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

Appendix A: Literature

Appendix A1: Coding of the Relevant Literature

Table A-1 below provides the text sections used for the classification of each study in Table 1. Many studies were not explicit about how their respondents were affected by the breach; accordingly, we either estimated to which extent actual breach victims were identified from available descriptions or contacted select authors of these studies to confirm their sample selection.

Table A-1: Coding of the relevant literature

Group studied		Article	Paper excerpt
Scenario-based	General public	Nofer et al. (2014)	In the second treatment group we added the sentence: "The bank has lost customer data. A former bank employee has stolen a CD with personal information and is now offering it for sale." […] Participants had to indicate the amount of money they were willing to invest into a financial product given the investment plan offered by the bank. (p. 344)
		Bansal and Zahedi (2015)	The website you saw announced late Sunday that criminal hackers broke into its systems and had access to personal information of potentially more than 24 million customer accounts. This sheer size is quite similar to the number of accounts that Sony's PlayStation Network reported stolen in April 2011 i.e. 77 million. (p. 67, Table 2)
	Potential breach victims	Wright and Xie (2019)	Participants began by naming a real company with which they had shared personal data (e.g., for billing purposes, communications, or to receive promotions). […] Next, participants read a news article reporting that the named company […] accidentally shared customer information to client companies. (p. 128-129)
	Actual breach victims	Mamonov and Koufaris (2014)	We exposed study participants to the vignette and asked them to fill out a survey and report how their attitudes and behavioral intentions would be impacted in relation to their carrier if they had discovered that their carrier had pre-installed the Carrier IQ software on their smartphones. This approach is designed to mimic closely a scenario in which consumers may learn about privacy-infringing technology through news media. (p. 1163)
		Choi et al. (2016)	The scenarios asked the subjects to imagine that they had just received an e-mail from the online vendor that they had named earlier. The message of the e-mail was that hackers had stolen their credit card information. (p. 919)
		Bentley and Ma (2020)	Participants were asked to enter the name of a company they had shopped with online. [Scenario 1] read as follows: […] Our computer administrators recently discovered that hackers have illegally accessed a database containing the personal account information of [Company] customers. This database includes credit card numbers and shipping addresses. Your account is one that has been affected. Please contact our customer service department if you have any questions. (p. 3)
		Masuch et al. (2021)	The participant was presented with the situation that he would like to start a new run, but that a message from the fitness tracker's provider appears shortly before the run begins, stating that an unauthorized third party violated some of his data. (p. 838)
		Nikkhah and Grover (2022)	We asked participants to provide the name of a company that they actually use and for which they need to provide personal information to receive the company's service or product. Then, we showed the participants Scenario A to allow them to imagine that a data breach happened in the company they mentioned earlier and that their personally identifiable information (PII) was stolen. (p. 2173)
		Guo et al. (2023)	We manipulated the two recovery strategies by designing suitable experiment scenarios. […] [Scenario] "We are very sorry to inform you that customer information on our website has been compromised due to a hacking attempt involving your credit card information. You are advised to monitor your credit card account."
Real-life breach	General public	Syed (2019)	We searched for relevant tweets using hashtags, e.g., #HDBreach, #Hddatabreach. (p. 7)
		Bachura et al. (2022)	All messages contained the hashtag #OPMHack.(p. 886)
		Lee and Lee (2012)	On Feb. 4, 2008, Internet Auction Co. ("Auction" hereafter), one of the largest Internet shopping sites in Korea, publicly admitted that its customer database had been compromised by an external hacker. (p. 375) Sampling criteria were 1) at least one purchase of goods or services over the Internet

Table A-1: Coding of the relevant literature			
Group studied		**Article**	**Paper excerpt**
	Potential breach victims		since Jan., 2008 and 2) registered membership with at least one of the three largest Internet shopping malls in Korea (i.e., Auction, Gmarket, and Interpark), as of Jan., 2008 (just before the Auction incident). (p. 384)
		Goode et al. (2017)	Candidate respondents were first required to indicate their ownership of a range of different electronic devices. Those who did not indicate ownership of a Sony PlayStation 3 were excluded from the participant group. (p. 712)
		Kude et al. (2017)	We collected data from customers who were affected by Target's data breach. […] To identify potential respondents who were affected by Target's data breach, the market research firm contacted individuals who lived in the USA and invited them to participate in our study. All interviews were carried out via phone and the sampling frame consisted of 2,500 US consumers who were encouraged via small monetary incentives provided by the market research firm. Of these, 212 (58 percent men) provided usable responses, resulting in a response rate of 8.5 percent. All responses were collected during a single weekend after Target had announced compensation as a response to its data breach and no reminders were employed. (p. 62)
		Mikhed and Vogan (2018)	The South Carolina data breach is a "treatment" that directly affected South Carolina residents at the time of the breach (October 2012) and indirectly affected residents of certain areas in neighboring Georgia and North Carolina (consumers in shared media markets) through the news. […] We use the local television markets as defined by Nielsen's Designated Market Areas (DMAs) to examine the reaction of North Carolina and Georgia residents to the breach. (p. 193) […] The breach, which was the largest to occur in 2012, affected about 81% of South Carolina residents. (p. 194)
		Ayaburi and Treku (2020)	We collected data by administering a web-based questionnaire survey to Facebook account holders using Amazon Mturk, which was deemed appropriate since our target respondents have experience of the research context. The (p. 176)
		Hoehle et al. (2021)	Using a market research company, we collected data from 1,084 participants in round 1 and 901 of those participants in round 2 (Table 3). Similar to the original study, in both rounds, most participants were men. However, in contrast to the original study, our participants were older and had higher salaries. This pattern of differences was to be expected, as the customers of PSN are, on average, likely to be younger given that it is related to gaming compared to the average shopper at Home Depot. (p. 769)
		Hoehle et al. (2022)	We used a professional market research firm to identify and collect data from customers who were affected by Target's data breach. Potential respondents were contacted via telephone and asked if they were willing to participate in our study. An important criterion for inclusion was that the potential respondents knew about Target's breach. […]The data collection started immediately after Target had publicly confirmed the data breach and it was reported on Krebsonsecurity.com on December 18, 2013 (Clark 2014). The first round was com- pleted within two business days. (p. 305). [Note: this was after the news broke, but before Target actually notified breached shoppers]
	Actual breach victims	Janakiraman et al. (2018)	The data set for this study comes from a publicly owned department store retailer headquartered in the United States. […] During the time span of the data set, the focal multichannel retailer suffered a data breach and subsequently announced publicly that customer payment data related to its physical store channel during a specific transaction time period was breached. In particular, customer debit and/or credit card information was compromised for customers who purchased in the physical stores (the "breached" channel, hereinafter) during a certain time window (the "breached" or the "affected" time period). (p. 90)
		Turjeman and Feinberg (2024)	Our analysis and statistical estimates pertain to male users that had paid at least once for credits, since all such users had to provide their full name and billing address in order to process payment. […] Importantly, these users were informed, on the day of the breach announcement, that their real names and addresses were in the hands of the hackers – entailing the risk of widespread exposure – along with other personal information, and an indication that they were seeking an affair. (p. 10)
		Agarwal et al. (2024)	The data breach involved 17 million users' names, email addresses, and passwords. The firm claimed that it had reset passwords for all affected users and logged them out of its app and website, and no payment information was leaked. We use administrative data from the breached platform for our analysis. (p. 2)

Appendix A2: Literature Review on Privacy

While privacy in general has been studied in legal literature since the late 19th century, the advent of increasing digitization and the internet has shifted the focus specifically toward **information privacy**. Unlike physical privacy, which relates to physical access to a person, information privacy relates to the access to personal data. Information privacy has emerged as a key research topic across disciplines, including information systems, legal studies, computer science, psychology, and economics, reflecting its relevance for internet users, policymakers, and companies processing data (Smith et al. 2011). The literature reveals several disconnects related to people's stated claims, attitudes, and actual behaviors. When prompted about their preferences, internet users generally state **preferences for high levels of privacy** and rate this issue as important to them (Acquisti et al. 2020). However, in their actual behavior online, this desired level of privacy is generally impossible to achieve, which leads to a **dissatisfaction** that has variously been characterized as privacy fatigue (Choi et al. 2018) or digital resignation (Draper and Turow 2019).

Many different phenomena have been investigated related to privacy decision-making. In behavioral studies, privacy concerns are often at the center of the nomological network, giving rise to the **antecedents-privacy concerns-outcomes (APCO) model** (Smith et al. 2011). For example, research on antecedents includes Malhotra et al. (2004), who study factors influencing internet users' information privacy concerns, and Xu et al. (2012), who study the role of perceived control over personal information on privacy concerns. Studies on outcomes, such as Lowry et al. (2011), examine how privacy concerns affect the use of self-disclosure technology. More recently, research has widened to study privacy concerns in different social or use contexts, such as peer disclosure (Zhang et al. 2022) or data sharing on the Internet of Things (Cichy et al. 2023).

The disconnect between individuals' stated privacy preferences and observed behavior, including the use of websites and services that violate their privacy and the free sharing of relatively private information online, has been called the "**privacy paradox**" (Barnes 2006). This has been especially observed in the context of online social networks (OSNs), where both joining the OSN and disclosing information to other users often contradict individuals' stated privacy preferences. Several explanations have been proposed for this paradox. First, general attitudes may not always translate into specific behaviors (Acquisti et al. 2016). Second, people may consciously deliberate the **cost-benefit trade-off** of individual information disclosure, a behavior called "privacy calculus" (Dinev and Hart 2006; Li et al. 2010). Third, privacy decisions are embedded in **social contexts** that affect the actual behavior (Kokolakis 2017). Fourth, people's privacy risk perceptions may be skewed due to different cognitive **biases and heuristics** (Adjerid et al. 2018). Finally, some researchers argue that the paradox only exists due to a **misinterpretation** of the term "paradox" and the actual constructs that are measured (Acquisti et al. 2020). Notably, Acquisti et al. (2020) emphasize that although revealed preferences in people's actual behavior may show that they do not value privacy very highly, this does not invalidate their explicitly stated preferences, and policymakers should be mindful of the role of biases and heuristics—people continuing to use a privacy-violating service does not remove the need for regulation.

Our results and their position in the data breach literature is both informed by and reflect on this general privacy literature. Our qualitative results (**Appendix D**) add to the discussion on people's dissatisfaction with their general privacy on FB; simultaneously, our quantitative results show that no long-term attitude change occurs since users regress their attitudes towards the OSN due to self-perception, and that users' attitudes are biased by cognitive dissonance. OSN operators or data processors in general may understand this to imply that no negative consequences need to be feared from data breaches and privacy violations. Thus, our results, taken together with those of Janakiraman et al. (2018) and Agarwal et al. (2024) even further support the idea that privacy concerns or dissatisfaction with the level of privacy **do not meaningfully affect everyday consumer behavior and attitudes**. Nonetheless, we follow Acquisti et al. (2020) in cautioning against an understanding that our results would imply no need for regulation because there is fundamentally no problem. Instead, through our Study 2 and qualitative results, we lend further credence to the idea that **social contexts** (such as the social switching costs keeping people from quitting FB) and **biases** (such as cognitive dissonance) **inhibit people from obtaining a desired level of privacy**, even to the extent that they readjust their attitudes to FB. This in fact necessitates a stronger regulatory response. Through our findings, we thus contribute to the literature on privacy and the privacy paradox by establishing it in a specific instance of a shocking privacy violation.

Another major difficulty is the fact that privacy practices are often highly opaque, and privacy policies are generally unreadable (Obar and Oeldorf-Hirsch 2020; Dehling and Sunyaev 2024). In response, Dehling and Sunyaev (2024) have developed a design theory to improve the information privacy practices of privacy notices. This is fundamentally tied to FB's data practices that enabled the Cambridge Analytica breach: if it had been more apparent to the users which data third-party apps can access, and if the third parties had had to give their consent, Cambridge Analytica's access to the data may perhaps have been prevented.

In another perspective, Xu and Zhang (2024) argue that internet users do not make purposeful privacy decisions but rather engage in unreflected "absorbed coping" in familiar situations, until a breakdown occurs that prompts reflective reasoning. Xu and Zhang (2024) call for further research into such breakdown situations. Our current study may pose a relevant contribution to their perspective, since the Cambridge Analytica breach likely represents such a breakdown; however, we find no sustainable changes in response to this breakdown of understanding. If and how data breach victims, such as our FB users, return from their privacy reconsiderations after the breakdown to their normal absorbed coping during everyday use may be an interesting phenomenon for future case studies.

Appendix B: Study 1

Appendix B1: Measures to Ensure the Validity of Online Panels

Lowry et al. (2016) suggest the following remedies to address problems in using Amazon's Mechanical Turk (MTurk) to collect data.

Representativeness. We report a study using quasi-experimental methods. Experiments have been shown to work particularly well on MTurk and earlier studies have confirmed the replicability of experimental findings generated on MTurk with nationally representative samples (e.g., Berinsky et al. 2012; Coppock 2019). In addition, the proportion of breached users in our sample is 27.4%, which is within 5 percentage points of the population ratio (31.5%) and provides confidence that our panel is representative of the broader population of U.S. Facebook users.

Respondents' identity. We take several measures to verify that our respondents were legitimate targets for the Cambridge Analytica breach. First, using the MTurk user interface, we limit the sample to the U.S., where the attention around the Cambridge Analytica breach was greatest. Second, in Study 1, we screened out participants who did not have a Facebook account because they could not be affected by the breach. Third, participants had the opportunity to share their thoughts regarding the breach at the end of the surveys. From the answers, we judged that many of them identified with the setting and had strong feelings about it. Overall, we believe that respondents' identity should not be a concern in our study.

Dishonesty and inattentiveness. We use two main strategies to address concerns regarding dishonesty and inattentiveness. First, we add randomly appearing attention check questions. In our main analysis, we keep only respondents who correctly answer all attention checks in each round. The questions are summarized in Table B-1. Second, as a robustness check, we eliminate respondents with unusually fast response times because these users might have put less effort into the tasks. The results in Table B-2 show that our results remain qualitatively unchanged to excluding respondents whose combined response time over both rounds are more than one or two standard deviations below the mean.

Table B-1: Attention check items

Round	Item	Question	Source
Rounds 1 and 3	Attention1	Please answer "Strongly Agree" to this question.	James et al. (2017)
	Attention2	Please answer "Never" for this item.	
	Attention3	The United States is on the continent of Africa.	
Round 2	Attention1	Please answer "Strongly Disagree" to this question.	
	Attention2	Please answer "Always" for this item.	
	Attention3	The United States is on the continent of Asia.	

Table B-2: Dropping response times more than one or two standard deviations (SD) below the mean

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	One SD	Two SD	One SD	Two SD	One SD	Two SD	One SD	Two SD	One SD	Two SD	One SD	Two SD
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Victim × Post	-0.13	-0.23*	-0.23*	-0.24*	0.58**	0.58***	0.37*	0.41**	-0.31**	-0.35**	0.11	0.17
	(0.11)	(0.11)	(0.11)	(0.10)	(0.18)	(0.17)	(0.15)	(0.14)	(0.12)	(0.12)	(0.13)	(0.13)
R^2	0.232	0.215	0.164	0.168	0.120	0.123	0.095	0.106	0.171	0.154	0.146	0.135

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. n = 662 and 752 for all "One SD" and "Two SD" models, respectively. Post is a dummy variable for the 2nd survey round, Victim is a dummy variable for individuals breached in the 2nd survey round. OSN = online social network. FB = Facebook. Robust standard errors clustered by respondent in parentheses. Regressions include terms for Victim, Post, Age, Gender, Prior breach, FB friends, FB frequency, and FB hours. Constant and control variables are omitted for brevity.

Appendix B2: Survey Items

Table B-3: Survey items			
Construct	**Item**	**Question**	**Source**
Continuance intention	Continuance1	I intend to continue using Facebook.	Venkatesh & Goyal (2010)
	Continuance2	I want to continue using Facebook rather than discontinue.	
	Continuance3	I predict I will continue using Facebook.	
	Continuance4	I plan to continue using Facebook.	
Trust	Trust1	Based on my experience with Facebook in the past, I know it is honest.	Gefen et al. (2003)
	Trust2	Based on my experience with Facebook in the past, I know it provides good service.	
	Trust3	Based on my experience with Facebook in the past, I know it is predictable.	
	Trust4	Based on my experience with Facebook in the past, I know it is trustworthy.	
Perceived breach	PerceivedBreach1	Facebook has failed to meet its obligation to me.	Choi et al. (2016)
	PerceivedBreach2	Facebook has done a poor job of meeting its obligations to me.	
	PerceivedBreach3	Facebook has neglected the most important obligations to me.	
Violation	Violation1	I feel extremely frustrated by how I was treated by Facebook.	Choi et al. (2016)
	Violation2	The more I think about it, the more hostile I feel towards Facebook.	
	Violation3	I feel a great deal of anger toward Facebook.	
OSN belongingness	Belong1	I am in tune with my Facebook friends.	James et al. (2017), adapted from Grieve et al. (2013)
	Belong2	I feel close to people on Facebook.	
	Belong3	I see Facebook friends as friendly and approachable.	
	Belong4	I feel understood by people on Facebook.	
	Belong5	I am able to relate to my Facebook friends.	
	Belong6	I find myself actively involved in Facebook friend's lives.	
	Belong7	I am able to connect with other people on Facebook.	
	Belong8	My Facebook friends feel like family.	
OSN anxiety	Anxiety1	Using Facebook makes me feel uneasy.	James et al. (2017), adapted from Thatcher & Perrewé (2002)
	Anxiety2	Using Facebook causes me stress.	
	Anxiety3	I sometimes feel anxious when I use Facebook.	

Table B-4: Demographics items		
Construct	**Question**	**Answer**
Gender	What is your gender?	
	1	Male
	2	Female
Age	What is your age?	
	1	Under 20
	2	20-29
	3	30-39
	4	40-49
	5	50-59
	6	60 or older
Prior data breach experience	Have you ever experienced a data breach (identity theft, wallet loss, etc.) before?	
	1	Yes
	2	No

Appendix B3: Correlation Tables

Table B-5: Correlation table for the pre-period

No	Variables	1	2	3	4	5	6	7	8	9	10	11	12	13
1	Victim	1.00												
2	Continuance intention	0.01	1.00											
3	Trust	-0.01	0.71***	1.00										
4	Perceived breach	-0.01	-0.62***	-0.72***	1.00									
5	Feelings of violation	0.03	-0.73***	-0.71***	0.76***	1.00								
6	OSN belongingness	0.06	0.51***	0.51***	-0.36***	-0.39***	1.00							
7	OSN anxiety	-0.04	-0.62***	-0.60***	0.59***	0.73***	-0.52***	1.00						
8	Age	-0.01	0.01	0.01	0.09†	-0.06	0.08	-0.00	1.00					
9	Gender	0.12*	0.13*	0.08†	-0.07	-0.10†	0.09†	-0.01	0.09†	1.00				
10	Prior breach	0.01	0.06	0.13*	-0.13*	-0.10†	0.01	-0.10*	-0.02	-0.07	1.00			
11	FB friends	0.23***	0.20***	0.23***	-0.20***	-0.10†	0.22***	-0.17**	-0.25***	0.01	-0.01	1.00		
12	FB frequency	0.19***	0.47***	0.31***	-0.28***	-0.27***	0.39***	-0.33***	-0.03	0.27***	0.05	0.36***	1.00	
13	FB hours	0.19***	0.35***	0.30***	-0.27***	-0.20***	0.30***	-0.22***	-0.07	0.30***	0.08	0.35***	0.60***	1.00

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. N = 380. OSN = online social network. FB = Facebook.

Table B-6: Correlation table for the post-period

No	Variables	1	2	3	4	5	6	7	8	9	10	11	12	13
1	Victim	1.00												
2	Continuance intention	-0.05	1.00											
3	Trust	-0.08	0.73***	1.00										
4	Perceived breach	0.14**	-0.64***	-0.74***	1.00									
5	Feelings of violation	0.13*	-0.67***	-0.65***	0.80***	1.00								
6	OSN belongingness	-0.06	0.55***	0.58***	-0.39***	-0.41***	1.00							
7	OSN anxiety	0.01	-0.67***	-0.66***	0.69***	0.73***	-0.48***	1.00						
8	Age	-0.01	0.05	0.02	0.02	-0.13*	0.05	-0.06	1.00					
9	Gender	0.12*	0.09†	0.02	-0.04	-0.08	0.04	0.00	0.09†	1.00				
10	Prior breach	0.01	0.07	0.12*	-0.07	-0.09†	0.08	-0.11*	-0.02	-0.07	1.00			
11	FB friends	0.23***	0.19***	0.24***	-0.16**	-0.09†	0.16**	-0.20***	-0.25***	0.01	-0.01	1.00		
12	FB frequency	0.19***	0.41***	0.31***	-0.22***	-0.19***	0.30***	-0.31***	-0.03	0.27***	0.05	0.36***	1.00	
13	FB hours	0.19***	0.31***	0.31***	-0.22***	-0.15**	0.25***	-0.20***	-0.07	0.30***	0.08	0.35***	0.60***	1.00

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. N = 380. OSN = online social network. FB = Facebook.

Appendix B4: Sample Attrition

Table B-7: Comparison between respondents who dropped out between rounds and those who did not							
	R1 only		R1 and R2		Difference		
	Mean	SD	Mean	SD	R2-R1	t	p
Continuance intention	4.67	1.68	4.75	1.72	0.08	(0.47)	0.64
Trust	3.64	1.26	3.64	1.34	-0.00	(-0.01)	0.99
Perceived breach	4.89	1.55	4.66	1.61	-0.22	(-1.31)	0.19
Feelings of violation	3.82	1.59	3.70	1.76	-0.12	(-0.66)	0.51
OSN belongingness	4.18	1.37	4.38	1.35	0.21	(1.43)	0.15
OSN anxiety	3.80	1.47	3.49	1.67	-0.31†	(-1.81)	0.07
Age	3.50	1.19	3.48	1.17	-0.14	(-0.11)	0.91
Gender	1.51	0.50	1.51	0.50	-0.01	(-0.10)	0.92
Prior breach	1.37	0.49	1.46	0.50	0.08	(1.54)	0.12
FB friends	3.05	1.35	3.19	1.28	0.14	(1.02)	0.31
FB frequency	3.59	1.38	3.72	1.35	0.12	(0.86)	0.39
FB hours	1.94	1.22	1.82	1.00	-0.12	(-1.03)	0.30
N	115		380		495		
† $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. OSN = online social network. FB = Facebook.							

Appendix B5: Standardized Effect Size for Repeated Measurements

The estimate for Cohen's d is typically applied in experimental designs, where participants are assigned to treatment and control conditions, but participants are measured only after the treatment (Morris 2008). In contrast, our study employs a difference-in-differences (DID) approach, where participants are assigned to either the treatment or control condition, and each participant is measured both before and after the treatment. This design helps control for preexisting differences, enabling us to estimate treatment effects more accurately. To calculate the effect size in a DID design, we define Cohen's d as:

$$d = \frac{(M_{post,T} - M_{pre,T}) - (M_{post,C} - M_{post,C})}{SD_{pre}} \quad (1)$$

where the standard deviation is defined as

$$SD_{pre} = \sqrt{\frac{(n_T - 1)SD_{pre,T}^2 + (n_C - 1)SD_{pre,C}^2}{n_T + n_C - 2}}. \quad (2)$$

In this setup, n_T represents the number of participants affected by the breach (treatment group) and n_C represents the number of participants unaffected by the breach (control group). The pre-period and post-period means for the treatment group are denoted as $M_{pre,T}$ and $M_{post,T}$, respectively. The pre-period and post-period means for the control group are denoted as $M_{pre,C}$ and $M_{post,C}$, respectively. Separate estimate of the standard deviation can be obtained for the treatment groups in the pre-period ($SD_{pre,T}$) and post-period ($SD_{post,T}$), as well as for the control group in the pre-period ($SD_{pre,C}$) and post-period ($SD_{post,C}$). These standard deviations can be combined in various ways to derive different estimates of the effect size d.

As defined in Equation (2), we use the pooled pre-period standard deviations. The variance of post-period scores in the treatment group might be inflated relative to the other conditions, as noted by Morris (2008), which can increase the pooled standard deviation and result in an underestimated effect size. By using only the pre-period standard deviations, we obtain an unbiased estimate of the population effect size, even when the post-period scores exhibit greater variability.[1] Table B-8 shows the results.

While Cohen's (1988) original interpretation of d suggested thresholds of 0.20 (small), 0.50 (medium), and 0.80 (large), more recent research suggests that these thresholds may be too large, with updated benchmarks at 0.15 (small), 0.36 (medium) and 0.65 (large) (Lovakov and Agadullina 2021). Based on these revised 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).

Because no data on perceptual changes after a real-world breach exist, we compare our effect size estimates to those of a scenario-based study. Nofer et al. (2014) found lower levels of trust among respondents in a security breach condition compared those in a control group (see Table B-9 for their items). We estimate the effect size for trust to be between 0.80 to 0.85[2]—about four to five times larger than the effect size we observe (0.17). Although the treatment in Nofer et al. (2014) differs slightly from ours—their study compared perceptions of customers between a breached company and a non-breached company, whereas our study focuses on whether a customer of a breached company was directly affected or not—this comparison underscores the ecological validity of our study. Scenario-based studies often emphasize the breach and its consequences, potentially inducing stronger reactions. In contrast, real-world breaches may evoke more nuanced and less intense responses, making our findings more reflective of actual outcomes.

[1] The results are qualitatively unchanged, when replacing SD_{pre} with the pooled standard deviations across pre- and post-periods, with $SD_{pooled} = \sqrt{\frac{(n_T-1)SD_{pre,T}^2+(n_C-1)SD_{pre,C}^2+(n_T-1)SD_{post,T}^2+(n_C-1)SD_{post,C}^2}{2\times(n_T+n_C-2)}}$.

[2] We calculate the effect size based on the unstandardized regression coefficient for the security breach variable (0.104). Since the standard deviation of the outcome variable, trust, is not reported, we assume a value of 1.35, as reported in the original study by Pavlou and Gefen (2004). Additionally, the exact number of participants in each treatment arm is not specified. However, given that there are 118 total participants divided across three treatment arms, we expect roughly 40 participants in the security breach condition.

Table B-8: Standardized effect sizes									
	Breached				Non-breached				d
Variable	n_T	$M_{pre,T}$	$SD_{pre,T}$	$M_{post,T}$	n_C	$M_{pre,C}$	$SD_{pre,C}$	$M_{post,C}$	
Continuance intention	104	4.784	1.690	4.647	276	4.741	1.739	4.844	-0.139
Trust	104	3.606	1.336	3.389	276	3.647	1.343	3.661	-0.172
Perceived breach	104	4.631	1.511	4.753	276	4.676	1.651	4.214	0.362
Feelings of violation	104	3.795	1.766	3.788	276	3.659	1.762	3.242	0.233
OSN belongingness	104	4.517	1.422	4.243	276	4.332	1.320	4.417	-0.266
OSN anxiety	104	3.391	1.641	3.641	276	3.524	1.677	3.615	0.096

Table B-9: Nofer et al. (2014) items for trust			
Construct	**Item**	**Question**	**Source**
Trust	Trust1	The described bank is honest with regard to its statements.	Pavlou and Gefen (2004)
	Trust2	According to the information provided the described bank is reliable and a serious trading partner.	
	Trust3	According to the information provided the described bank seems to be dependable.	
	Trust4	The described bank is trustworthy in general.	

Appendix B6: Matched Samples

Table B-10: Effect of being an actual data breach victim in a sample matched on the number of Facebook friends

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post	0.11†	0.11†	0.02	0.02	-0.47***	-0.47***	-0.43***	-0.43***	0.08	0.08	0.02	0.02
	(0.06)	(0.06)	(0.07)	(0.07)	(0.08)	(0.08)	(0.10)	(0.10)	(0.06)	(0.06)	(0.08)	(0.08)
Victim	-0.18	-0.37*	-0.27	-0.36*	0.24	0.33†	0.30	0.45*	-0.02	-0.12	0.06	0.17
	(0.20)	(0.18)	(0.17)	(0.15)	(0.20)	(0.18)	(0.22)	(0.20)	(0.17)	(0.16)	(0.20)	(0.19)
Victim × Post	-0.24*	-0.24*	-0.24*	-0.24*	0.59***	0.59***	0.43**	0.43**	-0.36**	-0.36**	0.23†	0.23†
	(0.11)	(0.11)	(0.11)	(0.11)	(0.17)	(0.17)	(0.15)	(0.15)	(0.12)	(0.12)	(0.13)	(0.14)
Age		0.08		0.09		0.00		-0.21*		0.13*		-0.11
		(0.09)		(0.07)		(0.07)		(0.08)		(0.06)		(0.08)
Gender		-0.03		-0.15		0.08		-0.16		-0.12		0.24
		(0.18)		(0.13)		(0.17)		(0.19)		(0.13)		(0.19)
Prior breach		0.18		0.21		-0.22		-0.29		0.03		-0.28†
		(0.17)		(0.14)		(0.16)		(0.18)		(0.13)		(0.17)
FB friends		0.13		0.23***		-0.28***		-0.21*		0.11†		-0.20*
		(0.09)		(0.06)		(0.08)		(0.09)		(0.06)		(0.09)
FB frequency		0.64***		0.23**		-0.25**		-0.34***		0.30***		-0.46***
		(0.09)		(0.07)		(0.08)		(0.10)		(0.08)		(0.09)
FB hours		0.08		0.26**		-0.25**		-0.10		0.19*		0.01
		(0.09)		(0.08)		(0.09)		(0.10)		(0.09)		(0.09)
Intercept	4.97***	1.43*	3.88***	1.27*	4.39***	7.05***	3.49***	7.08***	4.54***	2.37***	3.33***	6.18***
	(0.12)	(0.70)	(0.11)	(0.52)	(0.13)	(0.55)	(0.13)	(0.65)	(0.09)	(0.43)	(0.12)	(0.62)
R^2	0.007	0.255	0.016	0.250	0.032	0.218	0.025	0.163	0.008	0.186	0.004	0.153

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 760 for all models. Post is a dummy variable for the 2nd survey round, Victim is a dummy variable for individuals who stated being breached in the 2nd survey round. OSN = online social network. FB = Facebook. Robust standard errors clustered by respondent in parentheses.

Table B-11: Effect of being an actual data breach victim in a sample matched on the number of Facebook friends, gender, and Facebook frequency												
	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Post	0.09†	0.09†	0.06	0.06	-0.49***	-0.49***	-0.37***	-0.37***	0.03	0.03	0.06	0.06
	(0.05)	(0.06)	(0.07)	(0.07)	(0.10)	(0.10)	(0.09)	(0.09)	(0.07)	(0.07)	(0.07)	(0.07)
Victim	-0.40†	-0.42*	-0.34†	-0.37*	0.30	0.33†	0.48*	0.51*	-0.17	-0.19	0.18	0.20
	(0.21)	(0.18)	(0.18)	(0.16)	(0.20)	(0.19)	(0.22)	(0.21)	(0.18)	(0.17)	(0.22)	(0.21)
Victim × Post	-0.27*	-0.27*	-0.28*	-0.28*	0.60***	0.60***	0.37*	0.37*	-0.30*	-0.30*	0.18	0.18
	(0.11)	(0.11)	(0.11)	(0.12)	(0.18)	(0.18)	(0.15)	(0.15)	(0.13)	(0.13)	(0.14)	(0.14)
Age		0.05		0.06		-0.03		-0.24**		0.11†		-0.10
		(0.09)		(0.07)		(0.07)		(0.09)		(0.06)		(0.09)
Gender		-0.02		-0.14		-0.02		-0.25		-0.09		0.20
		(0.19)		(0.16)		(0.20)		(0.21)		(0.19)		(0.24)
Prior breach		0.18		0.30†		-0.27		-0.23		0.10		-0.28
		(0.18)		(0.16)		(0.18)		(0.19)		(0.16)		(0.21)
FB friends		0.10		0.21**		-0.24**		-0.25**		0.10		-0.19†
		(0.10)		(0.08)		(0.09)		(0.10)		(0.07)		(0.10)
FB frequency		0.65***		0.23*		-0.29**		-0.31**		0.28**		-0.41**
		(0.11)		(0.09)		(0.10)		(0.12)		(0.11)		(0.13)
FB hours		0.14†		0.27**		-0.19*		-0.06		0.20*		-0.02
		(0.08)		(0.09)		(0.08)		(0.09)		(0.10)		(0.09)
Constant	5.14***	1.45*	3.88***	1.21*	4.39***	7.36***	3.35***	7.17***	4.64***	2.34***	3.26***	6.02***
	(0.13)	(0.72)	(0.11)	(0.56)	(0.14)	(0.57)	(0.14)	(0.67)	(0.11)	(0.47)	(0.14)	(0.65)
R^2	0.022	0.264	0.026	0.239	0.041	0.194	0.037	0.167	0.015	0.168	0.007	0.119

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 668 for all models. Post is a dummy variable for the 2nd survey round, Victim is a dummy variable for individuals who stated being breached in the 2nd survey round. OSN = online social network. FB = Facebook. Robust standard errors clustered by respondent in parentheses.

Appendix B7: Main Model with Users Only Breached Through Friends

Table B-12: Effect of being an actual data breach victim on only those respondents who were breached by a friend

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	(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	0.11	-0.34†	0.13	-0.21	-0.22	0.11	0.08	0.36†	0.19	-0.10	-0.15	0.19
	(0.21)	(0.18)	(0.18)	(0.17)	(0.20)	(0.20)	(0.23)	(0.21)	(0.17)	(0.17)	(0.22)	(0.20)
Victim × Post	-0.14	-0.14	-0.29*	-0.29*	0.62**	0.62**	0.41**	0.41**	-0.43**	-0.43**	0.15	0.15
	(0.13)	(0.13)	(0.11)	(0.11)	(0.20)	(0.20)	(0.15)	(0.15)	(0.13)	(0.14)	(0.14)	(0.14)
Age		0.10		0.10		0.01		-0.19*		0.12*		-0.13†
		(0.07)		(0.06)		(0.07)		(0.08)		(0.05)		(0.07)
Gender		-0.10		-0.10		0.13		-0.05		-0.10		0.34†
		(0.17)		(0.14)		(0.17)		(0.19)		(0.13)		(0.18)
Prior breach		0.20		0.30*		-0.30†		-0.34*		0.15		-0.40*
		(0.16)		(0.13)		(0.16)		(0.17)		(0.12)		(0.16)
FB friends		0.13†		0.18**		-0.14†		-0.10		0.13*		-0.16*
		(0.07)		(0.06)		(0.07)		(0.08)		(0.06)		(0.08)
FB frequency		0.61***		0.23**		-0.25**		-0.32**		0.31***		-0.48***
		(0.10)		(0.07)		(0.09)		(0.10)		(0.07)		(0.09)
FB hours		0.14†		0.24**		-0.25*		-0.12		0.14		-0.06
		(0.08)		(0.08)		(0.10)		(0.10)		(0.09)		(0.09)
Constant	4.74***	1.53***	3.65***	1.25**	4.68***	6.63***	3.66***	6.53***	4.33***	2.13***	3.52***	6.32***
	(0.10)	(0.51)	(0.08)	(0.41)	(0.10)	(0.50)	(0.11)	(0.55)	(0.08)	(0.39)	(0.10)	(0.52)
R^2	0.001	0.238	0.002	0.176	0.015	0.131	0.014	0.112	0.004	0.162	0.002	0.165

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 706 for all models. Post is a dummy variable for the 2nd survey round, Victim is a dummy variable for individuals who stated being breached in the 2nd survey round. OSN = online social network. FB = Facebook. Robust standard errors clustered by respondent in parentheses.

Appendix B8: Split Sample Analyses Using Alternative Facebook Use Variables

Table B-13: Heterogeneity of effect across Number of FB use frequency												
	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	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	-0.11	-0.29*	-0.19	-0.29*	0.59†	0.58**	0.44†	0.33†	-0.45*	-0.30*	0.19	0.16
	(0.20)	(0.13)	(0.17)	(0.13)	(0.30)	(0.20)	(0.24)	(0.17)	(0.19)	(0.14)	(0.29)	(0.15)
N	292	468	292	468	292	468	292	468	292	468	292	468
R^2	0.145	0.081	0.068	0.143	0.095	0.105	0.110	0.113	0.110	0.059	0.131	0.065

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. Post is a dummy variable for the 2nd survey round, Victim is a dummy variable for individuals who stated that they were breached in the Cambridge Analytica breach in the 2nd survey round. OSN = online social network. FB = Facebook. Robust standard errors clustered by respondent in parentheses. Regressions include terms for Victim, Post, Age, Gender, Prior breach, FB friends, FB frequency, and FB hours. Constant and control variables are omitted for brevity.

Appendix B9: Measurement Invariance

Measurement invariance establishes that the same construct is being measured at different points in time (Ployhart and Vandenberg 2010). In table B-14 below, we find all our measures to exhibit configural invariance (i.e., all constructs underlie the same measures across periods). All of our measures except perceived breach also exhibit metric invariance (i.e., all items are similarly calibrated to constructs over time). As metric invariance can be a demanding requirement, especially over longer periods (Horn and McArdle 1992), we nonetheless retain perceived breach for the analysis.

Table B-14: Measurement invariance

Construct	Model	Log-likelihood ratio	D.f.	P > χ2	CFI	TLI	RMSEA	SRMR
Continuance intention	Configural	-2391.69	51		0.988	0.979	0.084	0.018
	Metric	-2393.30	45	0.7836	0.989	0.983	0.076	0.024
Trust	Configural	-2989.68	51		0.991	0.985	0.054	0.046
	Metric	-2991.08	45	0.8339	0.993	0.989	0.046	0.049
Perceived breach	Configural	-2580.20	39		0.986	0.966	0.092	0.040
	Metric	-2590.16	35	0.0005***	0.976	0.955	0.107	0.068
Feelings of violation	Configural	-2736.62	39		0.994	0.987	0.054	0.017
	Metric	-2733.49	35	0.1813	0.993	0.987	0.055	0.035
OSN belongingness	Configural	-5909.66	99		0.953	0.942	0.075	0.039
	Metric	-5912.82	85	0.9578	0.954	0.947	0.071	0.042
OSN anxiety	Configural	-2663.85	39		0.980	0.952	0.104	0.038
	Metric	-2667.88	35	0.0893	0.977	0.957	0.098	0.047

CFI = Comparative Fit Index, TLI = Tucker–Lewis Index, RMSEA = Root Mean Square Error of Approximation, SRMR = Standardized Root Mean Square Residual

Appendix B10: Power Analysis for Third Survey Round

For the sample in the third survey round, we used GPower 3.1 to conduct a power analysis identical to that for RQ1. Our sample size of 183 is sufficient to detect a medium-sized effect ($f^2 = 0.15$) with an error probability of $\alpha = 0.05$ (Cohen 1988) at a power of 0.96, remaining well above the accepted threshold of 0.80. We also conducted a sensitivity analysis with the effect size as outcome variable, which revealed that the sample is sufficient to detect effect sizes above 0.09 at a power of at least 0.80. Thus, the sample appears robustly powered from an ex-ante perspective, as it is powerful enough to detect both medium-sized effects ($f^2 = 0.15$) at a very high power level (0.96), and can even detect somewhat smaller effect sizes ($f^2 = 0.09$) at a power level commonly considered sufficient (0.80).

Appendix B11: Growth Curve Modeling

For robustness, we replace our panel OLS estimator for the effect over three periods with a growth curve modeling technique, specifically a random coefficient model (RCM) (Bliese and Ployhart 2002). This is a multilevel maximum likelihood estimator, in which the first level regresses the dependent variable on time period dummy variables, and the second level adds explanatory variables. While growth curve modeling techniques are usually seen in studies of relationships between stable factors over time (Ployhart and Vandenberg 2010), building an RCM involves a rigorous model construction process that investigates how precisely the dependent variable changes over time. We believe that this is instructive to better understand the role of time in our study. For brevity, the exact values of each model building stage are not reported in tabular form.

Bliese and Ployhart (2002) recommend first building the level 1 model of the relationship of the dependent variable with time. In step 1, the dependent variable is regressed on the time variable in model allowing for random intercept variation per respondent, and this regression is then tested for residual intraclass correlation. Unsurprisingly, the test for residual intraclass correlation showed high amounts of nonindependence for all six outcome variables, indicating that the model with intercept variation is adequate (this corresponds to an OLS fixed effects model).

In step 2, a quadratic term of the time variable is added to the model to test for nonlinear effects of time. If the added term is statistically significant, it is retained, otherwise it is dropped. In our models, the quadratic term is non-significant for all outcome variables. As the quadratic term prevents model convergence in later stages, we decided not to retain it. Ultimately, we do not proceed with quadratic time terms for any models.

In step 3, the slope is also allowed to vary for each respondent individually. Then, a likelihood ratio test is used to compare whether the model with slope variation fits the data significantly better than the model intercept variation only. In our outcome variables, slope variation outperforms intercept variation for continuance intention ($p < 0.001$), perceived breach ($p = 0.02$), and OSN anxiety ($p = 0.04$), for which we adopt slope variation. For the other variables, we continue with intercept variation only.

In step 4, the error structure is varied to compare between residuals that are uncorrelated and homoscedastic over time (the default), autoregressive, and correlated and heteroskedastic over time. Likelihood ratio tests are again used to compare the model performance between the models with different error structures. Here, trust, feelings of violation, OSN belongingness, and OSN anxiety show no performance improvements with any error structure over the default uncorrelated and homoscedastic residuals. Continuance intention shows improved performance with autocorrelated residuals and perceived breach with correlated and heteroskedastic residuals. This indicates that autocorrelation and heteroskedasticity does not appear to play a major role for most of our variables, except for continuance intention and perceived breach. This is instructive but does not meaningfully affect the interpretation of our OLS results, since we already employ cluster-robust standard errors that account for within-respondent residual autocorrelation.

In level 2, the explanatory variables (the victim indicator and its interaction with the time variable) are added to the model that emerged with the best fit from the four steps of level 1. Table B-15 shows the results. As this table shows, we obtain consistent results as compared to the three-period panel OLS model. Overall, this demonstrates that our results hold true even under different modeling assumptions regarding the change over time.

Table B-15: Effect of being an actual data breach victim with a third survey round modeled via a random coefficient model												
	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	(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)	(0.12)	(0.12)	(0.11)	(0.11)	(0.08)	(0.08)	(0.09)	(0.09)
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)	(0.08)	(0.12)	(0.12)	(0.11)	(0.11)	(0.08)	(0.08)	(0.10)	(0.10)
Victim	-0.30	-0.58*	-0.23	-0.50*	0.29	0.53*	0.35	0.56*	0.02	-0.20	0.22	0.41
	(0.28)	(0.26)	(0.22)	(0.21)	(0.27)	(0.25)	(0.30)	(0.29)	(0.22)	(0.21)	(0.28)	(0.26)
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)	(0.15)	(0.15)	(0.22)	(0.22)	(0.20)	(0.20)	(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)	(0.19)	(0.15)	(0.16)	(0.23)	(0.23)	(0.20)	(0.20)	(0.16)	(0.16)	(0.19)	(0.20)
Age		0.05		0.03		0.10		-0.08		0.07		-0.04
		(0.09)		(0.07)		(0.09)		(0.10)		(0.07)		(0.10)
Gender		0.19		-0.11		-0.25		-0.38		-0.09		0.00
		(0.23)		(0.18)		(0.22)		(0.25)		(0.18)		(0.23)
Prior breach		-0.04		0.25		-0.28		-0.22		-0.07		-0.17
		(0.21)		(0.17)		(0.21)		(0.23)		(0.17)		(0.22)
FB friends		0.08		0.19*		-0.09		-0.09		0.13		-0.12
		(0.10)		(0.08)		(0.10)		(0.11)		(0.08)		(0.11)
FB frequency		0.56***		0.17†		-0.26*		-0.29*		0.28**		-0.50***
		(0.12)		(0.09)		(0.12)		(0.13)		(0.09)		(0.12)
FB hours		0.22		0.34**		-0.36*		-0.20		0.21†		0.08
		(0.16)		(0.12)		(0.15)		(0.17)		(0.12)		(0.16)
Intercept	5.04***	2.01**	3.80***	1.75***	4.47***	6.73***	3.43***	6.23***	4.52***	2.75***	3.20***	5.60***
	(0.15)	(0.66)	(0.12)	(0.53)	(0.14)	(0.65)	(0.16)	(0.73)	(0.12)	(0.53)	(0.15)	(0.69)
Individual variation	Slope + Intercept		Intercept only		Slope + Intercept		Intercept only		Intercept only		Slope + Intercept	
Standard errors	Autocorrelated		Uncorrelated and homoskedastic		Correlated and heteroskedastic		Uncorrelated and homoskedastic		Uncorrelated and homoskedastic		Uncorrelated and homoskedastic	

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 549 for all models. Post and Post_6mo are dummy variables for the 2nd and 3rd data collection rounds, respectively. Victim is a dummy variable for individuals breached in the 2nd data collection round. OSN = online social network. FB = Facebook.

Appendix C: Study 2

Appendix C1: Survey Procedure Texts

In the first survey round, participants were presented with a text describing their history with the fictitious OSN SocialNet. This text served as the manipulation, differentiating between the high and low lock-in condition. The full text for each condition is presented below:

High lock-in:

> Imagine that you have many connections on SocialNet. Most of your friends do not use any platform other than SocialNet, making it difficult to stay in touch with them elsewhere. You have shared many photos, posts, and messages on SocialNet. Few other platforms offer the same features or user base, making it difficult to move your content and connections elsewhere. If you decide to leave SocialNet, you would find it difficult to migrate your content and continue your online interactions with your friends.

Low lock-in:

> Imagine that you have few connections on SocialNet. Most of your friends use multiple other platforms in addition to SocialNet, making it easy to stay in touch with them elsewhere. You have only shared a few posts, photos, and messages on SocialNet. Several other platforms offer the same features or user base, making it easy to move your content and connections elsewhere. If you decide to leave SocialNet, you would find it easy to migrate your content and continue your online interactions with your friends.

Immediately afterward, participants were presented with a data breach notification modeled after FB's. This is the notification text:

> Over the last days, you have heard media reporting about a large data breach at SocialNet. An app on SocialNet harvested profile data and used it for political advertising. SocialNet had previously removed this app without notifying the public or affected users. Today, you log in to SocialNet and see the following notification:

⚠ **Security Alert:** Based on our ongoing investigation, it appears that the following app banned by SocialNet 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?**
Digital You	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 second survey round, the lock-in texts from the first survey round were repeated to ensure saliency concerning the respondents' conditions. On the next page, the text differed between the proximal and distal condition.

Proximal:

One week ago, you heard media reporting about a large data breach at SocialNet. An app on SocialNet had harvested profile data and used it for political advertising. SocialNet had previously removed this app without notifying the public or affected users. After hearing about the breach, you logged in to SocialNet and saw the following notification.

⚠ **Security Alert:** Based on our ongoing investigation, it appears that the following app banned by SocialNet 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?**
Digital You	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.

Now, **one week** has passed since you received this notification.

Distal:

Six months ago, you heard media reporting about a large data breach at SocialNet. An app on SocialNet had harvested profile data and used it for political advertising. SocialNet had previously removed this app without notifying the public or affected users. After hearing about the breach, you logged in to SocialNet and saw the following notification.

⚠ **Security Alert:** Based on our ongoing investigation, it appears that the following app banned by SocialNet 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?**
Digital You	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.

Now, **six months** have passed since you received this notification.

Appendix C2: Survey Items

The survey items for the outcome variables and demographic variables were reused from Study 1 and solely adapted by replacing "Facebook" with "SocialNet". They can be found in Appendix B2.

Table C-1: Survey items

Construct	Item	Question	Source
Procedural costs	Procedural1	If I left SocialNet, I might have to learn new routines and ways of doing things.	Jones et al. (2007)
	Procedural2	If I left SocialNet, it might be a real hassle.	
	Procedural3	If I left SocialNet, I might have to spend a lot of time setting up a new account somewhere else.	
Social Switching costs	Social1	If I left SocialNet, I might lose the friendships I have developed at SocialNet.	Jones et al. (2007)
	Social2	If I left SocialNet, I might lose an important personal relationship at SocialNet.	
	Social3	If I left SocialNet, It might be very uncomfortable to tell friends at SocialNet that I am leaving.	
Conflict	Conflict1	To what extent did you feel conflicted when deciding to continue using SocialNet?	Vaidis et al. (2024)
Discomfort	Discomfort1	To what extent did you feel uncomfortable when deciding to continue using SocialNet?	

Appendix C3: Power Analysis, Sample Selection and Filtering

We used GPower 3.1 to conduct a power analysis to motivate our sampling process. The analysis showed that, to detect a medium-sized effect ($f^2 = 0.15$) with an error probability of $\alpha = 0.05$ at a power level of 0.80 (defaults as per Cohen 1988), our regression models would require a sample of 92, whereas detecting a small effect ($f^2 = 0.02$) at the same α and power level would require a sample of 647. Thus, to be able to detect small effects at sufficiently high power levels, we aimed for an initial sample of 900 respondents, or 225 per condition. This would allow us to achieve sufficient power to detect small effect sizes even after allowing for sample attrition between rounds and failed attention checks (see Frank et al. 2025).

On Prolific, we aimed to recruit 900 respondents who resided in the U.S., had an approval rate above 95% and had at least 50 previous submissions. Since Prolific filled the spots of respondents that timed out or that returned their submission automatically, we had a total of 1,020 attempted responses. Of the 1,020 respondents, 940 completed the survey, of which 827 correctly answered all three attention checks.

The 827 respondents who correctly completed the survey and did not fail any attention check were then invited to the second survey round. Of them, 205 were in the low lock-in proximate condition, 215 in high lock-in proximate, 202 in low lock-in distal, and 205 in high lock-in distal. Across all groups, 735 unique respondents returned to the second survey.[3] 721 respondents finished the survey and 672 respondents correctly answered all three attention checks. Finally, we removed all respondents with a *Q_RecaptchaScore* lower than 0.5 in any of the two survey rounds[4], leading to the final sample of 653. The final sample's makeup across the four experimental groups can be seen in Figure 4 of the main manuscript.

[3] We found no evidence that the respondents who entered the second survey were systematically different from those invited that did not return except that respondents who did not return rated slightly higher on trust (4.08 vs. 3.70, $p = 0.02$, $t = 2.34$).

[4] According to Qualtrics, these respondents are likely to be bots. See https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/fraud-detection/.

Appendix C4: Descriptive and Demographic Statistics

Table C-2: Descriptive statistics									
	Round 1			Round 2			Difference (Round 1 - Round 2)		
	α	Mean	SD	α	Mean	SD	b	t	p
Continuance intention	0.98	3.27	1.83	0.98	3.45	1.79	-0.18†	(-1.817)	0.07
Trust	0.92	3.63	1.47	0.92	3.58	1.48	0.05	(0.605)	0.55
Perceived breach	0.95	5.05	1.70	0.95	5.02	1.62	0.03	(0.288)	0.77
Feelings of violation	0.93	4.26	1.76	0.93	4.18	1.71	0.08	(0.793)	0.43
OSN belongingness	0.96	4.90	1.29	0.97	4.88	1.34	0.03	(0.386)	0.70
OSN anxiety	0.93	4.40	1.72	0.93	4.39	1.65	0.01	(0.088)	0.93
Procedural switching cost	0.87	4.39	1.71	0.90	4.42	1.77	-0.03	(-0.345)	0.73
Social switching cost	0.89	4.10	1.70	0.87	4.13	1.68	-0.03	(-0.338)	0.74
Age		42.18	13.93						
Gender		1.56	0.54						
Prior breach		1.62	0.49						

† $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. n = 653 for both round 1 and round 2. α = inter-item reliability. OSN = online social network.

Table C-3: Demographic statistics for each group			
	Age	Gender	Prior breach
Low Lock-in + Proximal (n = 169)	40.41	1.54	1.61
Low Lock-in + Distal (n = 145)	43.35	1.55	1.58
High Lock-in + Proximal (n = 173)	43.51	1.59	1.62
High Lock-in + Distal (n = 166)	41.57	1.54	1.65
ANOVA Results	$p > 0.10$, F = 1.89	$p > 0.10$, F = 0.32	$p > 0.10$, F = 0.56

Appendix C5: Correlation Tables

Table C-4: Correlation table for round 1

No		1	2	3	4	5	6	7	8	9	10	11	12	13
1	Locked	1.00												
2	Distal	0.03	1.00											
3	Continuance intention	0.33***	0.06	1.00										
4	Trust	0.15***	0.07†	0.66***	1.00									
5	Perceived breach	-0.16***	-0.05	-0.67***	-0.61***	1.00								
6	Feelings of violation	-0.12**	-0.11**	-0.64***	-0.57***	0.80***	1.00							
7	OSN belongingness	0.24***	0.05	0.49***	0.53***	-0.33***	-0.36***	1.00						
8	OSN anxiety	-0.14***	-0.11**	-0.63***	-0.57***	0.77***	0.82***	-0.34***	1.00					
9	Age	0.03	0.02	0.03	-0.03	0.07†	-0.02	0.06	0.04	1.00				
10	Gender	0.02	-0.02	-0.05	-0.06	0.05	0.01	-0.02	0.03	0.05	1.00			
11	Prior breach	0.04	0.00	-0.01	-0.12**	0.06	0.02	-0.04	0.08*	0.11**	0.07†	1.00		
12	Procedural cost	0.48***	-0.00	0.39***	0.28***	-0.16***	-0.08†	0.42***	-0.08*	0.04	-0.01	-0.01	1.00	
13	Social switching cost	0.43***	-0.04	0.40***	0.33***	-0.20***	-0.09*	0.45***	-0.12**	0.01	-0.03	-0.06	0.82***	1.00

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 653. OSN = online social network.

Table C-5: Correlation table for round 2

No		1	2	3	4	5	6	7	8	9	10	11	12	13
1	Locked	1.00												
2	Distal	0.03	1.00											
3	Continuance intention	0.32***	0.04	1.00										
4	Trust	0.11**	0.05	0.66***	1.00									
5	Perceived breach	-0.09*	-0.05	-0.63***	-0.65***	1.00								
6	Feelings of violation	-0.03	-0.10*	-0.57***	-0.61***	0.80***	1.00							
7	OSN belongingness	0.25***	0.02	0.48***	0.45***	-0.27***	-0.28***	1.00						
8	OSN anxiety	-0.06	-0.06	-0.62***	-0.62***	0.76***	0.83***	-0.25***	1.00					
9	Age	0.03	0.02	0.07†	-0.02	0.06	-0.08*	0.08*	-0.02	1.00				
10	Gender	0.02	-0.02	-0.04	-0.05	0.10**	0.06	-0.02	0.06	0.05	1.00			
11	Prior breach	0.04	0.00	-0.03	-0.11**	0.09*	0.03	-0.07†	0.07†	0.11**	0.07†	1.00		
12	Procedural cost	0.48***	-0.00	0.42***	0.30***	-0.15***	-0.04	0.48***	-0.09*	0.06	0.02	-0.01	1.00	
13	Social switching cost	0.46***	-0.01	0.43***	0.33***	-0.18***	-0.06	0.51***	-0.10*	-0.02	-0.00	-0.05	0.83***	1.00

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 653. OSN = online social network.

Appendix C6: Mediated Pathways of Lock-in Through Switching Costs

To better understand the psychological processes through which lock-in influences continuance intention and attitudes, we investigated the mediating roles of social and procedural switching costs. Social switching costs are the loss of social bonds and friendships that switching may entail, whereas procedural costs concern the time and effort of switching providers itself (Jones et al. 2007). Given that our lock-in manipulation was designed to directly vary the perceived difficulty of leaving the OSN, we theorized that these switching costs—the sacrifices consumers feel when moving between providers—would serve as a mediating mechanism. Table C-7 shows the significant direct effects of lock-in on both types of switching costs both for the baseline configuration shown in Table 10, as well as for the addition of the distal variable and the matched sample from Appendix C8.

Table C-6: Effect of treatments on mediators

	Social switching costs			Procedural costs		
	Base	Base+Distal	Base+Di.+CEM	Base	Base+Distal	Base+Di.+CEM
	(1)	(2)	(3)	(4)	(5)	(6)
2nd_round	0.00	-0.04	0.00	-0.00	0.00	0.02
	(0.09)	(0.10)	(0.11)	(0.09)	(0.11)	(0.12)
Locked	1.47***	1.48***	1.48***	1.63***	1.63***	1.66***
	(0.12)	(0.12)	(0.13)	(0.12)	(0.12)	(0.12)
2nd_round × Locked	0.06	0.06	0.07	0.07	0.07	0.05
	(0.11)	(0.11)	(0.12)	(0.12)	(0.12)	(0.12)
Distal		-0.18	-0.13		-0.05	-0.02
		(0.12)	(0.13)		(0.12)	(0.12)
2nd_round × Distal		0.09	0.04		-0.01	-0.01
		(0.11)	(0.11)		(0.11)	(0.12)
Constant	3.34***	3.42***	3.37***	3.54***	3.57***	3.52***
	(0.10)	(0.11)	(0.11)	(0.09)	(0.11)	(0.11)
N	1,306	1,306	1,300	1,306	1,306	1,300
R^2	0.197	0.199	0.200	0.230	0.230	0.237

† $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$. 2nd_round is a dummy variable for the 2nd data collection round, Locked is a dummy variable for the high lock-in condition, Distal is a dummy variable for the distal condition of the 2nd data collection round. Robust standard errors clustered by respondent in parentheses.

Next, we employed Hayes's PROCESS macro (Model 4, Release 5) for R (Hayes 2022). Given that Release 5 supports cluster-robust standard errors (using the *cluster* and *robustse* options), we clustered standard errors at the respondent level. Columns 1 and 2 of Table C-8 indicate that social switching costs significantly mediate the relationship between lock-in and continuance intention, trust, perceived breach, OSN belongingness, and OSN anxiety (indicated by 95% confidence intervals (CIs) excluding zero). Procedural costs, however, showed a significant mediating role only for continuance intention and OSN belongingness. We observed partial mediation for continuance intention and perceived breach (i.e., the significant direct effects of lock-in persisted; columns 3 and 4). In contrast, we found full mediation for trust, OSN belongingness, and OSN anxiety (i.e., the direct effects of lock-in became non-significant; $p > 0.05$). Notably, feelings of violation was the sole variable for which no significant indirect effect through either type of switching costs was found.

To further probe these indirect effects, we contrasted their strength through social versus procedural switching costs. We performed this contrast by constructing CIs around the difference between the indirect effects using bootstrap estimates. Columns 5 and 6 reveal that lock-in operates more strongly through social switching costs than through procedural costs in affecting trust (95% CIs excluding zero). This suggests that lock-in's influence, particularly on trust, is predominantly driven by the discomfort of losing social contacts rather than the effort of switching platforms.

Table C-7: Direct effects, indirect effects, and contrasts for mediation									
Independent variable	Mediator	Dependent variable	Indirect effect (1)	95% CI (2)	Direct effect (3)	95% CI (4)	Contrast (5)	95% CI (6)	Type of mediation
Locked	Social	Continuance intention	0.38	[0.22, 0.55]	0.60***	[0.32, 0.88]	0.15	[-0.15, 0.46]	Partial
	Procedural		0.23	[0.07, 0.39]					
	Social	Trust	0.38	[0.24, 0.52]	-0.03	[-0.26, 0.21]	0.28	[0.04, 0.54]	Full
	Procedural		0.10	[-0.04, 0.23]					
	Social	Perceived breach	-0.25	[-0.42, -0.10]	-0.31*	[-0.60, -0.02]	-0.27	[-0.56, 0.01]	Partial
	Procedural		0.02	[-0.14, 0.18]					
	Social	Feelings of violation	-0.13	[-0.29, 0.02]	-0.35*	[-0.65, -0.06]	-0.19	[-0.50, 0.10]	Not significant
	Procedural		0.06	[-0.11, 0.23]					
	Social	OSN belongingness	0.39	[0.28, 0.52]	0.01	[-0.19, 0.21]	0.19	[-0.01, 0.40]	Full
	Procedural		0.20	[0.08, 0.32]					
	Social	OSN anxiety	-0.19	[-0.35, -0.03]	-0.22	[-0.48, 0.04]	-0.27	[-0.57, 0.03]	Full
	Procedural		0.08	[-0.09, 0.24]					

* p < 0.05, ** p < 0.01, *** p < 0.001. n = 1,306. Confidence intervals (CI) for indirect effects and contrasts are based on 5,000 bootstrap samples. In each model, 2nd_round, 2nd_round x Locked, Distal, and 2nd_round x Distal were entered as covariates. Results remain highly consistent when we exclude 2nd_round x Locked to assess the effect of Locked across both rounds. We use robust standard errors clustered at the respondent level. Social = social switching costs, Procedural = procedural costs.

Appendix C7: Reconciling Study 1 and Study 2

We compare our Study 2 findings to those of Study 1 to assess the external validity. To ensure comparability with Study 2, we focused exclusively on participants in Study 1 who were victims of a breach by a friend, mirroring our manipulation in Study 2. We used daily FB hours and FB frequency as proxy measures for "lock-in" status, dichotomizing both variables at their respective medians in Round 1. We then interacted these variables with the third-round indicator. Due to the limited subsample (n = 35 victims), the analysis is underpowered, yielding only two statistically significant interactions (see Appendix C7). Users with high daily FB hours exhibited significantly less attitude regression (i.e., less improvement in their continuance intention) compared to their low-use peers. Results for users with high FB frequency show a consistent pattern with respect to their attitude regression for perceived breach compared to low-frequency users.

Table C-8: Effect of FB hours and FB frequency on victims' breach reactions over time (Study 1, Rounds 2 and 3)												
	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	(1)	(2)	(3)	(4)	(5)	**(6)**	(7)	(8)	(9)	(10)	(11)	(12)
Post_6mo	**0.39**†	0.17	0.22	0.32*	-0.01	**-0.48**	-0.29	-0.41†	0.27	0.12	0.03	-0.06
	(0.20)	(0.21)	(0.13)	(0.13)	(0.21)	**(0.29)**	(0.22)	(0.21)	(0.21)	(0.16)	(0.19)	(0.17)
Hours	**0.86**		0.24		0.03		-0.51		-0.21		0.87	
	(0.70)		(0.43)		(0.64)		(0.73)		(0.61)		(0.58)	
Post_6mo x Hours	**-0.62***		0.17		-0.76		-0.00		-0.08		0.12	
	(0.30)		(0.28)		(0.61)		(0.47)		(0.31)		(0.33)	
Freq		-0.14		-0.14		**-0.26**		0.30		-0.26		0.09
		(0.69)		(0.46)		**(0.68)**		(0.69)		(0.56)		(0.60)
Post_6mo x Freq		0.18		-0.15		**0.78**†		0.32		0.39		0.34
		(0.35)		(0.27)		**(0.42)**		(0.43)		(0.40)		(0.35)
R^2	**0.028**	0.005	0.023	0.017	0.020	**0.016**	0.021	0.022	0.012	0.011	0.062	0.008

† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. n = 70. Hours [Freq] is a dummy variable that equals one if the number of FB hours [FB frequency] in round 1 is above the sample median. The sample includes responses from Study 1, rounds 2 and 3, from all 35 victims who were breached by a friend and completed all three survey rounds. OSN = online social network. Robust standard errors clustered by respondent in parentheses. Constant omitted for brevity.

Appendix C8: Results Including Distal Values

Table C-9: Results including distal values

	Continuance intention		Trust		Perceived breach		Feelings of violation		OSN belongingness		OSN anxiety	
	Base+Distal	CEM	Base+Distal	CEM	Base+Distal	CEM	Base+Distal	CEM	Base+Distal	CEM	Base+Distal	CEM
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
2nd_round	0.25*	0.17†	0.05	0.01	-0.16	-0.09	-0.26**	-0.17†	-0.03	-0.10	-0.22*	-0.15
	(0.10)	(0.10)	(0.09)	(0.09)	(0.10)	(0.10)	(0.10)	(0.10)	(0.09)	(0.09)	(0.10)	(0.10)
Locked	1.21***	1.18***	0.44***	0.40***	-0.54***	-0.55***	-0.42**	-0.41**	0.61***	0.61***	-0.46***	-0.53***
	(0.13)	(0.14)	(0.11)	(0.12)	(0.13)	(0.13)	(0.14)	(0.14)	(0.10)	(0.10)	(0.13)	(0.14)
2nd_round × Locked	-0.06	-0.01	-0.13	-0.09	0.24†	0.25*	0.32**	0.35**	0.06	0.07	0.26*	0.33**
	(0.12)	(0.12)	(0.10)	(0.10)	(0.12)	(0.13)	(0.12)	(0.13)	(0.10)	(0.10)	(0.12)	(0.13)
Distal	0.18	0.03	0.19†	0.08	-0.17	0.03	-0.38**	-0.06	0.12	0.01	-0.36**	-0.09
	(0.14)	(0.14)	(0.11)	(0.11)	(0.13)	(0.13)	(0.14)	(0.14)	(0.10)	(0.10)	(0.13)	(0.14)
2nd_round × Distal	-0.08	-0.03	-0.06	-0.05	0.02	-0.06	0.04	-0.07	-0.08	-0.00	0.16	0.05
	(0.12)	(0.12)	(0.10)	(0.10)	(0.12)	(0.13)	(0.12)	(0.13)	(0.10)	(0.10)	(0.12)	(0.13)
N	1,306	1,300	1,306	1,300	1,306	1,300	1,306	1,300	1,306	1,300	1,306	1,300
R^2	0.110	0.108	0.021	0.016	0.020	0.018	0.019	0.008	0.061	0.061	0.019	0.014

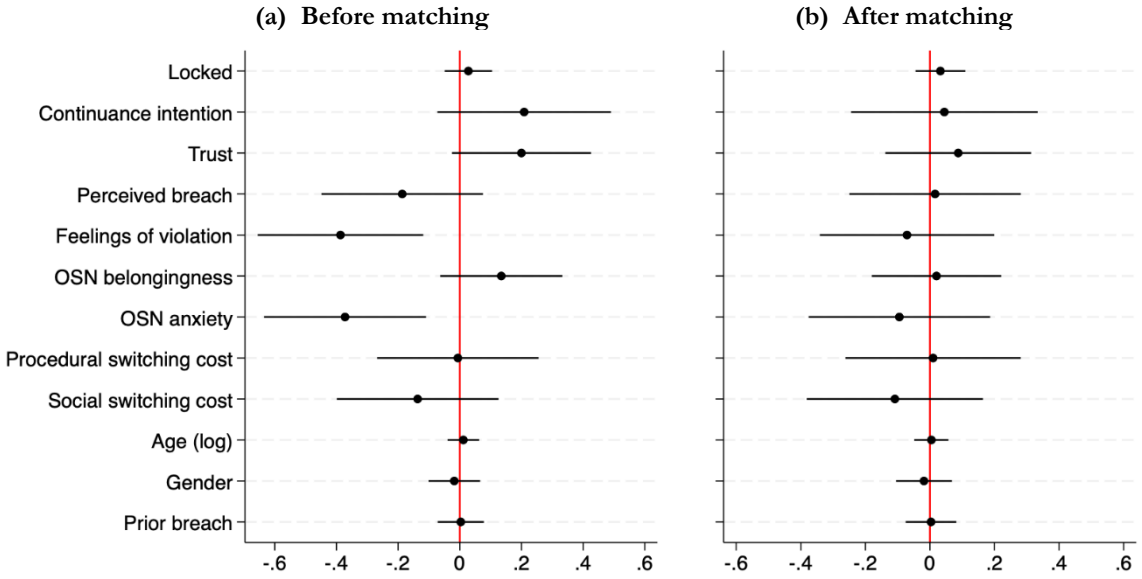
† p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001. 2nd_round is a dummy variable for the 2nd data collection round, Locked is a dummy variable for the high lock-in condition, Distal is a dummy variable for the distal condition. OSN = online social network. Robust standard errors clustered by respondent in parentheses. CEM = coarsened exact matching. Constant omitted for brevity.

Appendix C9: Response Rates and Matching for Distal and Proximal

We assess the robustness of the comparison between the proximal and distal groups. First, a potential concern regarding this comparison is that the observed effects might be influenced by differential response rates between the two groups. Fortunately, we observed only small imbalances: 81.4% of those invited to the proximal group were retained, compared to 76.4% in the distal group ($p = 0.07$, $\chi^2 = 3.13$). This indicates that differential response rates are not a significant concern in our analysis.

Second, we found baseline imbalances between proximal and distal respondents in Round 1 for perceived breach, feelings of violation, and OSN anxiety (Figure C-1a). To rule out any systematic differences of these baseline imbalances on our results, we conducted a robustness check using coarsened exact matching (CEM; see Burtch et al. 2022). This ensured comparability between participants in the distal and proximal conditions. We employed the *cem* package in Stata, matching on perceived breach, feelings of violation, and OSN anxiety, using four equally spaced cut points (e.g., Forderer and Burtch 2025; Wang et al. 2022). To retain as many participants as possible, we utilized weighted regressions instead of one-to-one (k2k) matching (e.g., Wang et al. 2022).

To check for balance post-matching, and since Stata's *ttest* command does not support weights, we ran separate linear regressions where each variable was regressed on the *Distal* dummy indicator (1 for the distal sample, 0 for the proximal sample). Figure C-1 visualizes the coefficients before matching (full sample) and after matching (CEM-weighted sample). Evidently, while significant differences were observed before matching, the *Distal* coefficient became substantially closer to zero and non-significant for all variables post-matching (Figure C-1b). Finally, we applied these weights to the full sample across both rounds and re-ran our original regressions (see even columns in Table C-9). The results remained consistent, suggesting that pre-treatment imbalances are unlikely to be a concern in our analysis.



Note: This figure reports the estimated coefficients (and respective 95 percent confidence intervals) from the regressions of the variables shown on the left on a *Distal* dummy indicator in the first survey round. Figure C-1a reports the results before matching and Figure C-1b reports the results using a CEM weighted regression after matching.

Figure C-1: Coefficients for baseline differences between distal and proximal samples before and after matching

Appendix D: Qualitative Evidence from Interviews

To further assess the above theoretical interpretation, we conducted 21 semi-structured interviews with actual breach victims one year after the breach. We recruited respondents via MTurk and screened them for their actual breach victim status.

Recruitment. We developed an interview guide with questions on respondents' Facebook use behavior, belongingness, blame attribution, reaction to the notification, trust, continuance intention, behavior changes, opinions of and trust in Facebook, and stances towards compensation. The interview guide was tested in two pilot interviews recruited from the original sample pool of MTurk users who had responded to all three survey rounds. After the interview, pilot interviewees were asked about the appropriateness and comprehensiveness of the interview guide, and based on their feedback the guide was extended with questions focused on feelings of betrayal and previous considerations to leave Facebook. As the pilot interviewees were only informed of their pilot status after the interview, their responses were retained in the data analysis.

We recruited the interviewees through a survey on Amazon MTurk, sent to Americans with at least 100 fulfilled tasks and an approval rate of at least 99 percent. Survey respondents were guided to the Facebook page displaying the breach notification and asked to upload a screenshot of the page. If they were affected, they could provide their email address for a follow-up interview. Out of 95 responses, 48 were affected by the breach, 41 of which provided their email addresses. 19 of them completed the interview. The responses of these 19 interviewees were added to those of the two pilot interviewees to form the overall interview sample of 21. Interviews took 30 to 50 minutes, were organized via Skype or Hangouts audio calls, and the interviewees were paid $10 in the form of an MTurk bonus. We followed the interview guidelines of Myers and Newman (2007) to ensure high quality and a shared understanding of the responses. All interviews took place between March 7 and April 26, 2019, with a last confirmatory interview on August 5, 2019.

Demographics. Nine interviewees were male and twelve were female. Interviewees ranged from 19 to 54 in age, with a median age of 32. Two interviewees had a high school degree, seven were either enrolled in college or had some college experience, eight had graduated from a four-year college, and four held graduate degrees. Compared to the overall U.S. population, the sample was slightly skewed toward more highly educated and younger individuals.

Data analysis. The interview data were analyzed and coded iteratively. Matrices and data displays were used to visualize and reduce the amount of information in the responses (Miles and Huberman 1994). Open coding was used to break down the data analytically, identify concepts, and compare them. Concepts were based on the interview guide and emerged organically through the responses. Already coded interviews were revisited when new concepts emerged in later interviews. Concepts were also compared between interviewees to ensure consistency. The relationships emerging from the coding and their fit with individual respondents were cross-validated by the first two authors to increase their robustness and reliability. Removing the pilot respondents from the sample does not change any qualitative result—all patterns identified for pilot respondents held true for other respondents, too.

Results. The interviews lead to two main conclusions about FB users' thoughts and feelings. First, they corroborate the presence of status quo inertia keeping users on FB. All but one respondent intended to continue using FB despite the breach. Especially lower-intensity users explicitly linked their continued presence on the platform to its necessity for maintaining connections to distant contacts and the social switching costs that leaving would incur, and many users described being locked in.

> *If there was a competitor that had, even maybe 30% of the user base that Facebook did, I definitely would not use Facebook.* (Respondent 7)
> *Yes [I want to keep using it] because it's a way that I can unite friends from all over the world, and otherwise I wouldn't really have connections with them, without Facebook.* (Respondent 13)

Users also showed regret avoidance, manifesting in not wanting to miss out on FB content if they leave the platform. However, some users reported initially reducing their FB activity after learning of the breach but then resuming their normal behavior. This finding, consistent with the results from Brown (2020), may show FB

users' early attempts to reduce dissonance by changing their behavior, only to later cease doing this due to status quo inertia:

> *Whenever I would hear, see news about the breach then I would find myself maybe not going on for a couple of days, but then I'd go back … It was never a long time, because there's things I want to see …, there's people I want to connect to on Facebook.* (Respondent 10)

Similarly, FB users, especially those who had known about having been breached before the interviews, often did not assign much importance to being breached. This may be another way of reducing dissonance by reducing the perceived importance of the data breach.

However, this may potentially also be a sign of self-perception, especially for users who reported few emotional ties to FB before the breach. When asked about their evaluation of the data breach and their continuance intention, some users who did not report feeling locked in described how their use did not change and, tied to this, their attitudes normalized.

> *I do [want to continue using FB], because I don't feel like this was anything big enough to break my trust, and I like using it enough that this wouldn't stop me.* (Respondent 6)
> *I can … get updated on what other people are doing in their lives, where are they now type of thing. [the breach] doesn't alter that behavior for me, I'm still going to scroll and look at what other people are posting.* (Respondent 20)

Thus, the interviews provide some tentative support for the presence of cognitive dissonance after the data breach as well as the presence of social switching cost on FB in general, but also point to FB users' attitudes being based in simple observation of their own behavior. Of course, the cross-sectional nature of the interviews means that they do not allow us to more deeply examine attitude change over time to clearly differentiate between the mechanisms of self-perception and cognitive dissonance, beyond users' self-reports of if and how their attitudes and behaviors changed.

The interviews also expand our understanding of OSNs by showing that FB users linked the breach with their privacy concerns about FB. Many users who reported no long-term trust and opinion changes after the breach already had low trust and negative attitudes. They seemed to view FB in a calculated manner, trading off privacy for contacts and entertainment, which made them more cynical in their reaction to the breach:

> *[S]ince Facebook is free, you have to assume that it's free because you are the product. … But I just sort of accept that that's the world today, and I take that risk … because I want to interact with people.* (Respondent 18)

We view this as an indication that the Cambridge Analytica data breach struck FB users in an OSN environment that is already characterized by privacy fatigue (Choi et al. 2018). However, these findings may also be influenced by our inviting respondents to actively deliberate their thoughts on FB and privacy. Future work could study the role of prior privacy attitudes in the reactions to a data breach.

References for the Online Appendices

Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. *J. Econom. Literature* 54(2):442–492.

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.

Adjerid I, Peer E, Acquisti A (2018) Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quart.* 42(2):465–488.

Agarwal S, Ghosh P, Ruan T, Zhang Y (2024) Transient customer response to data breaches of their information. *Management Sci.* 70(6):3381–4165.

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.

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

Barnes SB (2006) A privacy paradox: Social networking in the United States. *First Monday*.

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

Berinsky AJ, Huber GA., Lenz GS (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Anal.*, *20*(3):351–368.

Bliese PD, Ployhart RE (2002) Growth modeling using random coefficient models: Model building, testing, and illustrations. *Organ. Res. Methods* 5(4):362–387.

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.

Cichy P, Salge TO, Kohli R (2021) Privacy concerns and data sharing in the Internet of Things: Mixed methods evidence from connected cars. *MIS Quart.* 45(4):1863–1892.

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.

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

Coppock, A. (2019). Generalizing from survey experiments conducted on Mechanical Turk: A replication approach. *Political Sci. Res. Methods 7*(3):613–628.

Dehling T, Sunyaev A (2024) A design theory for transparency of information privacy practices. *Inform. Systems Res.* 35(3):956–977.

Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform. Systems Res.* 17(1):61–80.

Draper NA, Turow J (2019) The corporate cultivation of digital resignation. *New Media Soc.* 21(8):1824–1839.

Forderer J, Burtch G (2025). Estimating career benefits from online community leadership: evidence from stack exchange moderators. *Management Sci.* 71(3): 2443–2466.

Frank EL, Krautter K, Wu W, Jachimowicz, JM (2025). Riding the passion wave or fighting to stay afloat? A theory of differentiated passion contagion. *Admin. Sci. Quart.* 70(2):444–495.

Gefen D, Karahanna E, Straub DW (2003) Trust and TAM in online shopping: An integrated model. *MIS Quart.* 27(1):51–90.

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.

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.

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

Hayes AF (2022) *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, 3rd ed. (Guilford Publications, New York City, NY).

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.

Horn JL, McArdle JJ (1992) A practical and theoretical guide to measurement invariance in aging research. *Exp. Aging Res.* 18(3):117–144.

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.

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.

Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Security* 64:122–134.

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.

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.

Li H, Sarathy R, Xu H (2010) Understanding situational online information disclosure as a privacy calculus. *J. Comput. Inform. Systems* 51(1):62–71.

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, Cao J, Everard A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *J. Management Inform. Systems* 27(4):163–200.

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.

Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inform. Systems Res.* 15(4):336–355.

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.

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.

Miles MB, Huberman AM (1994) *Qualitative data analysis* (Sage, London, Thousand Oaks, New Delhi).

Morris, SB (2008) Estimating effect sizes from pretest-posttest-control group designs. *Organ. Res. Methods.* 11(2):364-386.

Myers MD, Newman M (2007) The qualitative interview in IS research: Examining the craft. *Inform. Organ.* 17(1):2–26.

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.

Obar JA, Oeldorf-Hirsch A (2020) The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Inform. Comm. Soc.* 23(1):128–147.

Pavlou, PA, Gefen D (2004) Building effective online marketplaces with institution-based trust. *Inform. Systems Res.*, 15(1):37–59.

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

Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quart.* 35(4):989–1015.

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

Thatcher JB, Perrewé PL (2002) An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quart.* 26(4):381–396.

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.

Venkatesh V, Goyal S (2010) Expectation disconfirmation and technology adoption: Polynomial modeling and response surface analysis. *MIS Quart.* 34(2):281–303.

Wang J, Li G, Hui, KL (2022). Monetary incentives and knowledge spillover: Evidence from a natural experiment. *Management Sci.* 68(5):3549–3572.

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

Xu H, Teo HH, Tan BCY, Agarwal R (2012) Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Inform. Systems Res.* 23(4):1342–1363.

Xu H, Zhang N (2024) An onto-epistemological analysis of information privacy research. *Inform. Systems Res.* 35(3):1422–1434.

Zhang N (Andy), Wang C (Alex), Karahanna E, Xu Y (2022) Peer privacy concerns: Conceptualization and measurement. *MIS Quart.* 46(1):491–530.