round. Robust standard errors clustered by respondent are in parentheses. Regressions include terms for *Victim*, *Post*, *Age*, *Gender*, *Prior breach*, *FB friends*, *FB frequency*, and *FB hours*. Control variables and constants are omitted for brevity. OSN, online social network; FB, Facebook.

† $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

6. RQ2: Evolution of Effects Over Time (Studies 1 and 2)

6.1. Extended Data Collection (Study 1, Round 3)

To answer RQ2, we extended Study 1 by conducting a third survey with the same participants from rounds 1 and 2 approximately six months after the breach notification (November 2 to 9, 2018). We obtained 194 responses, with 183 participants correctly answering all three attention checks (131 non-victims and 52 victims). To create a balanced panel, we included only these 183 participants who completed all three survey rounds. The measurement invariance of our instruments across waves was confirmed, as detailed in Appendix B9. Appendix B10 shows that the retained sample was sufficiently powered to detect medium-to-small effects.

6.2. Extended Analysis and Results

Next, we introduce *Post_6mo*, a dummy variable for the third survey responses, and interact it with *Victim:*

$$Y_{it} = \beta_0 + \beta_1 Victim_i + \beta_2 Post_t + \beta_2 Post\_6mo_t + \beta_3 (Victim_i \times Post_t) + \beta_4 (Victim_i \times Post\_6mo_t) + \gamma_1 X_i \quad (2)$$

where *Victim* × *Post_6mo* represents the breach victim effect six months post-notification. Table 9 provides two important findings. First, the results align with Table 6, suggesting broadly consistent results for the subsample that responded in all three periods. Second, *Victim* × *Post_6mo* is not consistently significant for continuance intention and all five attitudes (continuance intention: $p = 0.07$, trust: $p = 0.49$, perceived breach: $p = 0.19$, violation: $p = 0.62$, OSN belongingness: $p = 0.99$, and OSN anxiety: $p = 0.71$). This implies attitude regression, meaning the effects of being an actual breach victim fade within a few months. The results replicate when specified using a growth curve model (Appendix B11).

The results indicate that negative changes in FB users' attitudes and continuance intention after being breached are ephemeral. These results are in line with those of data breach victims' behavior changes. If users revert to pre-breach behavior but maintain negative attitudes, this implies that they only begrudgingly continue using the service, perhaps because of a lack of alternatives. Our results, however, indicate that users' attitudes also regress to the pre-breach mean. As maintaining negative attitudes is easier than sustaining behavior changes, the marketing literature often finds prolonged negative attitude changes after service failures (e.g., Grégoire et al. 2009), leading to the question of why attitudes regress here.

Table 9. Effect of Being an Actual Data Breach Victim in the Third Survey Round (Study 1)

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl	Base	Base + Ctrl
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post	0.06	0.06	0.03	0.03	−0.48***	−0.48***	−0.42***	−0.42***	0.06	0.06	0.07	0.07
	(0.08)	(0.08)	(0.08)	(0.08)	(0.11)	(0.11)	(0.10)	(0.11)	(0.08)	(0.08)	(0.10)	(0.10)
Post_6mo	−0.08	−0.08	−0.10	−0.10	−0.54***	−0.54***	−0.32**	−0.32**	−0.11	−0.11	0.17†	0.17†
	(0.10)	(0.10)	(0.08)	(0.09)	(0.12)	(0.12)	(0.11)	(0.11)	(0.09)	(0.09)	(0.10)	(0.10)
Victim	−0.30	−0.58*	−0.23	−0.50*	0.29	0.55*	0.35	0.56*	0.02	−0.20	0.22	0.41
	(0.28)	(0.26)	(0.20)	(0.19)	(0.24)	(0.23)	(0.28)	(0.27)	(0.22)	(0.22)	(0.25)	(0.25)
Victim × Post	−0.28†	−0.28†	−0.29*	−0.29*	0.58*	0.58*	0.48*	0.48*	−0.48**	−0.48**	0.08	0.08
	(0.15)	(0.15)	(0.14)	(0.14)	(0.24)	(0.24)	(0.19)	(0.19)	(0.16)	(0.16)	(0.18)	(0.18)
Victim × Post_6mo	0.36†	0.36†	0.11	0.11	0.31	0.31	0.10	0.10	−0.00	−0.00	−0.08	−0.08
	(0.19)	(0.20)	(0.16)	(0.16)	(0.24)	(0.24)	(0.19)	(0.20)	(0.17)	(0.17)	(0.21)	(0.21)
N	549	549	549	549	549	549	549	549	549	549	549	549
R^2	0.009	0.231	0.013	0.193	0.037	0.189	0.026	0.133	0.009	0.158	0.005	0.120

Notes. Post is a dummy variable for the second survey round, *Post_6mo* is a dummy variable for the third survey round, and *Victim* is a dummy variable for individuals who stated that they were breached in the Cambridge Analytica breach in the second survey round. Robust standard errors clustered by respondent are in parentheses. Control variables and constants are omitted for brevity. OSN, online social network; FB, Facebook; Base, baseline specification; Ctrl, control variables.

† $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

6.3. Exploration of the Underlying Mechanism (Study 2)

The mechanism behind the attitude regression can be explained by two prominent theories of attitude change: cognitive dissonance and self-perception. Cognitive dissonance theory posits that people experience discomfort when their attitudes and behavior are inconsistent, and they seek to reduce this dissonance by changing either their attitudes or their behavior (Festinger 1957). After the data breach, many users continued to use FB because of status quo inertia: Leaving would incur transition costs (e.g., convincing friends to move to another platform), uncertainty about future interactions, and involve the effort to make an active choice. Indeed, prior work shows that users remained on FB after the breach despite initial negative feelings (Brown 2020). This situation—continuing to use FB while disliking it—constitutes "counter-attitudinal behavior" (Harmon-Jones and Mills 1999, p. 9), which triggers dissonance. Since abandoning FB is costly, users are more likely to reduce dissonance by reducing their negative attitudes and downplaying the breach's significance, which leads to attitude regression.

Self-perception theory offers a different route to the same outcome. The theory holds that when people lack strong preexisting attitudes or situational pressures, they infer their attitudes by observing their own behavior (Bem 1972). After learning that they were breached, FB users may have initially formed negative attitudes. However, because status quo inertia kept them on FB, their behavior did not change. Observing themselves continuing to use the platform, they may have gradually concluded that their negative attitudes were weaker than they first thought. This inference process was especially likely when users' attitudes toward FB were not strongly held in the first place (Haddock and Maio, 2008).

Either of these two pathways—dissonance reduction or self-perception— offers plausible explanations for why attitudes regressed after the data breach. To explore which mechanism better accounts for this regression, we conducted Study 2.

6.3.1. Data Collection

Study 1 provided compelling evidence that continuance intention and attitudes regress over time following a data breach. However, the quasi-natural experimental setting limited our ability to isolate the underlying mechanisms. Specifically, the observed attitude regression could stem from either cognitive dissonance, where individuals adjust their attitudes to reduce discomfort from conflicting cognitions when behavior is constrained, or self-perception, where they infer their attitudes from their sustained behavior over time.

To test and distinguish between these competing theoretical explanations and to further validate the temporal effects observed in Study 1, we conducted Study 2: a preregistered,[7] scenario-based longitudinal experiment with two manipulations. To test whether cognitive dissonance led to attitude regression, we manipulated lock-in (high lock-in versus low lock-in conditions). Lock-in poses a significant barrier to leaving a platform, creating conflict between negative attitudes and continued use that triggers dissonance. If highly locked-in individuals adjust their attitudes more over time than those not locked-in, this supports cognitive dissonance as the mechanism. If attitudes regress irrespective of lock-in simply because enough time has passed for individuals to observe their actions and update their beliefs, this indicates non-dissonant self-perception. We used the passage of time (first versus second round) to measure attitude regression. We further manipulated the second round's timing (proximal versus distal condition) to assess how quickly attitude regression occurred. Our longitudinal design followed best practices in survey research, which shows that attitudes measured at multiple points in time are often more precise than cross-sectional designs (Clifford et al. 2021).

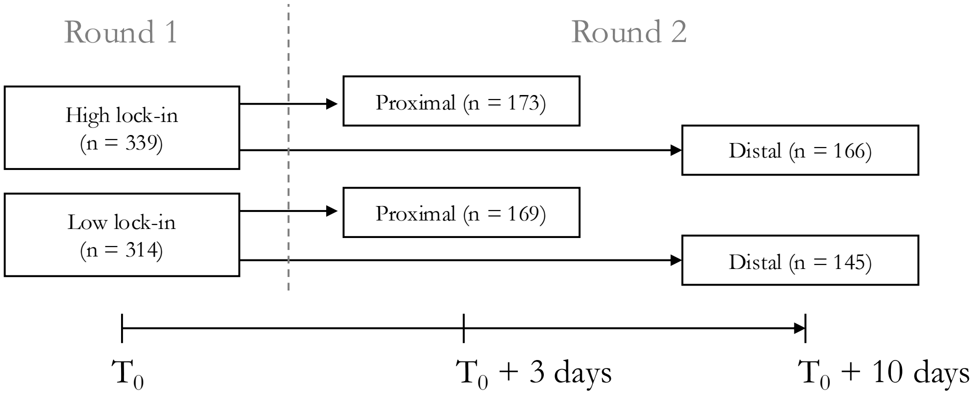
In the first survey, the participants read a text describing their history with a fictitious OSN, SocialNet. In

[7] The preregistration can be found under https://osf.io/edm84/.

the high lock-in condition, this text stated that most friends were on SocialNet only and had much content there. In the low lock-in condition, it stated that most friends were on various OSNs and had shared minimal content on SocialNet. Immediately after, the participants read a data breach notification modeled after FB's. On the next page, they responded to the continuance intention scale.[8] The remaining five dependent variables, as in Study 1, were then presented in random order to mitigate order effects. On the following pages, the participants completed scales for social switching costs and procedural costs (Jones et al. 2007) and items for feelings of conflict and discomfort (Vaidis et al. 2024). We randomized the order of the items within each scale.

To assess how quickly attitudes regress, we manipulated the passage of time between the two survey rounds for participants in the proximal and distal conditions. The proximal group was invited three days later. Their survey reiterated the lock-in, informing them that they had learned about the breach a week ago. The distal group was invited 10 days later. Again, their survey reiterated the lock-in, informing them that they had learned about the breach six months ago. Both groups then responded to the same questions as in the first survey. We opted for a relatively short real-time gap, successfully minimizing differential attrition rates (Appendix C9). Figure 4 visualizes the survey timing. Detailed survey procedures and items are provided in Appendices C1 and C2.

Figure 4. Overview of Longitudinal Experiment Procedures and Participants (Study 2)



6.3.2. Sample Characteristics

After both rounds and the removal of bots and respondents who failed attention checks, 653 respondents remained in the final sample. Detailed sample characteristics, including power analyses, descriptive statistics,

[8] To build trust in the survey and capture the participants' most tangible perceptions, we first presented continuance intention. This also minimized order effects that could arise from immediately prompting sensitive attitudes, such as OSN anxiety (Stantcheva 2023).

correlations, and validity and reliability tests, can be found in Appendices C3 to C5. We conducted a randomization check on the respondents' demographic variables, which indicated no statistically significant differences between the four experimental conditions in terms of respondents' age, gender, and prior breach experience (Appendix C4). This suggests that the randomization was successful at the respondent level.

6.3.3. Analysis and Results

We start with the following simple model specification:

$$y_{it} = \beta_0 + \beta_1 2nd\_round_t + \beta_2 Locked_i + \beta_3 (2nd\_round_t \times Locked_i) \tag{3}$$

2nd_round is coded 1 for observations from the second survey round. *Locked* is equal to 1 if respondent *i* is in the high lock-in condition. Their interaction indicates whether the change in continuance intention and attitudes from the first to the second survey rounds differs for high lock-in compared to low lock-in respondents.

Table 10 presents three sets of main results. First, consistent with our findings from Study 1, we observe evidence of improving post-breach user attitudes over time. In the second round, non-locked-in participants report higher continuance intention ($p = 0.01$) and lower feelings of violation ($p = 0.004$). We also find consistent but weaker results for perceived breach ($p = 0.08$) and OSN anxiety ($p = 0.099$), both significant at $\alpha = 0.10$. These findings suggest an increase in willingness to continue using SocialNet from the first to the second round, consistent with non-dissonant attitude regression.

Table 10. Results of the Scenario-based Experiment (Study 2)

	Continuance intention	Trust	Perceived breach	Feelings of violation	OSN belongingness	OSN anxiety
	(1)	(3)	(5)	(7)	(9)	(11)
2nd_round	0.22*	0.02	−0.15†	−0.25**	−0.06	−0.15†
	(0.09)	(0.08)	(0.09)	(0.09)	(0.08)	(0.09)
Locked	1.21***	0.45***	−0.54***	−0.43**	0.61***	−0.47***
	(0.13)	(0.11)	(0.13)	(0.14)	(0.10)	(0.13)
2nd_round × Locked	−0.06	−0.13	0.24*	0.33**	0.06	0.27*
	(0.12)	(0.10)	(0.12)	(0.12)	(0.10)	(0.12)
N	1,306	1,306	1,306	1,306	1,306	1,306
R^2	0.109	0.018	0.018	0.009	0.060	0.011

Notes. 2nd_round is a dummy variable for the second data collection round, and *Locked* is a dummy variable for the high lock-in condition. Robust standard errors clustered by respondent are in parentheses. Constants are omitted for brevity. OSN, online social network.
† $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Second, across all outcomes, the participants in the high lock-in condition evaluate SocialNet much more positively than those in the low lock-in condition. Specifically, they report higher continuance intention (p <

0.001), greater trust (p < 0.001), lower perceived breach (p < 0.001), lower feelings of violation (p = 0.002), higher OSN belongingness (p < 0.001), and lower OSN anxiety (p < 0.001). Thus, the participants with greater social and content-based investment in the platform hold more favorable attitudes about SocialNet after the data breach. Consistent with cognitive dissonance theory, these more positive attitudes may serve to reduce discomfort stemming from the conflict between attitudes and constrained behavior.

A core element of cognitive dissonance theory is the experience of internal conflict or psychological discomfort that motivates attitude change. We can observe this directly: Across both rounds, the high lock-in respondents report greater conflict (2.33 versus 2.89, p < 0.001, t = 7.53) and discomfort (2.59 versus 2.82, p = 0.003, t = 3.01) than the low lock-in respondents. Drawing on a recent large-scale multi-lab investigation (Vaidis et al. 2024), our findings provide strong empirical evidence for the presence of cognitive dissonance.

Third, the interaction between *2nd_round* and *Locked* is significant and positive for perceived breach (p = 0.05), feelings of violation (p = 0.008), and OSN anxiety (p = 0.03) and non-significant for the other variables. These positive coefficients indicate that the locked-in users' attitudes improve *similarly or less* over time compared to the non-locked-in ones (i.e., they show similar or reduced attitude regression). This suggests that cognitive dissonance does *not* lead to attitude regression. The locked-in users may have immediately adjusted their attitudes to reduce dissonance or that their dissonance remained unresolved over time. In fact, dissonance appears to persist for the locked-in users: In the second round, they still report significantly greater feelings of conflict (2.32 versus 2.89, p < 0.001, t = 5.50) and discomfort (2.60 versus 2.83, p = 0.03, t = 2.19) compared to the non-locked-in users. The latter group, being free to adjust their attitudes over time, demonstrates greater attitude regression, consistent with self-perception processes.

We further examine the mediated pathways by which lock-in affects attitudes via switching costs (see Appendix C6). The results indicate that social switching costs and procedural costs, which are the direct dissonance-inducing consequences of lock-in, partially or fully mediate the effects of lock-in on all five outcomes, other than feelings of violation. Both costs together fully mediate the effect of lock-in on OSN belongingness and partially mediate the effect of lock-in on continuance intention. Moreover, social switching costs fully mediate the effects of lock-in on trust and OSN anxiety and partially mediate the effect of lock-in on perceived breach. Procedural costs do not mediate the effects of lock-in on trust, perceived breach, and OSN anxiety.

We compare these findings to our Study 1 results to assess their external validity, using daily FB hours and FB frequency as proxy measures for lock-in for the victims breached by a friend. Despite their low power, the results (found in Appendix C7) provide some suggestive evidence for the occurrence of a similar pattern.

6.3.4. Proximal vs. Distal

We further explore the passage of time by including *Distal*, coded 1 for the distal sample, and the interaction *Distal* × *2nd_round*, representing the change from the first to the second rounds for the distal compared to the proximal groups. The results in Appendix C8 indicate no additional attitude change for the distal sample. Thus, in our experiment, victims' attitudes do not regress further over six months than they do within a week.[9] Finally, because of baseline imbalances, we construct a matched sample of proximal and distal respondents using weighted coarsened exact matching, a common approach for reducing experimental imbalances (e.g., Burtch et al. 2022; Appendix C9). Robustness checks on the matched sample yield consistent results (Appendix C8).

Our experiment indicates that cognitive dissonance generally plays a major role in influencing attitudes about an OSN after a data breach. However, our results suggest that attitude regression over time appears primarily driven by non-dissonant users in a process consistent with self-perception, occurring relatively rapidly after initial negative attitude formation, with little change between one week and six months after the data breach. Appendix D provides qualitative evidence for both cognitive dissonance and self-perception on FB from 21 semi-structured interviews with breach victims one year after the Cambridge Analytica breach (Figure 1).

7. Discussion

7.1. Contributions and Implications

In this research note, we argued that identifying actual breach victims' reactions is important when researching data breaches and showed this using FB's breach notification of the Cambridge Analytica breach. Actual breach victims exhibit greater changes in continuance intention and attitudes (OSN belongingness, feelings of violation, perceived breach, and trust) after learning that they have been breached. More intensive users drive decreases in trust and continuance intention. However, the differences between victims and non-victims disappear within six

[9] In the manipulation check, the respondents in the distal condition indicated that more time had passed since learning of the breach than those in the proximal condition (4.31 versus 3.44, $p < 0.01$, $t = 3.75$), indicating that the experimental manipulation was successful.

months. In our follow-up longitudinal experiment, we found that post-breach attitudes were strongly shaped by cognitive dissonance, with users adjusting their attitudes if they felt locked in to the OSN. Our results point to self-perception by non-dissonant users as the mechanism behind attitude regression, while the attitudes of dissonant users are more stable. Table 11 compares our contributions to prior works.

This note makes three major contributions to research. Related to RQ1, it contributes to the literature on data breaches and privacy violations by studying breach victims' attitudes after a breach notification. While much prior work is concerned with recovery of trust and PCB perceptions (e.g., Choi et al. 2016; Hoehle et al. 2022), we empirically show the actual effects of being breached on attitudes in the short and long terms. This provides a necessary foundation for studies of breach responses by establishing a first-order effect. Actual breach victims show stronger adverse reactions than non-victims in continuance intention, as well as four of the five attitudes.

Table 11. Our Findings and Contributions Relative to Other Major Data Breach Studies

Study	Breach	Type of data	Findings	Stated contributions
Goode et al. 2017	Sony	Survey, attitudes	Compensation meeting expectations is effective at influencing breach outcomes	1) Data collection from actual security event 2) Policy management after a breach 3) Study of PCB in the consumer context
Janakiraman et al. 2018	Retail	Behavioral	Being breached reduces spending and increases channel switching short term	1) Use of actual consumer data to study effects 2) Identification of harm severity as a mechanism
Hoehle et al. 2022	Target	Survey, attitudes	Compensation-related expectation disconfirmation leads to worsened customer perceptions	1) Incorporation of justice theory in IS security 2) Development of mediating mechanisms 3) Application of polynomial modeling to data breaches
Bachura et al. 2022	OPM	Behavioral	Emotional social media reactions traverse stages of anxiety, anger, and sadness	1) Exploration of large-scale data from Twitter in the breach context 2) Analysis of breach emotions 3) Use of a data-driven analysis approach
Turjeman and Feinberg 2023	Ashley Madison	Behavioral	Breached users slightly reduce their searches and messaging and delete more photos	[No dedicated contributions section]
Agarwal et al. 2024	Zomato	Behavioral	Users of a breached platform reduce digital payments and increase cash payments in the short term	[No dedicated contributions section]
This study	Facebook	Survey, attitudes	Being breached affects attitude outcomes in the short term, with mixed effects for use intensity	1) Establishment of small first-order effects of being breached on attitudes 2) Indication of effects depending little on OSN use and prior breach experience 3) Signs of attitudes regressing over time, likely driven by self-perception

Notes. OPM, Office of Personnel Management; PCB, psychological contract breach. OSN, online social network.

We also contribute to the literature on OSN privacy. OSN users' inability to protect their privacy from OSN owners, advertisers, and third-party apps is well recognized (Hull et al. 2011; Stutzman et al. 2013). We find that users' reactions to a data breach in terms of perceived breach, violation, and OSN belongingness do not depend on their extent of use, but their reactions in terms of trust and continuance intention do. The low sensitivity of affected OSN data may reduce users' reactions to being breached, relative to breaches of financial or other sensitive data. However, this unique OSN context with FB friends as the attack conduit has led to impacts not seen in other contexts (e.g., on OSN belongingness). That an OSN data breach can affect attitudes toward other users may broaden the theorization of data breach harm beyond financial and psychological harm (Solove and Citron 2018). Users with prior breach experience have similar or stronger attitudinal reactions to breaches than those without. Nevertheless, only users without prior breach experience show reduced continuance intention, implying that repeatedly breached users come to terms with data breaches and are unlikely to stop using FB, consistent with the notion of breach fatigue (Kwon and Johnson 2015; Choi et al. 2018).

Finally, we find that breach attitudes appear to revert after a data breach. This suggests that users' lack of persistent behavioral changes is not *in spite of* continued negative attitudes but is *paralleled by* a lack of persistent attitude changes. Surprisingly, this attitude regression appears to be primarily caused by non-dissonant processes, such as self-perception. While one might intuitively expect attitudes to regress to reduce dissonance because of lock-in on an OSN, we find dissonance to be somewhat time invariant. This hints at users' perceptions of the OSN being nuanced, as they balance relatively positive attitudes and feelings of discomfort and conflict. Our work responds to recent calls for more research into perceptual changes after data breaches to help better understand behavioral changes (Agarwal et al. 2024).

7.2. Limitations and Future Research

Our findings are subject to some limitations, which hold implications for future research. First, given the longitudinal study design, our Study 1 samples suffered from retention issues, especially for the third survey round. The identified effect sizes in Study 1 are modest, with values for Cohen's *d* ranging from 0.10 to 0.36. This is small compared to behavioral studies' findings. For example, Janakiraman et al. (2018) found a 32% decrease in spending by breached customers. This could be for several reasons, including the pre-period effects of having heard about the breach through the media, the innocuous framing of the notification, or a muted immediate reaction shown by dissonant users. Identifying and comparing the strength of reactions in larger samples over time may be a fruitful avenue for future research. Related to this, the long delay between rounds 2 and 3 of Study 1 may have increased random error, potentially reducing the observed effect sizes and thus the power of round 3. Future research can integrate post-breach longitudinal surveys with larger samples and more frequent data collection periods to enhance the robustness of our findings.

Second, we studied one highly publicized OSN data breach that occurred in 2018. Since then, the OSN environment has changed in terms of technical permission and user behavior. OSNs have since restricted access to their application programming interfaces (APIs), and users have migrated from feeds to closed groups and video content (The Economist 2024). How these developments affect privacy perceptions and reactions to privacy violations on OSNs is unclear. This is relevant given our results that an OSN breach may negatively influence feelings of OSN belongingness. These feelings likely depend on the wider OSN environment and type of use. The political context of Cambridge Analytica and the non-sensitive data involved may have also affected our results. Future research can thus replicate our results across contexts or in a changed OSN environment.

Third, while Study 2 offered suggestive evidence that cognitive dissonance affects breach victims' attitudes and that non-dissonant users drive the change, absent behavioral data, we cannot fully isolate self-perception as the unique mechanism. While our experimental design ruled out some alternative mechanisms—the breach is salient through the treatment (ruling out psychological distance or habituation), and respondents do not observe others using SocialNet (ruling out social comparison)—future research can measure both attitudes and behavior for a more explicit test. The scenario-based nature of Study 2 is another limitation, which future work might remedy through analyses of real-world data. Further research is required to compare attitudinal and behavioral effects, such as those found by Janakiraman et al. (2018) and Agarwal et al. (2024).

7.3. Regulatory and Business Implications

While prior works on data breaches have studied the impact of compensation and apologies on restoring customer perceptions (e.g., Hoehle et al. 2022), our finding that the differences between actual breach victims and non-victims disappear quickly calls into question the utility of compensation. FB did not compensate the victims of the Cambridge Analytica breach or any of its later data breaches (but they settled a class action lawsuit in 2023). Regulation may be needed to ensure adequate protective compensation (e.g., credit monitoring), as victims do not punish companies despite data breaches posing a threat to their livelihood (Pang and Vance 2025).

We contribute to the literature on consumers' inability to act after becoming victims of privacy violations

(Acquisti et al. 2020). Users tolerate privacy violations due to their status quo inertia, which renders any attitude and behavior changes ephemeral—even in the absence of compensation. OSNs' strong network effects increase social switching costs, making switching or boycotts unfeasible. Individuals seek OSNs for social and family contacts, increasing social switching costs and lock-in likelihood, so policies against monopolistic OSNs will have minimal impact. OSNs can thus engage in harmful privacy practices without meaningful market responses, making regulation even more important. Stronger and broader privacy regulations may be needed to prevent data breaches and privacy violations. Notably, FB's third-party app sharing that caused the data breach would have been illegal under the European Union's General Data Protection Regulation (Symeonidis et al. 2018).

From an operational perspective, the Cambridge Analytica breach resulted from third-party access to user data through friends. Researchers had highlighted the privacy risks and potential abuses of such third-party apps for years before this breach (Hull et al. 2011; Symeonidis et al. 2018), without affecting FB's third-party permission policies. FB only implemented greater API restrictions after the breach, suggesting that it could have been prevented if FB had acted earlier. Thus, to prevent such violations and policy failures, greater collaboration is needed among academic researchers, policymakers, and OSNs.

References

Acquisti A, Brandimarte L, Loewenstein G (2020) Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *J. Consumer Psych.* 30(4):736–758.

Agarwal S, Ghosh P, Ruan T, Zhang Y (2024) Transient customer response to data breaches of their information. *Management Sci.* 70(6):4105–4114.

Ayaburi EW, Treku DN (2020) Effect of penitence on social media trust and privacy concerns: The case of Facebook. *Internat. J. Inform. Management* 50:171–181.

Bachura E, Valecha R, Chen R, Rao HR (2022) The OPM data breach: An investigation of shared emotional reactions on Twitter. *MIS Quart.* 46(2):881–910.

Badshah N (2018) Facebook to contact 87 million users affected by data breach. *The Guardian* (April 8), https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach.

Bansal G, Zahedi FM (2015) Trust violation and repair: The information privacy perspective. *Decision Support Systems* 71:62–77.

Bem DJ (1972) Self-perception theory. *Adv. Experiment. Soc. Psych.* 6:1–62.

Bentley JM, Ma L (2020) Testing perceptions of organizational apologies after a data breach crisis. *Public Relat. Rev.* 46(5):101975.

Brown AJ (2020) "Should I stay or should I leave?": Exploring (dis)continued Facebook use after the Cambridge Analytica scandal. *Soc. Media Soc.* 6(1):1–8.

Burtch G, He Q, Hong Y, Lee D (2022) How do peer awards motivate creative content? Experimental evidence from Reddit. *Management Sci.* 68(5):3488–3506.

Cadwalladr C, Graham-Harrison E (2018) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian* (March 17), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cochran WG (1977) *Sampling Techniques*, 3rd ed. (John Wiley & Sohns, New York).

Choi BCF, Kim SS, Jiang Z (Jack) (2016) Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *J. Management Inform. Systems* 33(3):904–933.

Choi H, Park J, Jung Y (2018) The role of privacy fatigue in online privacy behavior. *Comput. Human Behav.* 81:42–51.

Clifford S, Sheagley G, Piston S (2021) Increasing precision without altering treatment effects: Repeated measures designs in survey experiments. *Amer. Political Sci. Rev.* 115(3):1048–1065.

Cohen J (1988) *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. (Lawrence Erlbaum Associates, Hillsdale, NJ).

Dehling T, Sunyaev A (2024) A design theory for transparency of information privacy practices. *Inform. Systems Res.* 35(3).

Festinger L (1957) *A Theory of Cognitive Dissonance* (Stanford University Press, Stanford, CA).

Fung B (2019) Facebook will pay an unprecedented $5 billion penalty over privacy breaches. *CNN Business* (July 24), https://edition.cnn.com/2019/07/24/tech/facebook-ftc-settlement/index.html.

Goode S, Hoehle H, Venkatesh V, Brown SA (2017) User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. *MIS Quart.* 41(3):703–727.

Grégoire Y, Tripp TM, Legoux R (2009) When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance. *J. Marketing* 73(6):18–32.

Grieve R, Indian M, Witteveen K, Tolan GA, Marrington J (2013) Face-to-face or Facebook: Can social connectedness be derived online? *Comput. Human Behav.* 29(3):604–609.

Guo Y, Wang C, Chen X (2023) Functional or financial remedies? The effectiveness of recovery strategies after a data breach. *J. Enterprise Inform. Management.* 37(1):148–169.

Haddock G, Maio GR (2008) Attitudes: Content, structure and functions. Hewstone M, Stroebe W, Jonas K, eds. *Introduction to Social Psychology: A European Perspective*, 4th ed. (BPS Blackwell, Oxford, UK), 112–133.

Harmon-Jones E, Mills J, eds. (1999) *Cognitive Dissonance: Progress on a Pivotal Theory in Social Psychology* (American Psychological Association, Washington, DC).

Hern A (2018) Cambridge Analytica: How did it turn clicks into votes? *The Guardian* (May 6), https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie.

Hinds J, Williams EJ, Joinson AN (2020) "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *Internat. J. Human Comput. Stud.* 143(April):102498.

Hoehle H, Wei J, Schuetz S, Venkatesh V (2021) User compensation as a data breach recovery action: A methodological replication and investigation of generalizability based on the Home Depot breach. *Internet Res.* 31(3):765–781.

Hoehle H, Venkatesh V, Brown SA, Tepper BJ, Kude T (2022) Impact of customer compensation strategies on outcomes and the mediating role of justice perceptions: A longitudinal study of Target's data breach. *MIS Quart.* 46(1):299–340.

Hull G, Lipford HR, Latulipe C (2011) Contextual gaps: Privacy issues on Facebook. *Ethics Inform. Tech.* 13(4):289–302.

IBM (2023) What is a data breach? Retrieved July 15, 2025, https://www.ibm.com/topics/data-breach.

James TL, Lowry PB, Wallace L, Warkentin M (2017) The effect of belongingness on obsessive-compulsive disorder in the use of online social networks. *J. Management Inform. Systems* 34(2):560–596.

Janakiraman R, Lim JH, Rishika R (2018) The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *J. Marketing* 82(2):85–105.

John OP, Donahue EM, Kentle RL (1991) *The Big Five Inventory - Versions 4a and 54* (University of California, Berkeley, Institute of Personality and Social Research, Berkeley, CA).

Jones MA, Reynolds KE, Mothersbaugh DL, Beatty SE (2007) The positive and negative effects of switching costs on relational outcomes. *J. Service Res.* 9(4):335–355.

King J, Lampinen A, Smolen A (2011) Privacy: Is there an app for that? *Proc. 7th Sympos. Usable Privacy Security (New York, USA), Article 12, 1-20*.

Kude T, Hoehle H, Sykes TA (2017) Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *Internat. J. Oper. Production Management* 37(1):56–74.

Kwon J, Johnson ME (2015) The market effect of healthcare security: Do patients care about data breaches? *14th Workshop Econom. Inform. Security (Delft, Netherlands).*

Lee M, Lee J (2012) The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Inform. Systems Frontiers* 14(2):375–393.

Lovakov A, Agadullina ER (2021) Empirically derived guidelines for effect size interpretation in social psychology. *European J. Soc. Psych.* 51(3):485–504.

Lowry PB, D'Arcy J, Hammer B, Moody GD (2016) "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *J. Strategic Inform. Systems* 25(3):232–240.

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. *Comm. Assoc. Inform. Systems* 34(60):1157–1174.

Martin KD, Borah A, Palmatier RW (2017) Data privacy: Effects on customer and firm performance. *J. Marketing* 81(1):36–58.

Masuch K, Greve M, Trang S (2021) What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electron. Markets* 31(4):829–848.

Mikhed V, Vogan M (2018) How data breaches affect consumer credit. *J. Banking Finance* 88:192–207.

Nikkhah HR, Grover V (2022) An empirical investigation of company response to data breaches. *MIS Quart.* 46(4):2163–2196.

Nofer M, Hinz O, Muntermann J, Roßnagel H (2014) The economic impact of privacy violations and security breaches: A laboratory experiment. *Bus. Inform. Systems Engrg.* 6(6):339–348.

Pang MS, Vance A (2025) Breached and denied: The cost of data breaches on individuals as mortgage application denials. *MIS Quart.* 49(2):465–494.

Ployhart RE, Vandenberg RJ (2010) Longitudinal research: The theory, design, and analysis of change. *J. Management* 36(1):94–120.

Schroeder S (2019) U.S. users are leaving Facebook, new study claims. *Mashable* (March 7), https://mashable.com/article/facebook-losing-users-us/.

Solove DJ, Citron DK (2018) Risk and anxiety: A theory of data breach harms. *TX Law Rev.* 96:738–785.

Stantcheva S (2023). How to run surveys: A guide to creating your own identifying variation and revealing the invisible. *Annual Rev. Econom.* 15(1):205–234.

Statista (2023) Number of Facebook users in the United States from 2018 to 2027. https://www.statista.com/statistics/408971/number-of-us-facebook-users/ (accessed October 14, 2025).

Stutzman FD, Gross R, Acquisti A (2013) Silent listeners: The evolution of privacy and disclosure on Facebook. *J. Privacy Confidentiality* 4(2): 7–41.

Syed R (2019) Enterprise reputation threats on social media: A case of data breach framing. *J. Strategic Inform. Systems* 28(3):257–274.

Symeonidis I, Biczók G, Shirazi F, Pérez-Solà C, Schroers J, Preneel B (2018) Collateral damage of Facebook third-party applications: A comprehensive study. *Comp. Security* 77:179–208.

The Economist (2024) As Facebook turns 20, politics is out; impersonal video feeds are in. (February 1), https://www.economist.com/briefing/2024/02/01/as-facebook-turns-20-politics-is-out-impersonal-video-feeds-are-in.

Turjeman D, Feinberg FM (2024) When the data are out: Measuring behavioral changes following a data breach. *Marketing Sci.* 43(2):440–461.

Vaidis DC, Sleegers WWA, Van Leeuwen F, DeMarree KG, Sætrevik B, Ross RM, Schmidt K, et al. (2024) A multilab replication of the induced-compliance paradigm of cognitive dissonance. *Adv. Methods Practices Psych. Sci.* 7(1):1-26.

Wright SA, Xie GX (2019) Perceived privacy violation: Exploring the malleability of privacy expectations. *J. Bus. Ethics* 156:123–140.