Marketing Science Institute Working Paper Series 2025

Report No. 25-123

Customer Privacy Journey

Natalie Chisam, Jordan W. Moffett and Kelly D. Martin

"Customer Privacy Journey" © 2025

Natalie Chisam, Jordan W. Moffett and Kelly D. Martin

MSI Working Papers are Distributed for the benefit of MSI corporate and academic members and the general public. Reports are not to be reproduced or published in any form or by any means, electronic or mechanical, without written permission.

Customer Privacy Journey

Natalie Chisam, PhD*
Assistant Professor of Marketing
College of Business at University of Nebraska–Lincoln
HLH 345F, P.O. Box 880492, Lincoln, NE 68588-0492
913.530.5763
nchisam@unl.edu

Jordan W. Moffett, PhD*
Assistant Professor of Marketing
Gatton College of Business and Economics at University of Kentucky
550 South Limestone, Lexington, Kentucky 40506
337.802.5979
jwmoffett@uky.edu

Kelly D. Martin, PhD*
Professor of Marketing and Tinberg "Business for a Better World" University Professor
College of Business at Colorado State University
501 West Laurel Street, Fort Collins, Colorado 80523
970.491.7269
kelly.martin@colostate.edu

* Equal authorship

Declaration of Conflicting Interests: The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Financial disclosure: The author(s) received no financial support for the research, authorship, and/or publication of this article.

Customer Privacy Journey

Abstract: Ongoing cycles of data collection and exposure are reshaping how customers think about privacy and engage with firms, yet most research treats privacy as a static, one-time data disclosure or breach event. This study introduces the *customer privacy journey*—a dynamic, stage-based framework that reconceptualizes privacy as an evolving experience embedded in the customer–firm data exchange relationship. In the pre-breach stage, as firms collect data and accumulate power, customers feel vulnerable to disclosure risk. In the breach stage, that risk becomes realized, sparking feelings of privacy violation. In the post-breach stage, residual risk—especially when trust is not restored—triggers privacy fatigue, an underexplored phenomenon marked by exhaustion and cynicism. The privacy journey is cyclical: customers may re-enter the pre-breach stage, carrying forward prior experiences that shape future reactions. Firms can intervene at each stage by fostering security, justice, and autonomy, respectively. Privacy architectures, such as regulatory frameworks, indirectly shape the privacy journey by guiding standard firm behaviors. Customer perceptions of risk (privacy resources) and trust in the firm's power (relational expectations) directly moderate it. The proposed framework and six guiding tenets offer a foundation for future research and practical strategies to navigate privacy in a dynamic, data-driven world.

Keywords: Privacy, data breach, customer journey, privacy fatigue, relationship dynamics, relationship marketing, public policy

Customers today face mounting pressure in their digital lives. They are increasingly aware that firms track their personal data through rewards programs, websites, apps, and everyday interactions. At the same time, data breaches have become alarmingly routine. In 2024 alone, cyberattacks compromised over 1.35 billion U.S. accounts—nearly four times the U.S. population—indicating that many individuals experienced multiple data breaches (Statista 2025). This ongoing cycle of data collection and exposure is reshaping how customers view privacy; it is fueling growing concern, prompting calls for stronger regulation (Johnston 2023), and shaping what people buy (Bhatnagar 2024). Most customer privacy research offers static, isolated snapshots—capturing how customers feel when first asked to share data (Acquisti, John, and Loewenstein 2012; Okazaki et al. 2020) or how they respond immediately after a data breach (Janakiraman, Lim, and Rishika 2018; Martin, Borah, and Palmatier 2017). *This leaves a critical gap: privacy experiences are neither static nor isolated—they evolve over time*. Without a dynamic understanding of how privacy unfolds, firms lack the insight to anticipate customer reactions, sustain trust, and adapt to shifting expectations in data exchange relationships.

In response, we introduce the *customer privacy journey*—a dynamic, stage-based framework that conceptualizes privacy not as a single moment of data collection or breach, but as an unfolding experience rooted in ongoing data exchange with a firm.[1] Unlike purchase journeys, where individuals make deliberate choices with clear goals (Hamilton et al. 2021; Lemon and Verhoef 2016), privacy journeys unfold in the background. Customers know their data are being collected, but often lack control over when, how, or why. Their experiences reflect limited agency in a system dominated by firm power and consistent risk exposure.

---

[1] We use the terms "customer privacy journey" and "privacy journey" interchangeably. Similarly, we use the terms "data breach" and "breach" interchangeably.

Integrating perspectives on privacy (Lwin, Wirtz, and Williams 2007; Solove 2002) and relationship marketing dynamics (Harmeling et al. 2015; Zhang et al. 2016), we theorize that *the privacy journey entails evolving psychological reactions to data-related power asymmetries and risk-related inflection points in the customer–firm data exchange relationship*. It begins with a pre-breach stage, as customers become aware of data collection and the power firms derive from it, marking the first inflection point and prompting feelings of privacy vulnerability. The second inflection point occurs when this disclosure risk is realized through a breach, triggering feelings of privacy violation. In a post-breach stage, a third inflection point arises through the firm's response or the passage of time without resolution, where residual risk induces privacy fatigue: a form of customer exhaustion stemming from ongoing data privacy issues. Although noted in emerging work (Chen et al. 2023; Choi, Park, and Jung 2018), privacy fatigue is understudied.

Notably, this privacy journey is cyclical: prior privacy experiences shape future ones. When customers re-enter the pre-breach stage, they often carry over privacy fatigue, deepening their overall weariness with data exchange. They then become more sensitive to disclosure risk, less responsive to future realized risk, and more attuned to lingering residual risk. We propose stage-specific firm interventions designed to foster a sense of security, justice, and autonomy, respectively, and argue these are more effective than conventional internal data practices or regulatory mandates, collectively known as privacy architectures (Lessig 1999; Solove 2004). Customer-level factors directly moderate their privacy experiences. *Privacy resources* are a customer's knowledge and motivation to independently manage their data privacy (Brough and Martin 2020), and influence how they perceive risk associated with a firm's data-related power. *Relational expectations* are a customer's pre-existing beliefs about how the relationship should be governed, including mutual obligations, social norms, and anticipated data management by the firm (Harmeling et al. 2015), and shape whether they trust the firm's use of that power.

This research makes several contributions. First, we advance a dynamic understanding of privacy by introducing and conceptualizing the privacy journey as a fluid, evolving sequence of interactions within the customer–firm data exchange relationship. While prior research has yielded important insights, it remains fragmented, often treating the customer, firm, or regulatory perspective in isolation and overlooking their interdependence (Bleier, Goldfarb, and Tucker 2020). Our framework brings these perspectives together to capture the interplay between customer psychology, firm interventions, and structural privacy architectures, articulated through six core tenets. In doing so, it offers a unified foundation for theorizing how privacy experiences unfold across distinct stages and highlights key inflection points where firms can shape outcomes. This stage-based approach responds to calls for new conceptualizations of customer journeys (Hamilton et al. 2021; Siebert et al. 2020) and broader, managerially relevant theorizing in marketing (Kindermann et al. 2024; Kozlenkova et al. 2024). The privacy journey framework provides a roadmap for advancing privacy research and helping firms manage data exchange relationships amid continuous customer data flows and changing privacy expectations.

Second, our conceptualization advances an undertheorized dimension of privacy: the data-related power dynamics between customers and firms. Prior privacy research often emphasizes structural forces, such as privacy architectures or data contexts, as primary drivers of customer reactions to power imbalances (Bornschein, Schmidt, and Maier 2020; Lwin, Wirtz, and Williams 2007). While our framework acknowledges these conditions, it centers on how customers perceive the power imbalances embedded within them. We argue that customers interpret these asymmetries according to two key factors: their privacy resources and relational expectations. These moderating factors influence how customers experience privacy vulnerability, violation, or fatigue, and whether firm interventions are restorative or merely performative. For example, in the pre-breach stage, both low-resource and high-resource customers may experience heightened privacy vulnerability, stemming from confusion in the former and hyper-awareness in the latter. By the post-breach stage, these resources function differently: high-resource customers are better positioned to process breaches and respond to autonomy-enhancing interventions, while low-resource customers may feel overwhelmed, making recovery efforts less effective or even counterproductive. These dynamics offer guidance for firms to tailor interventions to different customer segments across the privacy journey.

Third, we introduce privacy fatigue as a distinct late-stage psychological reaction to breaches. Extending prior research on short-term reactions, such as emotional violation and trust erosion (Janakiraman, Lim, and Rishika 2018; Martin, Borah, and Palmatier 2017), and emerging work on digital fatigue (Ursu, Zhang, and Honka 2023), we conceptualize privacy fatigue as the gradual, cumulative toll of navigating persistent data collection and repeated breaches. This challenges the assumption that post-breach recovery is complete once firm performance rebounds, reflecting customer sentiments that "Companies lose your data and then nothing happens" (Stewart 2022). Consequently, few firms are equipped to detect or address this fatigue. While customer behavior may normalize (Agarwal et al. 2024; Turjeman and Feinberg 2024), privacy fatigue can linger—silently undermining well-being, suppressing future engagement, and eroding long-term data exchange relationships. Importantly, our framework also reconceptualizes privacy reactions as cyclical rather than linear. Customers often re-enter the privacy journey already fatigued, altering how they experience disclosure, breach, and recovery. This recursive structure reframes post-breach recovery as more than a justice issue: it highlights the need for autonomy-restoring interventions that reengage fatigued customers on their own terms and prevent disengagement from compounding over time.

To illustrate the proposed privacy journey framework and its underlying logic, we utilize the large-scale AT&T breach announced in July 2024. We conduct a real-time, longitudinal three-wave survey, combining open-ended and matching questions to track customers' evolving psychological reactions throughout a real privacy journey as it unfolds. These insights, integrated with YouGov's BrandIndex metrics, uncover a deeper pattern: brand advocacy plummets right after the breach and, although it appears to rebound, survey data reveal mounting privacy fatigue. These findings underscore the risk that behavioral metrics can mask the very disengagement firms need to see, calling for a reassessment of how post-breach recovery is conceptualized in privacy research and measured in practice.

Fundamentals of Customer Privacy Experiences

Prior privacy research offers valuable insights but stops short of fully articulating the foundational elements that shape how customers navigate their evolving privacy experiences (Martin and Murphy 2017; Solove 2002). We extend this work by synthesizing privacy literature with research on relationship dynamics (Lwin, Wirtz, and Williams 2007; Palmatier et al. 2013), revealing how their combined premises support a more dynamic view of privacy experiences. Although the customer–firm relationship is sometimes implicit in privacy research (Krafft et al. 2021), our study makes it explicit, embedding privacy experiences within ongoing data exchange relationships where power dynamics play a central role.

Within customer–firm data exchange relationships, we argue that customers' privacy experiences are largely shaped by how they perceive the firm's data-related power, that is, its capacity to collect, use, and control data. The rapid expansion of customer data collection and a rise in high-profile breaches have intensified concerns about data safety and the growing power firms wield (ITRC 2025). With this power comes an elevated responsibility to foster a risk-assured and trustworthy environment, as customers increasingly expect firms to handle their data responsibly (Lwin, Wirtz, and Williams 2007). Customers are not passive recipients—when firms unilaterally exercise power by processing data without meaningful consent, oversight, or transparency, they may interpret such actions as undermining relational norms, including trust, accountability, and fairness (Bi et al. 2024). Such power imbalances can prompt customers to withhold information, seek alternatives, or disengage (Lwin, Wirtz, and Williams 2007).

Building on the data-related power imbalance as the foundational condition of the privacy journey, we outline two premises: (1) privacy experiences unfold over time and are directly shaped by key events, or *inflection points*, that reconfigure customers' perceptions of risk and trust; and (2) these evolving experiences are supported by *privacy architectures*, which are the technical and regulatory structures, such as software code, data infrastructure, and legal mandates, that enable and constrain the flow of customer data and, in doing so, regulate firm behavior and indirectly shape customers' privacy experiences (Lessig 1999; Reidenberg 1993).

Customer Privacy Experience Dynamics and Inflection Points

The customer privacy experience begins once customers become aware that the firm is collecting or will collect their data, often shared actively or passively through routine interactions with technology-driven services, such as navigation apps or retail transactions (Krafft et al. 2021). Whether trivial or highly sensitive, each detail gathered becomes a data point forming a digital profile (Melzner, Bonezzi, and Meyvis 2023), shifting data-related power to firms (Fournier and Alvarez 2013). This shift exemplifies a broader dynamic of informational power, or the ability to influence others by setting conditions or shaping environments (Gaski and Nevin 1985; Labrecque et al. 2013). In the context of privacy, a firm's power stems from its possession of customer data and its capacity to determine how it is used. Personalized experiences or short-term incentives (e.g., loyalty discounts) may offer immediate customer benefits; yet, long-term data disclosure risks, such as intrusive profiling and identity theft, loom especially as engagement continues (Krafft et al. 2021).

Customer information can help firms build and maintain ongoing relationships (Krafft et al. 2021), and is especially critical considering customer dynamics, or the temporal shifts in customer attitudes and behaviors (Zhang and Chang 2021). However, in pursuing continuous data collection to foster broader relationship development, firms expose themselves and their customers to privacy risks, which are likely to alter privacy experiences. Despite growing recognition of customer change dynamics (Acquisti, Brandimarte, and Loewenstein 2020), most customer-side privacy research focuses on static, isolated events such as data disclosure requests (Acquisti, John, and Loewenstein 2012) and breach notifications (Madan, Savani, and Katsikeas 2023; Zhu et al. 2024). This leaves a gap in understanding the longitudinal, event-triggered, and compounded progression of customer privacy experiences.

If firms responsibly manage customer data by ensuring mutual respect and benevolent intent (Brough et al. 2022; Martin, Borah, and Palmatier 2017), customers may continue disclosing data, enabling firms to generate insights and strengthen broader relationships (Krafft et al. 2021). With time, customers may become more accepting of data disclosure risks, particularly when they trust the firm and see benefits in sustaining their data exchange relationship (Acquisti, Brandimarte, and Loewenstein 2020; Dagger, Danaher, and Gibbs 2009). However, breaches fundamentally disrupt this symbiotic exchange (Martin and Murphy 2017), introducing an inflection point that may sharply alter customer privacy experiences.

Research on relationship dynamics shows that while some events gradually shape customer–firm relationships, others serve as inflection points that redefine trust and engagement (Harmeling et al. 2015). We propose that breaches represent the latter: disruptive events that trigger relational disconfirmation. The firm's data-related power creates an inherent responsibility to customers, and a breach violates this social contract. Unlike other crises, breaches often involve irretrievable data, making their effects more permanent and trust-eroding (Malhotra and Malhotra 2011; Rasoulian et al. 2023). As such, we expect a breach to serve as a critical event in the customer's privacy experience, prompting a re-evaluation of the data exchange relationship and whether, and how, it should continue.

Customer Privacy Experiences Supported by Privacy Architectures

Privacy experiences involve customer reactions to shifting perceptions of risk and trust, rooted in power imbalances. However, these experiences do not occur in a vacuum. They are shaped and constrained by the broader privacy architecture in which firms operate. Initially conceptualized by legal scholars, privacy architectures guide firm behavior in managing customer privacy (Lessig 1999; Reidenberg 1993). Their presence and strength, whether adopted voluntarily by firms or mandated by regulation, vary across contexts, influencing how data are managed, disruptions are handled, and privacy is viewed in society (Solove 2004). Just as physical architecture structures human movement through built environments, privacy architecture shapes how data flows from customers to firms and beyond (Solove 2002).

At the point of data collection, privacy architectures, particularly when robust, help protect against harm by embedding safeguards into data systems and processes. This approach, often referred to as privacy-by-design, encourages firms to build protective mechanisms into data practices (Duncan 2007). Regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA) formalize this principle by requiring data minimization and collection justification (Goldsteen et al. 2022). In both firm-initiated and legally mandated contexts, firms may adopt data retention rules, limiting how long customer data are stored before deletion (Politou, Alepis, and Patsakis 2018). These internal processes can become customer-facing when firms embrace transparency to help customers understand how their data are used and how to engage with privacy protection tools.

Privacy architectures also may critically shape firm behavior when things go wrong at key inflection points. While prevention and transparency aim to minimize risk, breach response mechanisms influence how well firms contain damage and preserve customer trust. Some regulatory frameworks specify actions and timelines (Olukoya 2022). In the U.S., all states mandate breach notification to customers and regulators (FTC 2025), and the Securities and Exchange Commission penalizes firms for misrepresenting breaches, as in the Pearson case, where an actual incident was labeled “hypothetical” (Rundle 2021). Firms may also implement internal protocols as part of proactive governance or compliance efforts, detailing steps for breach notification and remediation (Rasoulian et al. 2017; Zhu et al. 2024). In some cases, privacy architectures support legal redress by defining damages for affected customers (Olukoya 2022). When such protections are robust, penalties can be significant, as with the €1.2 billion fine against Meta for repeated data mishandling (Satariano 2023).

Privacy architectures are thus the structural foundation beneath customers’ privacy experiences—supporting but not defining them. Less something customers directly feel and more like rails guiding a train, privacy architectures shape the institutional context and influence firm behavior by determining available paths, embedded protections, and breach responses. In doing so, they indirectly shape privacy experiences by constraining or enabling firm action. While necessary, privacy architectures alone are insufficient for capturing the dynamic nature of privacy or for guiding firms in addressing customers’ evolving psychological needs.

Customer Privacy Journey Conceptual Framework

Building on these customer privacy fundamentals, we introduce a dynamic, multi-stage privacy journey framework that offers a more complete account of how customer privacy experiences evolve and where and how firms can effectively intervene. This privacy journey unfolds across three stages—pre-breach, breach, and post-breach—each defined by a risk-related inflection point that alters privacy experiences and supported by privacy architectures that guide standard firm practices. See Figure 1 for an overview and Table 1 for construct definitions.

Pre-Data Breach Stage

Customer privacy vulnerability pre-data breach. The privacy journey begins when a customer becomes aware that their data are or will be collected, whether actively disclosed, automatically captured via third-party brokers, or gathered through hybrid means. Awareness is critical (Dalmia and Diehl 2025): as customers assume the disclosure risks associated with data collection, they begin to experience *privacy vulnerability*, defined as customer susceptibility to harm arising from the firm’s collection, access, or use of their personal data (Martin, Borah, and Palmatier 2017). Even in the absence of a breach or evident misuse, customers may feel anxious or uneasy (Smith and Cooper-Martin 1997), simply because their data have been collected. At the heart of this vulnerability lies a power imbalance: once a firm collects customer data, it gains informational power that customers cannot easily restore. Firms determine how, when, and by whom customer data are accessed and used. As firms acquire more intimate and extensive data, this power imbalance grows (Lwin, Wirtz, and Williams 2007; Mende et al. 2024), deepening how vulnerable the customer feels. Even when customers willingly disclose data for personalization or social connection (Aguirre et al. 2015; Reeck et al. 2023), the cumulative nature of data collection still amplifies privacy vulnerability.

Figure 1. Customer Privacy Journey Model

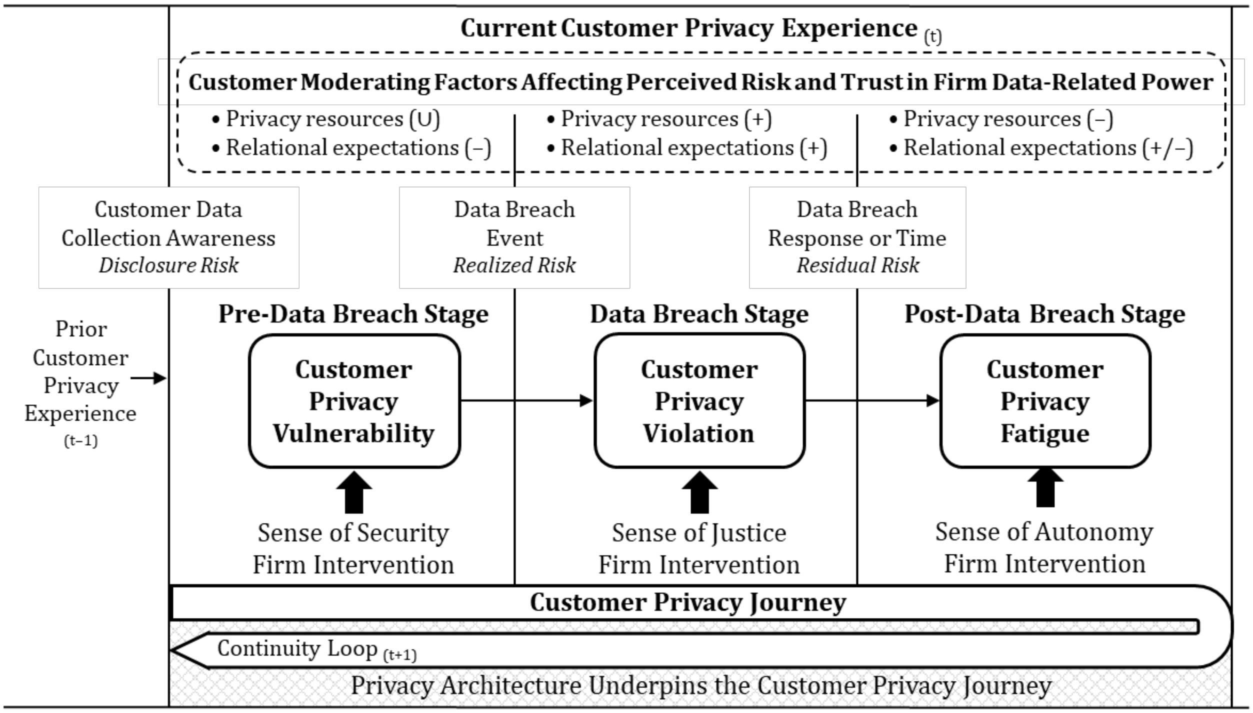

Current Customer Privacy Experience (t)
Customer Moderating Factors Affecting Perceived Risk and Trust in Firm Data-Related Power
• Privacy resources (∪)
• Relational expectations (–)
• Privacy resources (+)
• Relational expectations (+)
• Privacy resources (–)
• Relational expectations (+/–)
Customer Data Collection Awareness
Disclosure Risk
Data Breach Event
Realized Risk
Data Breach Response or Time
Residual Risk
Prior Customer Privacy Experience (t–1)
Pre-Data Breach Stage
Data Breach Stage
Post-Data Breach Stage
Customer Privacy Vulnerability
Customer Privacy Violation
Customer Privacy Fatigue
Sense of Security Firm Intervention
Sense of Justice Firm Intervention
Sense of Autonomy Firm Intervention
Customer Privacy Journey
Continuity Loop (t+1)
Privacy Architecture Underpins the Customer Privacy Journey

Table 1. Construct Definitions

Constructs	**Definitions**
Customer privacy journey	A customer's evolving privacy experiences within a customer–firm data exchange relationship, unfolding across three stages: pre-breach, breach, and post-breach.
Privacy architectures	The technical and regulatory structures, such as software code, data infrastructure, and legal mandates, that enable and constrain the flow of customer data (Lessig 1999; Reidenberg 1993).
Pre-Data Breach Stage	
Customer privacy vulnerability	Customer susceptibility to harm arising from the firm's collection, access, or use of their personal data (Martin, Borah, and Palmatier 2017).
Sense of security firm intervention	The extent to which a customer believes that they are protected from the misuse, loss, or compromise of their personal data (Zeithaml et al. 2002).
Data Breach Stage	
Customer privacy violation	Customer feelings of anger and betrayal, arising from the belief that the firm failed to uphold its responsibility to protect their personal data (Martin, Borah, and Palmatier 2017).
Sense of justice firm intervention	The extent to which a customer believes that appropriate reparations have been made for the harm resulting from a data breach (Grégoire et al. 2018).
Post-Data Breach Stage	
Customer privacy fatigue	Customer exhaustion with ongoing data privacy issues, manifesting in emotional exhaustion and/or cynicism (Choi, Park, and Jung 2018).
Sense of autonomy firm intervention	The extent to which a customer believes that they can freely manage or control how their personal data are used (Tucker 2014; White and Simpson 2013).
Customer Moderating Factors Affecting Perceived Risk and Trust in Firm Data-Related Power	
Customer privacy resources	A customer's knowledge and motivation to independently manage their data privacy (Brough and Martin 2020).
Customer relational expectations	A customer's pre-existing beliefs about how the relationship should be governed, including mutual obligations, social norms, and anticipated data management by the firm (Harmeling et al. 2015).

When customers experience privacy vulnerability, it can trigger adverse reactions, such as discomfort from the realization that their personal information has been surrendered without a full understanding of how it will be used or protected (Walker 2016). In response, customers may seek to minimize their susceptibility to harm by limiting the firm's access to their data or disengaging altogether. This early-stage retreat can disrupt relationship development, undermining the firm's ability to personalize offerings or generate insights from customer behavior. Privacy vulnerability thus inhibits trust formation and constrains the firm's ability to cultivate customer engagement.

Privacy architectures form the structural backdrop to privacy vulnerability. Elements like data protection laws, authentication protocols, and access controls often operate behind the scenes. When firms make these protections visible, they may help reduce privacy vulnerability by signaling accountability and benevolence. However, in practice, such safeguards function as imperfect safety nets that offer reassurance but rarely eliminate the underlying power asymmetry that drives privacy vulnerability—for example, privacy policies are designed to inform, yet they are often ignored or misunderstood (Dalmia and Diehl 2025; Walker 2016). Even when customers are informed, cognitive biases and information overload can exacerbate privacy concerns (Acquisti, Brandimarte, and Loewenstein 2020; Brough et al. 2022). These nuances suggest that privacy vulnerability is not a transient issue but a persistent characteristic of data exchange relationships—albeit its salience likely varies across customers, contexts, and time.

Firm intervention via a sense of security pre-data breach. In response to experiencing privacy vulnerability, customers seek reassurance from firms, which they perceive as responsible for safeguarding their data. A firm's ability to deliver a *sense of security*, defined as the extent to which a customer believes that they are protected from the misuse, loss, or compromise of their personal data (Zeithaml et al. 2002), becomes a critical early-stage intervention. Delivering security fosters trust in the firm's accountability, which helps rebalance the perceived power asymmetry by assuring customers that protective measures are in place. This, in turn, reduces privacy vulnerability. A sense of security acts as a "protective cocoon" against abstract, often invisible threats (Giddens 1991). Notably, fostering a sense of security requires more than compliance with "notice and choice" provisions embedded in many privacy architectures, which can paradoxically increase privacy vulnerability by drawing attention to data disclosure risks (Brough et al. 2022). Instead, firms must communicate transparently and clearly about how data are protected, why safeguards are effective, and how such measures reflect not just competence but also benevolence. When done well, these efforts both reinforce trust in the firm and bolster confidence in the privacy architectures supporting responsible data management (Campbell et al. 2020; Thompson, Henry, and Bardhi 2018).

Crucially, the burden of protection should not fall on customers at this stage, as they already feel vulnerable. Firms must recognize their position of power and take proactive steps to foster an environment grounded in security and ethical data use. In the pre-breach stage, interventions that emphasize firm-driven protection rather than relying on customer self-management are more likely to reduce privacy vulnerability. For example, Unilever integrates privacy-by-design principles across its operations, going beyond legal compliance to embed transparency, accountability, and trust into its data practices from the outset (Unilever 2025).

Consistent with other customer journey frameworks (Lemon and Verhoef 2016), the pre-breach stage can last moments, months, or years, and although its duration varies, privacy experiences are rarely static. Recent research suggests that customer vulnerability can be disrupted by inflection points that reshape experiences (Mende et al. 2024; Salisbury et al. 2023).

With respect to privacy experiences, a breach represents such a disruption, triggering a cascade of new psychological reactions and behavioral responses.

Data Breach Stage

Customer privacy violation during the data breach. When customers become aware of a breach, they enter the breach stage, during which they must assess the event's significance and the firm's responsibility in the failure (Kähr et al. 2016). Given the firm's powerful position in the data exchange relationship, customers will likely attribute blame to the firm, assuming the firm neglected its duty to protect their data. At this point, the previously tolerated disclosure risk becomes realized risk, eliciting *privacy violation*, defined as customer feelings of anger and betrayal, arising from the belief that the firm failed to uphold its responsibility to protect their personal data (Martin, Borah, and Palmatier 2017). In this stage, privacy violation emerges as the dominant psychological reaction, though privacy vulnerability may persist, particularly if the firm failed to instill a sense of security in the pre-breach stage. In such cases, customers will be more sensitive to the realized risk and thus feel more violated.

Customers trust firms to handle their data responsibly, but breaches shatter that trust (Rasoulian et al. 2017). This loss of trust can carry cascading effects, ultimately harming firm performance (Harmeling et al. 2015; Ward and Ostrom 2006). When customers feel violated, they often view the firm's actions as unfair—an appraisal that triggers justice-seeking responses such as marketplace aggression, negative word of mouth, or boycotts (Grégoire, Laufer, and Tripp 2010; Kähr et al. 2016). Customers may even falsify information if they remain in the data exchange relationship (Lwin, Wirtz, and Williams 2007). Justice-seeking helps customers ease psychological distress and reassert a sense of fairness (Grégoire and Fisher 2008).

Robust privacy architectures may reduce breach frequency or severity, but they cannot fully eliminate risk. In self-regulating markets with limited oversight, weak or absent privacy architectures likely lead to more frequent breaches and inadequate responses (Reich, Campbell, and Madrigal 2020). Customers in these settings may feel especially violated, not because privacy architectures directly shape their psychological reaction, but because the firm's insufficient breach response signals a broader lack of systemic accountability.

Firm intervention via a sense of justice during the data breach. When customers experience privacy violation, they want the firm to "make it right" by addressing grievances and restoring a *sense of justice*, defined as the extent to which a customer believes that appropriate reparations have been made for the harm resulting from a breach (Grégoire et al. 2018). Delivering justice restores a sense of fairness, which helps rebalance the perceived power asymmetry by reassuring customers that the firm acknowledges the harm and accepts accountability for it. This, in turn, can reduce feelings of privacy violation. Until then, forgiveness may be difficult (Aquino, Tripp, and Bies 2006). Once a breach is operationally contained, firms face a critical juncture that necessitates both internal (e.g., fixing technical architecture failures) and external recovery to restore the customer–firm data exchange relationship. Recovery efforts must go beyond internal fixes to deliver a sense of justice, often beginning with the breach notification. While some disclosures are vague or downplay the incident (Zou and Schaub 2019), clear and timely notifications can reduce the perceived threats (Romanosky, Telang, and Acquisti 2011). Importantly, recovery efforts do not occur in a vacuum. Although privacy architectures can inform firm responses, regulations or policies alone rarely signal that the firm itself is committed to responsible data privacy management.

To prevent excessive customer retribution and reduce litigation costs, firms must deliver prompt, respectful, and meaningful resolutions—core elements of an effective justice-based response (Ashworth and Free 2006; Shao et al. 2022). Such efforts often begin with breach disclosure and may include notifying customers, expressing remorse, outlining corrective actions, and offering support such as free credit or identity monitoring services (Bourdon 2017; Gwebu, Wang, and Wang 2018). However, the effectiveness of these responses varies widely. For example, Cash App faced criticism for delayed notifications, vague communication, and poor support after its breach (Kost 2024). Users reported being "ghosted," contributing to feelings of abandonment and a $15 million settlement (Forbes 2024). In contrast, following its cyberattack, the Red Cross responded swiftly, implemented enhanced security measures, and avoided class action litigation (Weinberg 2023).

These cases, along with prior research on other types of failures, suggest that feelings of privacy violation may subside or persist depending on the perceived sincerity and adequacy of the firm's response (Grégoire and Fisher 2008; Mende et al. 2024). This stage can culminate in an inflection point driven by firm intervention: a timely, transparent, and accountable response, as in the Red Cross case, can restore justice and help customers transition more smoothly to the post-breach stage, where they may feel acknowledged and even begin to rebuild some trust (Nikkhah and Grover 2022; Salisbury et al. 2023). In contrast, weak or absent interventions, as seen in the Cash App example, can prolong this stage, leaving customers with residual anger and betrayal. These varied outcomes underscore how firm interventions influence customers' immediate psychological reactions and their broader privacy journeys.

Post-Data Breach Stage

Customer privacy fatigue post-data breach. Customers can enter the post-breach stage through multiple paths. Some following effective firm interventions, while others enter gradually as unresolved experiences wear them down. Regardless of how they arrive, or how much privacy violation persists, a psychological shift occurs: from reacting to the realized risk of a breach to coping with the lingering uncertainty of future harm. Reflecting on this residual risk, customers may feel weary, resigned, or detached, experiencing *privacy fatigue*, defined as customer exhaustion with ongoing data privacy issues (Choi, Park, and Jung 2018). Privacy fatigue may begin earlier in the privacy journey, but it becomes psychologically salient in the post-breach stage. It intensifies over time, especially following recurrent breaches that compromise personal data, whether with the focal firm or others (Chen et al. 2023). While privacy fatigue has received limited attention in marketing, it has been discussed in information systems (Tang, Akram, and Shi 2021), psychology (Chen et al. 2023), and the business press (Ermey 2024). Crucially, privacy fatigue is not apathy; fatigued customers are not indifferent. They are worn down by the ongoing strain of managing privacy in overwhelming or unrewarding environments. As a result, they may lose the capacity, motivation, or confidence to stay engaged. This fatigue can lead to behaviors that appear inconsistent with their privacy concerns, not because customers no longer care, but because they no longer feel able to respond effectively (Alashoor et al. 2023).

Prior work suggests that privacy fatigue manifests in two ways: emotional exhaustion and cynicism (Choi, Park, and Jung 2018). *Emotional exhaustion* refers to the depletion of mental and emotional energy, leaving customers overwhelmed and unable to manage their privacy (Hargittai and Marwick 2016). As exhaustion deepens, they may stop actively protecting their data or using privacy tools (Choi, Park, and Jung 2018). *Cynicism* reflects growing mistrust of firms' privacy efforts, as customers develop a negative outlook and believe their data will never be fully secure, leading to frustration, resignation, or futility (Alwafi and Fakieh 2024). Such responses to privacy fatigue may gradually erode the data exchange relationship. As customers disengage, they may leave privacy risks to chance, passively relying on default privacy settings, continuing to use platforms without caution, or failing to monitor data exposure (Tang, Akram, and Shi 2021). While such behaviors increase customer disclosure risk, firms ultimately bear the consequences. If another breach occurs, even due to customer inattention (e.g., weak passwords, avoiding two-factor authentication), customers are likely to blame the firm for failing to provide a trustworthy environment, retriggering privacy violation and further eroding trust (Figure 1). Although some studies suggest that firm performance may rebound quickly after a single breach (Agarwal et al. 2024; Turjeman and Feinberg 2024), such recovery overlooks the longer-term psychological toll on customers, the strategic consequences for the firm, and the compounding effects of repeated breaches. Fatigued customers may disengage, switch providers, or reduce their use of the firm's services. Even among those who stay, lingering mistrust may result in reduced data sharing or negative word of mouth (Chen et al. 2023; Hargittai and Marwick 2016).

The visibility and credibility of privacy architectures also shape how customers perceive the data exchange environment in this stage. Weak or opaque privacy architectures can amplify lingering uncertainty and contribute to privacy fatigue. In contrast, strong privacy architectures that visibly signals accountability and institutional benevolence may help support customer reengagement by offering a sense of structure and stability. Still, even the most robust privacy architectures are not sufficient on their own. Privacy regulations often focus on harm prevention and response in earlier stages, such as mandating breach notifications or obtaining customer consent, while overlooking the long-term psychological recovery of affected customers. For example, while the GDPR emphasizes transparency, data minimization, and penalties for misuse, it does not address how firms should support customers psychologically or relationally after a breach. If prevailing assumptions treat breaches as discrete, idiosyncratic events and expect business to return to normal, most firms will lack processes or protocols to recognize, let alone address, privacy fatigue. Supporting meaningful recovery requires more than compliance: customers must feel empowered to act within these systems, not just supported by them.

Firm intervention via sense of autonomy post-data breach. When customers experience privacy fatigue, firms should intervene by fostering a *sense of autonomy*, defined as the extent to which customers believe that they can freely manage or control how their personal data are used (Tucker 2014; White and Simpson 2013). Delivering autonomy positions the customer as an active participant in the data exchange relationship, rebalancing the perceived power asymmetry by signaling that they can make meaningful choices rather than passively accept firm control. This, in turn, reduces privacy fatigue. Crucially, autonomy should not impose burdens (Schwartz 2004); it should empower customers to make informed decisions if they choose to engage. This is critical in the context of privacy fatigue, where emotional exhaustion and cynicism can make reengagement difficult. Even small acts of agency, such as toggling a setting or correcting a data point, can help reenergize fatigued customers (Tucker 2014). However, these choices must be manageable and intuitive. Firms can support autonomy through clear opt-in mechanisms, privacy rights (e.g., data deletion or portability), and user-friendly privacy tools like customizable dashboards (Palmatier and Martin 2019). For example, Microsoft integrates autonomy into its technical privacy architecture using a human-centered approach where users can view collected data, manage preferences, and delete information in a dashboard (Evans et al. 2025).

Although firm breach responses often trigger the transition into the post-breach stage, the passage of time alone can also move customers forward. When this shift occurs without resolution, lingering feelings of privacy violation can make customers more sensitive to residual risk, increasing their susceptibility to privacy fatigue. In such cases, firms must adapt their strategies: shifting from justice-only interventions to those that restore autonomy. If firms continue to focus only on apologies or compensation that may feel hollow or irrelevant to fatigued customers who have already moved beyond the acute breach experience, they risk missing what these customers need most: a renewed sense of autonomy.

Customer Privacy Journey Continuity Loop

By restoring a sense of autonomy in the post-breach stage, firms can mitigate the negative effects of privacy fatigue and create conditions for reengagement, inviting customers back into the data exchange relationship. Without meaningful intervention, customers may remain stalled in the post-breach stage or exit the data exchange relationship altogether. When reengagement occurs, whether prompted by firm action or the customer's initiative, we argue that the privacy journey does not simply reset. As with other journey-based frameworks (e.g., Lemon and Verhoef 2016) and perspectives on relationship dynamics (e.g., Zhang et al. 2016), prior experiences shape how customers interpret and react to future ones. Importantly, these prior experiences are not always confined to the focal customer–firm data exchange relationship. Privacy fatigue can accumulate across interactions with different firms in the broader digital ecosystem, where continuous data collection and repeated breaches contribute to a broader erosion of trust. Rather than returning to a neutral pre-breach stage, customers reenter the privacy journey with renewed disclosure risk, coupled with heightened wariness, depleted psychological resources, and revised expectations grounded in the prior harm they experienced.

In this way, the privacy journey is cyclical rather than linear. Each loop carries forward psychological residue from prior privacy experiences. Lingering privacy fatigue leaves emotionally exhausted customers with fewer psychological resources to assess ongoing disclosure risks and cynical ones with less trust in the firm, thereby heightening their privacy vulnerability. If risk is realized again through another breach, fatigued customers may react with dulled feelings of privacy violation, not because the harm is less severe, but because they have become desensitized to breaches over time (Choi, Park, and Jung 2018). This erosion of responsiveness reflects a deeper form of disengagement. At the same time, residual uncertainty in the aftermath of a breach becomes more psychologically taxing, compounding privacy fatigue. With each cycle, customers grow more alert to the likelihood of future harm but feel less capable of protecting themselves. Research on digital environments shows unresolved fatigue can suppress customer engagement with firms (Thompson, Hamilton, and Rust 2005; Ursu, Zhang, and Honka 2023), suggesting similar behaviors may emerge from privacy fatigue. These recursive dynamics underscore the importance of sustained firm engagement to restore trust and interrupt the accumulation of unresolved privacy fatigue over cycles (Figure 1).

In summary, the privacy journey unfolds across three stages—pre-breach, breach, and post-breach—each shaped by distinct psychological reactions to how personal data are handled. Prior customer privacy experiences shape future ones. These experiences are indirectly influenced by underlying privacy architectures, which guide firm behavior with varying effectiveness. Firms must go beyond architectural compliance to deliver targeted, stage-specific interventions that mitigate negative reactions and rebalance perceptions of data-related power asymmetries.

> **Tenet 1 (Foundational Tenet):** The customer privacy journey unfolds across three stages—pre-data breach, data breach, and post-data breach—each marked by a distinct risk-related inflection point and corresponding psychological reaction. In the pre-data breach stage, customers face disclosure risk as they become aware of data collection, triggering feelings of privacy vulnerability. In the breach stage, realized risk emerges as threats materialize, leading to feelings of privacy violation. In the post-data breach stage, residual risk lingers, giving rise to privacy fatigue.
>
> **Tenet 2 (Continuity Loop Tenet):** The customer privacy journey is cyclical, looping as customers remain active in the data exchange relationship. Each new cycle can begin with lingering privacy fatigue, which makes customers more wary of disclosure risk, thereby increasing privacy vulnerability; less reactive to realized risk, thereby dampening privacy violation; and more attuned to residual risk, thereby intensifying privacy fatigue.

> **Tenet 3 (Privacy Architectures Tenet):** Privacy architectures underpin the customer privacy journey, indirectly shaping privacy experiences through structured mitigation efforts that support data breach prevention in the pre-data breach stage, guide firm response and accountability during the data breach stage, and enable recovery and trust repair in the post-data breach stage. While necessary, privacy architectures are insufficient to rebalance perceived data-related power asymmetries underlying customers' psychological reactions.

> **Tenet 4 (Firm Interventions Tenet):** Throughout the customer privacy journey, firms can deploy targeted interventions—offering a sense of security, justice, and autonomy—to mitigate customers' psychological reactions of privacy vulnerability, privacy violation, and privacy fatigue, respectively, at each stage.

Customer Moderating Factors of the Customer Privacy Journey

A firm's data-related power is foundational to the privacy journey, bringing with it the responsibility to provide a risk-assured and trustworthy environment. We propose that two customer-level factors moderate how individuals experience this power imbalance across the privacy journey: (1) customer privacy resources, and (2) customer relational expectations. Privacy resources influence how customers perceive the risks associated with the firm's data-related power, whereas relational expectations determine the extent to which they trust the firm to use that power responsibly. Thus, while privacy architecture establishes the structural conditions of the data exchange, these customer-level moderators directly shape how customers perceive and psychologically react to the firm's power within that structure.

Moderating Role of Customer Privacy Resources

We begin with the role of customers' privacy resources, which help them assess risks and, in turn, alter their experiences across the privacy journey.

In the pre-breach stage, privacy resources shape how customers perceive data disclosure risk. Customers with low privacy resources often experience heightened privacy vulnerability, stemming not only from confusion about what is being collected or how it might be used, but also from a diminished sense of agency—uncertainty about what, if anything, they can do in response (Walker 2016; Zimmermann et al. 2024). Those with high privacy resources may also experience elevated vulnerability, but for different reasons: their strong sense of agency, paired with heightened awareness of the scope and sensitivity of data collection, can amplify perceived disclosure risk (Brough et al. 2022). In contrast, customers with moderate privacy resources who feel reasonably informed but not overwhelmed are likely to perceive disclosure risk with calibrated concern, lowering their privacy vulnerability.

When a breach occurs, privacy resources influence how customers perceive the now-realized risk, shaping whether the breach is seen as confusing and inevitable or consequential and alarming. Customers with low levels of privacy resources likely experience muted privacy violation, as their limited understanding of data practices and diminished sense of agency make it difficult to make sense of what happened. The breach feels confusing, hard to attribute, evaluate, or respond to, reinforcing a perceived power imbalance between firms and customers. Some may even feel that this kind of thing “just happens.” Consistent with this logic, research finds that breach notifications do not alarm everyone (Zou and Schaub 2019), and individuals more accepting of power asymmetries often continue patronizing the firm after a breach (Madan, Savani, and Katsikeas 2023). Some may even internalize the event, attributing it to their own confusion or lack of vigilance, leading them to feel disappointed or resigned, but not deeply wronged (Dommeyer and Gross 2003). In contrast, high-resource customers, or those actively engaged in managing their privacy, likely perceive the breach as far more consequential. Their awareness of the complexity and sensitivity of their data, coupled with proactive efforts to protect it, creates a belief that they are doing their part and that the firm will do the same (Camacho, de Jong, and Stremersch 2014). A breach shatters that belief. What was once abstract risk is now real harm, triggering a sharp sense of betrayal. For these customers who anticipated and were better prepared, the breach feels unfair, ultimately intensifying privacy violation.

In the aftermath of a breach, privacy resources influence how customers perceive the residual risk, shaping whether they feel overwhelmed and stuck or empowered to act and move forward. Customers with low levels of privacy resources often lack the knowledge or confidence to understand what went wrong, or how to protect themselves in its aftermath (Brough, Kamleitner, and Martin 2023). As a result, they may experience heightened privacy fatigue, frustrated by their data exposure but uncertain how to respond. This privacy fatigue will only be compounded by a perceived lack of agency: when continued use of the service feels unavoidable, customers may feel trapped in the relationship (Gelbrich 2010). If they reengage, it is likely out of resignation rather than autonomy, perpetuating a cycle of privacy fatigue and renewed privacy vulnerability. In contrast, customers with high levels of privacy resources may experience greater privacy violation in the breach stage, but they are better equipped to recover in its aftermath. Their knowledge should help them assess the implications of the breach, and their motivation should fuel meaningful action, whether by strengthening privacy protections on their own, demanding redress, or switching providers. These actions help restore a sense of autonomy. Consequently, we propose that privacy resources serve as a buffer against post-breach fatigue, enabling individuals to reengage on their own terms.

> **Tenet 5 (Privacy Resources Tenet):** Customers' privacy resources moderate how they perceive risk associated with the firm's data-related power across the customer privacy journey. Pre-data breach, both low and high resource levels heighten perceived disclosure risk, increasing privacy vulnerability. During a data breach, high-resource customers perceive the realized risk as more serious, increasing privacy violation. Post-data breach, high resource levels help customers manage any residual risk, reducing privacy fatigue.

Moderating Role of Customer Relational Expectations

We consider a second important factor: customer relational expectations, which shape privacy experiences across the privacy journey as they anchor them in the broader customer–firm relationship and influence whether customers trust the firm's use of data-related power.

In the pre-breach stage, relational expectations shape how customers perceive the act of data collection, whether it signals mutual respect and benevolent intent, or a transactional request driven by unclear or self-interested motives. In trusted relationships, customers develop expectations based on consistent, respectful firm behavior (Grégoire and Fisher 2006; Palmatier et al. 2006). These expectations create informal relational norms that promote comfort and reduce uncertainty in data exchange relationships (Schlosser, White, and Lloyd 2006; Zhang et al. 2016), which in turn lowers the psychological weight of personal data collection. When customers view the firm as relationally committed, data collection and sharing feel safe—a reflection of mutual respect rather than just a power imbalance, likely reducing feelings of privacy vulnerability. This perceived safety functions similarly to the type of intervention we propose at this stage: one that delivers a sense of security. In contrast, when relational expectations are weak or underdeveloped, such as in newer, transactional, or calculative relationships (Palmatier 2008), customers lack a reliable basis for assessing the firm's intent. Data collection may feel abrupt or extractive without a foundation of prior fairness or shared norms, intensifying feelings of privacy vulnerability.

When a breach occurs, relational expectations influence how customers perceive the meaning of the event, shaping whether it is seen as a recoverable lapse or a transformational betrayal of trust. While pre-breach beliefs can be reinforced through firm behaviors that foster safety and trust, a breach threatens those beliefs, especially if it contradicts assumptions about the firm's benevolence in managing the relationship (Harmeling et al. 2015). For customers with high relational expectations, such disconfirmations are especially potent. They are more likely to see the breach not as a technical mishap, but as a relational, moral failure that undermines mutual respect, fairness, and trust (Harmeling et al. 2015; Komarova Loureiro, Haws, and Bearden

2018). For example, in such instances, a long-tenured customer may come to reinterpret years of trust-building as manipulative or hollow, prompting a sharp reassessment of the relationship (Baxter and Bullis 1986). These disconfirmations evoke strong feelings of betrayal and trigger relational sensemaking and detachment (Grégoire and Fisher 2008), thereby amplifying privacy violation. In contrast, customers with low relational expectations may still feel frustrated or disappointed but are less likely to see the breach as a serious relational failure. Their broader "zone of indifference" allows them to view such events as unfortunate but not surprising (Harmeling et al. 2015; Parasuraman, Zeithaml, and Berry 1994). Because the event does not violate a deeply held relational standard, the psychological impact is muted, and privacy violation is lowered.

In the aftermath of a breach, relational expectations shape how customers perceive the firm's breach response—what it did or did not do—ultimately determining whether they spiral into privacy fatigue or regain some degree of trust during the transition. For customers with high relational expectations, a poor or absent breach response likely reinforces the sense of betrayal and extends their feelings of privacy violation, ultimately deepening the rupture in the relationship (Grégoire and Fisher 2008). Lingering privacy violation likely heightens sensitivity to residual risk, leading to greater privacy fatigue. Customers may feel especially emotionally exhausted, increasingly cynical, and disengaged from the firm's privacy efforts. Alternatively, for these same customers, a high-quality, justice-oriented breach response, such as the kind of intervention we propose during the breach stage, may preserve or partially restore trust as the customer transitions into this post-breach stage. When firms demonstrate accountability, customers with high relational expectations may reinterpret the breach as an isolated lapse and extend forgiveness (Aquino, Tripp, and Bies 2006; Nikkhah and Grover 2022). This should help them avoid intense privacy fatigue. Yet, this benefit of the doubt is finite: repeated failures with the focal firm can erode forgiveness, leading even committed customers to harden into resentment and detachment (Grégoire, Laufer, and Tripp 2010).

For customers with low relational expectations, a poor response is often anticipated and merely reinforces their already low regard for the firm (Grégoire and Fisher 2008). This exacerbates privacy fatigue through resignation rather than betrayal. Even if a strong, justice-focused intervention occurs, it may do little to buffer their privacy fatigue, as there is no relational foundation to rebuild from. In these cases, privacy fatigue arises not from relational disruption but from the absence of meaningful relational investment to begin with. Thus, in the post-breach stage, relational expectations do not exert a uniform influence. Rather, they interact with the firm's breach response to determine whether privacy fatigue is intensified, mitigated, or sustained.

> **Tenet 6 (Relational Expectations Tenet):** Customers' relational expectations moderate their trust in the firm's use of data-related power across the privacy journey. Pre-data breach, high expectations foster trust in the data exchange, decreasing privacy vulnerability. During a data breach, high expectations heighten the likelihood of perceiving the event as a relational failure, increasing privacy violation. Post-data breach, high expectations increase privacy fatigue if the firm's response is absent or weak but help restore trust when the response is strong.

Illustrative Example of the Customer Privacy Journey

We offer preliminary proof of concept for the privacy journey by overlaying longitudinal survey insights capturing customers' evolving privacy experiences onto secondary YouGov BrandIndex data on brand advocacy behaviors. The recent AT&T breach serves as a highly relevant example, as we captured their customers' real-time reactions shortly after the breach was made public, and its scale and scope were substantial, affecting nearly 110 million customers (Chapman 2024).

Importantly, a range of privacy architectures supported AT&T customers, including internal firm initiatives and regulatory frameworks, before, during, and after the breach. AT&T maintained a data security audit committee, appointed a chief security officer, followed National Institute of Standards and Technology best practices, complied with international and state-level regulations (e.g., GDPR and CPRA), conducted compliance reviews, and promoted customer education through the National Cybersecurity Alliance and AT&T Cyber Aware (AT&T 2025).

Longitudinal Survey Design, Sample, and Methodological Details

We conducted a three-wave longitudinal survey of AT&T customers following the breach announced in July 2024. Each wave included open-ended questions inviting participants to reflect on their experiences. Wave 1, fielded shortly after the breach announcement, asked respondents to describe their feelings before and immediately after learning of the incident (e.g., “How did you feel about your data privacy with AT&T before the breach?”). In Waves 2 and 3, participants reported how they felt at the time of each survey. In Wave 2, after the open-ended portion, participants completed a matching task, categorizing feelings of privacy vulnerability, violation, and fatigue at three key points: before the breach, immediately after the breach, and at the time of the survey. This design allowed triangulation of psychological reactions while minimizing demand effects. Web Appendix A reports full methodological details.

Participants were recruited using Prolific filters for AT&T customers, with screening questions to confirm eligibility. The initial survey (n = 490; M_{Age} = 38.37 years; 63.3% female, 37.9% male, 1.6% non-binary, and .2% other) launched 12 days after AT&T publicly confirmed the breach. Participants who completed the initial survey were invited to Wave 2 (n = 315; 64% response rate), and those who completed Wave 2 were invited to Wave 3 (n = 211; 67% response rate), administered approximately two and four months later. The longitudinal design allowed us to track changes in psychological reactions over time. We analyzed open-ended responses using the human–LLM (large language model) method introduced by Arora, Chakraborty, and Nishimura (2025). With targeted prompts, the LLM identified whether responses reflected key elements of our proposed framework and extracted illustrative quotes for each stage of the privacy journey. To validate these findings, two independent coders blind to the research questions reviewed the responses to confirm the presence and interpretation of identified themes.

Brand Advocacy Design, Sample, and Methodological Details

We complemented the survey insights with YouGov BrandIndex data tracking customer perceptions. Our dependent variable, brand advocacy, is a key indicator of behavioral engagement (Harmeling et al. 2017), measured by the percentage of respondents recommending or avoiding the brand (–100% to 100%). To reduce selection bias, YouGov surveys 5,000 people daily from a 7-million-member panel balanced on demographic benchmarks. This real-time data allows consistent comparisons over time (Rust et al. 2021), enabling analysis of AT&T's brand advocacy shifts after the breach against customers of its competitors: T-Mobile, Verizon, US Cellular, Lumen, and Xfinity Mobile. Our analysis focuses on customers of each brand, rather than the general population. We use a two-way fixed effects heterogeneous treatment effects difference-in-differences (DID) model (Wooldridge 2021), where AT&T serves as the treatment group and competitors as controls. The study covers April 2024 to January 2025, three months pre- and six months post-breach, with 234 balanced weekly observations across the six brands. Web Appendix B reports full methodological details.

We include controls for advertising awareness and word-of-mouth (WOM) exposure obtained from YouGov, as both may independently affect brand advocacy. Advertising awareness is measured by: "Have you seen advertising for this brand in the past two weeks?"

and WOM by “Have you talked about this brand in the past two weeks?” Both are expressed as percentages (0% to 100%). Brand fixed effects account for time-invariant brand-level characteristics, such as baseline perceptions or marketing strategies, and week fixed effects adjust for time-varying factors affecting all brands, such as seasonality or macroeconomic conditions. We break down the insights across the privacy journey, and Figure 2 offers a summary overview.

Initial Evidence of Customer Privacy Journey

Insights into the pre-data breach stage. The privacy journey begins when customers become aware of data collection, entering the pre-breach stage, where we theorize that they experience privacy vulnerability. In Wave 1 responses, the human–LLM method revealed that privacy vulnerability was widespread; respondents felt vulnerable, unsafe, or concerned before learning about the breach. While Figure 2 and Web Appendix A provide additional examples, some illustrative quotes include: “I did not feel…safe about my data privacy,” and “My data…was always at risk.” These findings are reinforced by Wave 2’s matching task, in which 75% of respondents categorized privacy vulnerability as the dominant psychological reaction in the pre-breach phase.

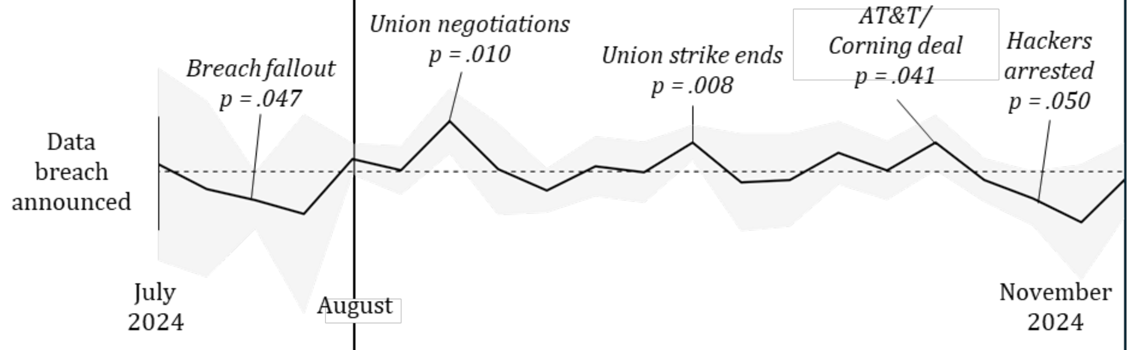
AT&T’s customer brand advocacy remained stable relative to that of its industry peers’ pre-breach (i.e., the pre-treatment phase). While this stability supports the parallel trends assumption required for our difference-in-differences estimation ($F(4, 5) = .89$, $p = .530$), it also reveals a disconnect: behavioral parity does not imply psychological security. Even in the absence of observable relative declines in brand advocacy, customers still felt vulnerable within their data exchange relationships. This underscores the importance of detecting latent privacy vulnerability and seizing opportunities for proactive intervention early in the privacy journey.

Figure 2. Illustrative Case Example of Customer Privacy Journey

Pre-Data Breach Stage	Data Breach Stage	Post-Data Breach Stage
Primary psychological reaction and illustrative quotes from the longitudinal survey[1]		
"I did not feel…safe about my data privacy," "My data and privacy [were] vulnerable," "my data was [not] protected very well," "My data…was always at risk," "I wasn't super confident that they were taking measures to be secure."	*"I felt violated," "I personally feel violated… my data could possibly be on the black market," "I felt betrayed…my privacy had been violated," "I feel disappointed and violated…a better job should have been done," "Betrayed."*	*"My data has been breached too many times to count," "There are so many data breaches…that I just don't care anymore," "It is a pretty hopeless situation that is unavoidable," "I don't really feel like there is anything I can do these days but let all these companies fumble my information and expect a $5 apology," "I still feel that my data could constantly be at risk of being breached," "Data being leaked seems like a fact of life," "Many of us have been desensitized to announcements about privacy concerns."*
Sense of Vulnerability (75% of AT&T customers)	**Sense of Violation** (80% of AT&T customers)	**Sense of Privacy Fatigue** (75% of AT&T customers)

Data breach effect on AT&T customer brand advocacy compared to the industry using YouGov BrandIndex data[2]

AT&T's brand advocacy did not differ significantly from industry peers during the pre-treatment period, indicating that the parallel trends assumption was met ($p = .478$).



AT&T Customer Privacy Journey

Continuity loop

[1] Longitudinal surveys were conducted with AT&T customers. Web Appendix A reports details. [2] Effects represent the average treatment effect on the treated, estimated using a heterogeneous difference-in-differences approach. AT&T is treated following the data breach, with industry competitors as the control group. Statistically significant effects are indicated; analytical details are available in Web Appendix B.

Insights into the data breach stage. Once a breach occurs, customers enter the breach stage of the privacy journey, where we theorize that disclosure risk becomes realized, triggering psychological reactions of privacy violation. We again applied the human–LLM methodology to analyze open-ended survey responses from Wave 1. When prompted about whether participants reported privacy violation immediately following the breach, the LLM confirmed that many expressed strong feelings of violation, betrayal, and fear of misuse. While Figure 2 and Web Appendix A include additional examples, some illustrative quotes include: “I felt violated,” and “I felt betrayed…my privacy had been violated.” These patterns are reinforced by results from the Wave 2 matching task, in which 80% of respondents associated privacy violation with the breach stage.

The brand advocacy data provides converging support. Following the breach disclosure in July 2024, we observe a significant negative average treatment effect on brand advocacy for AT&T (ATT = –20.13, p = .047), consistent with public backlash and media demands for firm accountability. Although the breach stage can vary in length, this decline in brand advocacy appears short-lived: within approximately four weeks, brand advocacy levels begin to recover, and subsequent treatment effects are no longer statistically significant.

Insights into the post-data breach stage. Customers enter the post-breach stage, typically triggered by a firm’s response or, in its absence, by the passage of time. AT&T offered no notable customer-facing breach recovery effort beyond the breach disclosure, suggesting a time-driven transition into the post-breach stage. To assess evolving customer privacy experiences, we analyzed open-ended responses from Wave 2, administered approximately two months after the breach was made public. Participants were asked how they currently felt about the incident. Applying the human–LLM methodology, we found that many participants expressed signs of privacy fatigue, including emotional exhaustion and cynicism. These sentiments had overtaken earlier feelings of privacy vulnerability and violation, signaling a wearier psychological reaction at this stage. Figure 2 and Web Appendix A provide additional examples, but some illustrative quotes include: “My data has been breached too many times to count,” and “It is a pretty hopeless situation that is unavoidable.” These insights are reinforced by the Wave 2 matching task, in which 83% of respondents identified privacy fatigue as the dominant psychological reaction in the post-breach stage, aligning with our theorizing.

Brand advocacy patterns provide additional context. Post-breach, AT&T experienced a series of short-term positive effects in August (ATT = 35.57, p = .010), September (ATT = 20.49, p = .008), and October (ATT = 20.50, p = .041), likely driven by unrelated developments such as union negotiations (CWA 2024; Hyde 2024) and a $1 billion partnership with Corning (Reuters 2024). However, brand advocacy declined again in November when the hackers responsible for the breach were arrested (ATT = –18.88, p = .050). This pattern is consistent with privacy fatigue building below the surface, temporarily obscured by unrelated news but reactivated and linked to negative brand advocacy when the breach resurfaces in public attention.

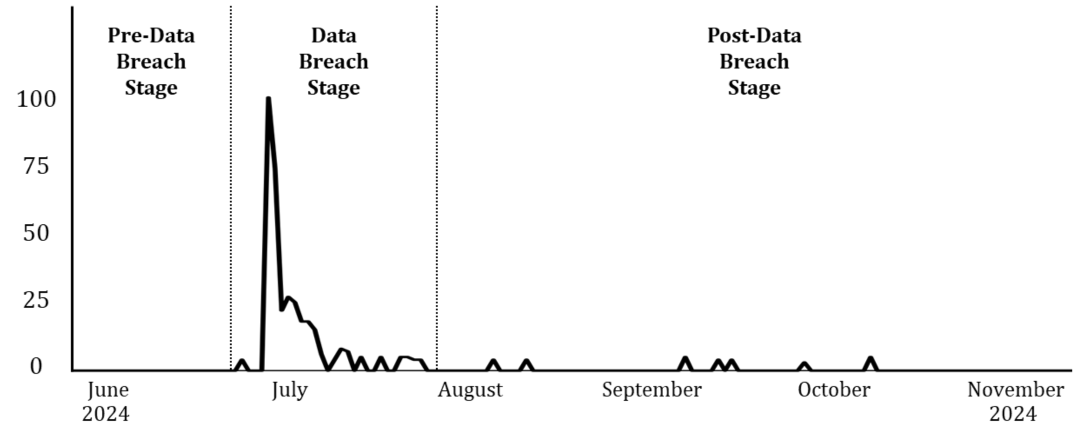
Insights into the continuity loop. Based on our theorizing, the privacy journey loops back to a new pre-breach stage (t + 1), for returning customers, where they once again encounter data collection and disclosure risk—reviving privacy vulnerability shaped by lingering privacy fatigue. To assess this reentry point, we analyzed open-ended responses from Wave 3, conducted approximately four months after the breach was announced. The human–LLM analysis revealed renewed and deepened privacy vulnerability among participants. Illustrative quotes include: “I have been getting more spam calls and texts...I feel scared and I know my info is out on the dark web now,” and “It’s hard not to wonder if this could happen again, or whether they truly have the necessary protections in place to prevent further incidents” (see also Web Appendix A).

Privacy fatigue also remained a persistent theme, suggesting its carryover. Some participants once again described emotional exhaustion and cynicism. For example: "I am still frustrated it took place, but I have accepted that it happened and don't dwell on it," and "At this point, I assume my data has been leaked by just about every company that has it." To explore whether privacy fatigue intensified over time, we also asked the LLM to assess longitudinal patterns across the three survey waves. The model confirmed early signs of privacy fatigue even before the breach occurred, salient privacy fatigue post-breach, and persistent privacy fatigue as customers reentered the pre-breach stage. This suggests not only that fatigue persists, but that it may accumulate, especially in the absence of meaningful firm interventions. Of note, AT&T operated under a range of robust privacy architectures yet still encountered negative customer psychological reactions, reinforcing our theorizing that while these structures are necessary, they are not sufficient to alleviate such reactions.

These findings further underscore the importance of integrating firm-level behavioral indicators with customer-level psychological insights when assessing privacy journeys. YouGov data shows that brand advocacy rebounded in the months following the breach, but such metrics may paint a misleading picture. Open-ended responses reveal signs of latent privacy fatigue that persists beneath early behavioral recovery and, in some cases, may intensify over time.

Robustness check. As a robustness check, we accessed Google Search Trends data to examine public interest in the AT&T breach. Given the breach's scale, these searches likely include many AT&T customers. The results mirror the YouGov brand advocacy pattern: an initial spike in AT&T breach-related searches followed by a tapering decline after about four weeks (Figure 3). Together, these patterns suggest that while behavioral and attention indicators may normalize quickly, they fail to capture the full psychological arc of the privacy journey.

Figure 3. AT&T Data Breach Search Intensity



Note: This figure shows the normalized Google search interest in the United States for the search term "att data breach."

General Discussion and Implications

By establishing a framework of the privacy journey, this research offers a foundation for rethinking privacy as a dynamic, ongoing experience. The model outlines three stages: pre-breach, where disclosure risk induces psychological reactions of privacy vulnerability; breach, where realized risk triggers privacy violation; and post-breach, where residual risk gives rise to privacy fatigue. The journey is cyclical for customers who remain in the data exchange relationship, carrying privacy fatigue into subsequent experiences. It unfolds within surrounding privacy architectures, which guide, but do not define, firm intervention. Each stage corresponds to a distinct intervention: security, justice, and autonomy, respectively. The framework also identifies two key customer-level moderators of privacy resources and relational expectations, which shape how customers perceive risk in and interpret the firm's use of power across the journey. In doing so, it offers several theoretical, managerial, and policy implications.

Theoretical Implications

This research introduces a dynamic, multi-stage privacy journey framework that reconceptualizes privacy as an evolving experience embedded in customer–firm data exchange relationships. While it builds on customer journey literature (e.g., Hamilton et al. 2021; Lemon and Verhoef 2016), the framework is uniquely grounded in the interplay of persistent data-related power imbalances, risk-related inflection points, and the structural role of privacy architectures. It also moves beyond static, rational-choice models of privacy that treat power as a fixed feature of the external environment (e.g., Lwin, Wirtz, and Williams 2007), by explaining how customers react to power imbalances depending on their stage of the privacy journey, privacy resources, and relational expectations. In doing so, we reposition privacy as a psychologically and relationally embedded process shaped by ongoing power asymmetries and evolving patterns of perceived risk and trust.

Moreover, by conceptualizing the privacy journey as cyclical rather than linear, our framework challenges prevailing assumptions in privacy research that treat breaches as isolated events with finite recovery arcs, extending prior work in this area (e.g., Rasoulian et al. 2017; Turjeman and Feinberg 2024). We theorize that privacy experiences accumulate and recur such that prior exposure to risk reshapes how customers enter and interpret subsequent interactions. This cyclical view emphasizes the temporal depth and recursive nature of privacy fatigue. Rather than assuming behavioral normalization signals psychological resolution, we show that customers may experience lingering privacy fatigue after outward engagement resumes. Justice-oriented responses may be necessary but insufficient; autonomy-restoring interventions become critical when fatigue sets in. In this way, we contribute to the emerging conversation on privacy fatigue (Chen et al. 2023; Choi, Park, and Jung 2018), highlighting it as a distinct psychological outcome that reshapes the customer–firm data exchange relationship and extends broader marketing research on customer fatigue in digital contexts (e.g., Ursu, Zhang, and Honka 2023).

Finally, we extend prior views of privacy resources, which are mostly treated as protective (e.g., Brough and Martin 2020). Our framework advances that both low and high levels of privacy resources can heighten privacy vulnerability, either through a lack of understanding or hyper-vigilance. This purportedly U-shaped relationship invites a rethinking of privacy and digital literacy, inviting deeper theorizing and exploration into privacy resource-based constructs in future research. Together, these contributions advance emerging discussion around customer well-being, power dynamics, and firm responsibility in digital environments.

Practical Implications

The privacy journey framework offers strategic insight into managing privacy as an evolving customer experience, rather than a static compliance function or isolated crisis. It calls for more intentional coordination between firms and policy makers to address the ongoing nature of customers' privacy experiences. Contrary to some firm practices and regulatory assumptions, customers do not simply opt in or out of data collection or react only at the moment of a breach. They navigate psychological reactions of privacy vulnerability, violation, and fatigue that unfold over time and reshape trust in the firm. Critically, these experiences are not linear or self-contained, which has practical consequences. Surface-level behavior may normalize after a breach, but psychological reactions of lingering fatigue and distrust may accumulate, quietly undermining the data exchange relationship over time. Firms must go beyond static compliance, aligning interventions with customers' stages in the privacy journey, privacy resources, and relational expectations, all within the broader conditions of privacy architectures.

While firms have traditionally relied largely on privacy architectures to guide behavior, these structures are insufficient on their own. As shown in the AT&T example, privacy architectures may enable or constrain certain actions but do not account for how customers perceive power, interpret risk, or evaluate trust over time. Addressing today's privacy challenges requires strategies that are dynamic, psychologically attuned, and relationally grounded.

Privacy resources and relational expectations carry double-edged implications. Customers with high privacy resources may seem better equipped to manage disclosure risk, but that same awareness heightens their privacy vulnerability and increases the need for firm intervention. Strong relational expectations may build trust early on but raise psychological stakes during and after a breach. If the firm's response falls short, these customers are more likely to feel violated and disengage. In short, the very qualities that signal strong pre-breach relationships can intensify harm when mismanaged.

Firms must deliver distinct forms of support at each stage of the journey. In the pre-breach stage, customers seek a sense of security, especially when they lack the resources to evaluate risk, are equipped with so many resources that they become hyper-aware, or lack the relationship history to infer benevolent intent. During a breach, firms must restore justice through clear, timely, and sincere responses, particularly when customers hold high expectations of accountability and fairness, as is often the case for those with elevated privacy resources and strong relational expectations. Post-breach, firms must restore autonomy, especially for customers experiencing privacy fatigue, which is more likely among those with low privacy resources or weak relational expectations, as they lack the capacity or trust foundation to reengage with privacy efforts on their own. This challenges the assumption that more control is always better (Zimmermann et al. 2024); when fatigued, customers may find too much control overwhelming. What matters most is the ability to engage with privacy on one's own terms.

Finally, both firms and policy makers must look beyond behavioral signals to manage the full privacy journey. Outward engagement may resume after a breach, but psychological strain, especially privacy fatigue, can quietly destabilize the relationship. Firms should integrate sentiment measures and early indicators of privacy fatigue into customer relationship systems to detect distress before it becomes visible or leads to churn. Privacy regulations must also evolve. Most focus on procedural compliance or one-time breach responses, overlooking how psychological strain unfolds and accumulates over time. To be effective, privacy regulations must move beyond one-time protections toward flexible enforcement standards and design principles that reflect the long-term psychological arc of customer privacy journeys.

Future Research Agenda

The privacy journey framework centers on customer–firm data exchange relationships, which form the foundation of customer privacy experiences. By establishing this foundation, this research invites new perspectives on privacy as an evolving experience. It encourages empirical inquiry into the psychological dynamics, strategic interventions, and privacy architectures that shape data exchange over time, as outlined in six core tenets. It also offers a platform for extensions across customer psychology, firm strategy, and institutional contexts.

How customer privacy experiences evolve within individuals. Our framework acknowledges that customers may remain in the pre-breach stage for prolonged or indefinite periods, if they have not encountered a breach or if substantial time has passed since they last re-entered the stage. Future research can examine whether extended time in this stage reduces privacy vulnerability, as firms might hope, or gives rise to complacency, which is likely marked by overconfidence and low vigilance in privacy management (e.g., Westin 2003). While the consequences of complacency may resemble those of privacy fatigue, complacency stems from unrealized risk and a false sense of safety instead of residual risk. Complacency may warrant scholarly attention as a latent form of vulnerability. Future research could investigate whether complacency is a stable trait or develops through safe privacy experiences, and how firms might re-engage complacent customers without accidentally triggering privacy vulnerability or privacy fatigue, such as through “newness cues” that renew attention (Wood and Lynch 2002). Detecting and differentiating complacency would sharpen firm targeting and enrich theory on psychological heterogeneity in the privacy journey.

Although our framework outlines stage-specific interventions, future research should examine how these efforts function in sequence. Do consistent firm actions across stages build credibility and trust, or does misalignment (e.g., strong messaging pre-breach but weak post-breach follow-through) undermine recovery? Prior work establishes that the personalization and sequencing of customer–firm communication significantly shapes outcomes (Moffett, Garretson Folse, and Palmatier 2021). Building on this insight, researchers could explore how to optimize the sequencing, timing, and personalization of privacy interventions to meet evolving customer needs. Longitudinal or field-based studies may reveal how customers evaluate the coherence of firm behavior across the privacy journey and how that shapes data exchange relationships.

Our framework also reconceptualizes post-breach recovery as an ongoing psychological process, where customers may initially re-engage while continuing to experience privacy fatigue. This construct, underexplored in prior research, may weaken the effectiveness of subsequent firm interventions or dampen long-term responsiveness to privacy efforts. Future research should explore this avenue and investigate how firms might detect early signals and incorporate them into customer relationship systems to support fatigue-sensitive interventions.

How customer privacy experiences scale across the digital ecosystem. Our framework centers on the focal customer–firm dyad, acknowledging that prior privacy experiences can include those with other firms. Future research could thus explore how privacy experiences are embedded within and shaped by broader network dynamics. These experiences may scale into market-level patterns of trust, disengagement, or governance, especially as customers interact with multiple firms and observe how others respond to privacy incidents. Privacy fatigue originates at the individual level but may spread across customer networks or market segments, eroding norms of data accountability or reducing participation in digital systems over time. Future research could explore whether privacy fatigue spreads in this way and how firms and institutions might respond through fatigue-sensitive design, cross-industry signaling, or coordinated governance.

Customer perceptions are shaped not only by direct firm actions but also by the behaviors, attitudes, and disclosures of peers. Prior work on social journeys shows that proximal others influence how individuals interpret and emotionally respond to key moments (Hamilton et al. 2021). Future research could examine how peer dynamics shape perceptions of disclosure, realized, and residual risk, particularly in public, collective, or involuntary privacy events (e.g., joint accounts, group data leaks, or algorithmic exposure). Firms also operate in interdependent networks. A breach at one firm may erode trust in others (Martin, Borah, and Palmatier 2017), while privacy leadership may raise expectations across the industry. Future work could investigate how firm-to-firm dynamics shape evolving perceptions of privacy risk and trust across interconnected platforms, partnerships, and digital ecosystems.

How social, institutional, and cultural systems shape customer privacy experience trajectories. Privacy resources, a key moderator in our framework, may be shaped by social and economic structures. Future research could examine how these privacy resources are developed, depleted, or replenished over time. Firm-led efforts such as educational outreach, inclusive design, or tiered support may help close resource gaps, but their effectiveness likely varies across populations. Socioeconomic status—defined by income, education, and occupational status (Scott et al. 2024)—may shape how privacy literacy is accessed and applied. For example, customers with strong literacy but low socioeconomic status may still experience privacy vulnerability, while those with high status but limited awareness may underestimate disclosure risk and thereby feel less vulnerable. Research could investigate these asymmetries and explore how different resource profiles shape privacy experiences and responses to firm interventions. This work could inform more targeted capacity-building strategies for both firms and policy makers.

Finally, although privacy architecture underpins the privacy journey, future research should explore how these structures evolve in response to macro-level legal, political, and cultural forces. External events such as the overturning of Roe v. Wade (Fitzgerald et al. 2023), immigration crackdowns, and conversations about digital rights and artificial intelligence may reshape perceptions of data risk, particularly for sensitive data like location, health, or genetics (Daviet, Nave, and Wind 2022). Studies could examine how such disruptions interact with customer-level privacy psychology. For instance, a firm's silence, neutrality, or advocacy in politically charged moments may shape customer trust even when the issue appears unrelated to data. These signals may be interpreted differently across cultures, depending on factors like power distance or uncertainty avoidance (Madan, Savani, and Katsikeas 2023). Exploring the intersection of institutional volatility, social values, and customer psychology could clarify how privacy expectations shift and how firms can sustain trust in increasingly complex environments.

In summary, our privacy journey conceptualization gives rise to a set of promising research directions that reinforce the dynamic nature of privacy experiences and offer a fruitful path for scholars to better understand and influence how customers and firms navigate power imbalances, risk, and trust in a dynamic, data-driven world.

References

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2020), "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving it in the Digital Age," *Journal of Consumer Psychology*, 30 (4), 736–58.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein (2012), "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research*, 49 (2), 160–74.

Agarwal, Sumit, Pulak Ghosh, Tianyue Ruan, and Yunqi Zhang (2024), "Transient Customer Response to Data Breaches of their Information," *Management Science*, 70 (6), 4105–14.

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko De Ruyter, and Martin Wetzels (2015), "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing*, 91 (1), 34–49.

Alashoor, Tawfiq, Mark Keil, H. Jeff Smith, and Allen R. McConnell (2023), "Too Tired and in Too Good of a Mood to Worry about Privacy: Explaining the Privacy Paradox through the Lens of Effort Level in Information Processing," *Information Systems Research*, 34 (4), 1415–36.

Alwafi, Ghadeer, and Bahjat Fakieh (2024), "A Machine Learning Model to Predict Privacy Fatigued Users from Social Media Personalized Advertisements," *Scientific Reports*, 14 (1), 3685.

Aquino, Karl, Thomas M. Tripp, and Robert J. Bies (2006), "Getting Even or Moving On? Power, Procedural Justice, and Types of Offense as Predictors of Revenge, Forgiveness, Reconciliation, and Avoidance in Organizations," *Journal of Applied Psychology*, 91 (3), 653–68.

Arora, Neeraj, Ishita Chakraborty, and Yohei Nishimura (2025), "AI–Human Hybrids for Marketing Research: Leveraging Large Language Models (LLMs) as Collaborators," *Journal of Marketing*, 89 (2), 43–70.

Ashworth, Laurence, and Clinton Free (2006), "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns," *Journal of Business Ethics*, 67 (2), 107–23.

AT&T (2025), "Cybersecurity," (accessed June 12, 2025), sustainability.att.com/priority-topics/cybersecurity.

Baxter, Leslie A., and Connie Bullis (1986), "Turning Points in Developing Romantic Relationships," *Human Communication Research*, 12 (4), 469–93.

Bhatnagar, Arjun (2023), "The Year of Consumer Privacy Empowerment," (January 3), www.forbes.com/councils/forbestechcouncil/2024/01/03/2023-the-year-of-consumer-privacy-empowerment/.

Bi, Sheng, Jun Pang, Huan Chen, and Andrew Perkins (2024), "When Feeling Powerless, We Crave Nostalgia: The Impact of Powerlessness on the Preference for Nostalgic Products," *Journal of the Academy of Marketing Science*, 52 (4), 998–1017.

Bleier, Alexander, Avi Goldfarb, and Catherine Tucker (2020), "Consumer Privacy and the Future of Data-Based Innovation and Marketing," *International Journal of Research in Marketing*, 37 (3), 466–80.

Bornschein, Rico, Lennard Schmidt, and Erik Maier (2020), "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices," *Journal of Public Policy & Marketing*, 39 (2), 135–54.

Bourdon, Bill (2017), "The Avoidable Mistakes Executives Continue to Make After a Data

Breach,” (November 20), https://hbr.org/2017/11/the-avoidable-mistakes-executives-continue-to-make-after-a-data-breach.

Brough, Aaron R., and Kelly D. Martin (2020), “Critical Roles of Knowledge and Motivation in Privacy Research,” *Current Opinion in Psychology*, 31, 11–15.

Brough, Aaron R., Bernadette Kamleitner, and Kelly D. Martin (2023), “Physical and Digital Privacy: How Developed and Developing Countries Differ in Both Vulnerability and Protection,” *Journal of International Marketing*, 31 (4), 76–79.

Brough, Aaron R., David A. Norton, Shannon L. Sciarappa, and Leslie K. John (2022), “The Bulletproof Glass Effect: Unintended Consequences of Privacy Notices,” *Journal of Marketing Research*, 59 (4), 739–54.

Camacho, Nuno, Martijn De Jong, and Stefan Stremersch (2014), “The Effect of Consumer Empowerment on Adherence to Expert Advice,” *International Journal of Research in Marketing*, 31 (3), 293–308.

Campbell, Margaret C., J. Jeffrey Inman, Amna Kirmani, and Linda L. Price (2020), “In Times of Trouble: A Framework for Understanding Consumers’ Responses to Threats,” *Journal of Consumer Research*, 47 (3), 311–26.

Chapman, Michelle (2024), “Data of nearly all AT&T customers downloaded from a third-party platform in security breach,” (July 13), https://apnews.com/article/att-data-breach-text-cell-b5cdc8d6c9e1b980cb2163f34b297dad.

Chen, Subai, Chenyu Gu, Juan Wei, and Mingjie Lv (2023), “Research on the Influence Mechanism of Privacy Invasion Experiences with Privacy Protection Intentions in Social Media Contexts: Regulatory Focus as the Moderator,” *Frontiers in Psychology*, 13, 1031592.

Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung (2018), “The Role of Privacy Fatigue in Online Privacy Behavior,” *Computers in Human Behavior*, 81, 42–51.

CWA (2024), “CWA and AT&T Enter Federal Mediation as Southeastern Strike Continues Over Unfair Labor Practices,” (August 21), https://cwa-union.org/news/releases/cwa-and-att-enter-federal-mediation-southeastern-strike-continues-over-unfair-labor.

Dagger, Tracey S., Peter J. Danaher, and Brian J. Gibbs (2009), “How Often versus How Long: The Interplay of Contact Frequency and Relationship Duration in Consumer-Reported Service Relationship Strength,” *Journal of Service Research*, 11 (4), 371–388.

Dalmia, Maansi, and Kristin Diehl (2025), “Privacy Is Important, but When Is It Thought About?” *Journal of the Association for Consumer Research*, 10 (3), 226–39.

Daviet, Remi, Gideon Nave, and Jerry Wind (2022), “Genetic Data: Potential Uses and Misuses in Marketing,” *Journal of Marketing*, 86 (1), 7–26.

Dommeyer, Curt J., and Barbara L. Gross (2003), “What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies,” *Journal of Interactive Marketing*, 17 (2), 34–51.

Duncan, George (2007), “Privacy by Design,” *Science*, 317 (5842), 1178–79.

Ermey, Ryan (2024), “‘The Worst Thing You Can Do’ After a Data Breach, according to a Cybersecurity Expert,” (accessed June 12, 2025), www.cnbc.com/2024/07/30/cybersecurity-expert-the-worst-thing-to-do-after-a-data-breach.html.

Evans, David C., Alisa Bacon, Christophe Berthoud, and Abigail Steinem (2025), “Toward a More Human-Centered View of Privacy Needs: An Industry Perspective,” *Journal of the Association for Consumer Research*, 10 (3), 240–48.

Fitzgerald, M. Paula, Jeff Langenderfer, Roberta Renzelli-Cain, and Elizabeth A. Critch (2023), “Marketing and Public Policy Implications of Dobbs v. Jackson Women’s Health Organization,” *Journal of Public Policy & Marketing*, 42 (4), 303–25.

Forbes, Ahjané (2024), “Cash App $15M Security Settlement Deadline is Here. What You Need to Know to File a Claim,” (November 18), www.usatoday.com/story/money/personalfinance/2024/11/18/cash-app-security-settlement-claims-breach/76359226007/.

Fournier, Susan, and Claudio Alvarez (2013), “Relating Badly to Brands,” *Journal of Consumer Psychology*, 23 (2), 253–64.

FTC (2025), “Data Breach Response: A Guide for Business,” (accessed June 12, 2025), www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

Gaski, John F., and John R. Nevin (1985), “The Differential Effects of Exercised and Unexercised Power Sources in a Marketing Channel,” *Journal of Marketing Research*, 22 (2), 130–42.

Gelbrich, Katja (2010), “Anger, Frustration, and Helplessness after Service Failure: Coping Strategies and Effective Informational Support,” *Journal of the Academy of Marketing Science*, 38 (5), 567–85.

Giddens, Anthony (1991), *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Stanford University Press.

Goldsteen, Abigail, Gilad Ezov, Ron Shmelkin, Micha Moffie, and Ariel Farkash (2022), “Data Minimization for GDPR Compliance in Machine Learning Models,” *AI and Ethics*, 2 (3), 477–91.

Grégoire, Yany, and Robert J. Fisher (2008), “Customer Betrayal and Retaliation: When Your Best Customers Become Your Worst Enemies,” *Journal of the Academy of Marketing Science*, 36 (2), 247–61.

Grégoire, Yany, Fateme Ghadami, Sandra Laporte, Sylvain Sénécal, and Denis Larocque (2018), “How Can Firms Stop Consumer Revenge? The Effects of Direct and Indirect Revenge on Post-Complaint Responses,” *Journal of the Academy of Marketing Science*, 46 (6), 1052–71.

Grégoire, Yany, Daniel Laufer, and Thomas M. Tripp (2010), “A Comprehensive Model of Consumer Direct and Indirect Revenge: Understanding the Effects of Perceived Greed and Consumer Power,” *Journal of the Academy of Marketing Science*, 38 (6), 738–58.

Gwebu, Kholekile L., Jing Wang, and Li Wang (2018), “The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management,” *Journal of Management Information Systems*, 35 (2), 683–714.

Hamilton, Ryan, Rosellina Ferraro, Kelly L. Haws, and Anirban Mukhopadhyay (2021), “Traveling with Companions: The Social Consumer Journey,” *Journal of Marketing*, 85 (1), 68–92.

Hargittai, Eszter, and Alice Marwick (2016), “‘What Can I really do?’ Explaining the Privacy Paradox with Online Apathy,” *International Journal of Communication*, 10, 21.

Harmeling, Colleen M., Jordan W. Moffett, Mark J. Arnold, and Brad D. Carlson (2017), “Toward a Theory of Customer Engagement Marketing,” *Journal of the Academy of Marketing Science*, 45 (3), 312–35.

Harmeling, Colleen M., Robert W. Palmatier, Mark B. Houston, Mark J. Arnold, and Stephen A. Samaha (2015), “Transformational Relationship Events,” *Journal of Marketing*, 79 (5), 39–62.

Hyde, Marlon (2024), “AT&T Reaches Deal with Union Telecom Workers, Ending Southeast Strike,” (September 16), www.wabe.org/att-reaches-deal-with-union-telecom-workers-ending-southeast-strike/.

ITRC (2025), “2024 Data Breach Report,” (January 28), www.idtheftcenter.org/publication/2024-data-breach-report/.

Janakiraman, Ramkumar, Joon Ho Lim, and Rishika Rishika (2018), “The Effect of a Data Breach Announcement on Consumer Behavior: Evidence from a Multichannel Retailer,” *Journal of Marketing*, 82 (2), 85–105.

Johnston, Kristin (2023), “Data Privacy Can Be a Competitive Advantage,” (accessed June 13, 2024), www.bloomberglaw.com/external/document/XB3VGCMG000000/data-collection-management-professional-perspective-data-privacy.

Kähr, Andrea, Bettina Nyffenegger, Harley Krohmer, and Wayne D. Hoyer (2016), “When Hostile Consumers Wreak Havoc on Your Brand: The Phenomenon of Consumer Brand Sabotage,” *Journal of Marketing*, 80 (3), 25–41.

Kindermann, Bastian, Daniel Wentzel, David Antons, and Torsten-Oliver Salge (2024), “Conceptual Contributions in Marketing Scholarship: Patterns, Mechanisms, and Rebalancing Options,” *Journal of Marketing*, 88 (3), 29–49.

Komarova Loureiro, Yuliya, Kelly L. Haws, and William O. Bearden (2018), “Businesses Beware: Consumer Immoral Retaliation in Response to Perceived Moral Violations by Companies,” *Journal of Service Research*, 21 (2), 184–200.

Kost, Edward (2024), “How Did the Cash App Data Breach Happen?” (accessed June 13, 2025), www.upguard.com/blog/how-did-the-cash-app-data-breach-happen.

Kozlenkova, Irina V., Caleb Warren, Suresh Kotha, Reihane Boghrati, and Robert W. Palmatier (2024) “Conceptual Research: Multidisciplinary Insights for Marketing,” *Journal of Marketing*, published online November 16, https://doi.org/10.1177/00222429241302814.

Krafft, Manfred, V. Kumar, Colleen Harmeling, Siddharth Singh, Ting Zhu, Jialie Chen, Tom Duncan, Whitney Fortin, and Erin Rosa (2021), “Insight is Power: Understanding the Terms of the Consumer–Firm Data Exchange,” *Journal of Retailing*, 97 (1), 133–49.

Labrecque, Lauren I., Jonas Vor Dem Esche, Charla Mathwick, Thomas P. Novak, and Charles F. Hofacker (2013), “Consumer Power: Evolution in the Digital Age,” *Journal of Interactive Marketing*, 27 (4), 257–69.

Lemon, Katherine N., and Peter C. Verhoef (2016), “Understanding Consumer Experience Throughout the Consumer Journey,” *Journal of Marketing*, 80 (6), 69–96.

Lessig, Lawrence. *Code: And Other Laws of Cyberspace*. New York, N.Y: Basic Books, 1999.

Lwin, May, Jochen Wirtz, and Jerome D. Williams (2007), “Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective,” *Journal of the Academy of Marketing Science*, 35 (4), 72–85

Malhotra, Arvind, and Claudia Kubowicz Malhotra (2011), “Evaluating Consumer Information Breaches as Service Failures: An Event Study Approach,” *Journal of Service Research*, 14 (1), 44–59.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier (2017), “Data Privacy: Effects on Consumer and Firm Performance,” *Journal of Marketing*, 81 (1), 36–58.

Martin, Kelly D., and Patrick E. Murphy (2017), “The Role of Data Privacy in Marketing,” *Journal of the Academy of Marketing Science*, 45, 135–55.

Melzner, Johann, Andrea Bonezzi, and Tom Meyvis (2023), “Information Disclosure in the Era of Voice Technology,” *Journal of Marketing*, 87 (4), 491–509.

Mende, Martin, Tonya Williams Bradford, Anne L. Roggeveen, Maura L. Scott, and Mariella Zavala (2024), “Consumer Vulnerability Dynamics and Marketing: Conceptual Foundations and Future Research Opportunities,” *Journal of the Academy of Marketing Science*, 1–22.

Moffett, Jordan W., Judith Anne Garretson Folse, and Robert W. Palmatier (2021), "A Theory of Multiformat Communication: Mechanisms, Dynamics, and Strategies," *Journal of the Academy of Marketing Science*, 49 (3), 441–61.

Nikkhah, Hamid Reza, and Varun Grover (2022), "An Empirical investigation of company Response to Data Breaches," *MIS Quarterly*, 46 (4), 2163–96.

Okazaki, Shintaro, Martin Eisend, Kirk Plangger, Ko de Ruyter, and Dhruv Grewal (2020), "Understanding the Strategic Consequences of Consumer Privacy Concerns: A Meta-Analytic Review," *Journal of Retailing*, 96 (4), 458–473.

Olukoya, Oluwafemi (2022), "Assessing Frameworks for Eliciting Privacy & Security Requirements from Laws and Regulations," *Computers & Security*, 117, 102697.

Palmatier, Robert W. (2008), *Relationship marketing*. Marketing Science Institute.

Palmatier, Robert W., Rajiv P. Dant, Dhruv Grewal, and Kenneth R. Evans (2006), "Factors Influencing the Effectiveness of Relationship Marketing: A Meta-Analysis," *Journal of Marketing*, 70 (4), 136–153.

Palmatier, Robert W., Mark B. Houston, Rajiv P. Dant, and Dhruv Grewal (2013), "Relationship Velocity: Toward a Theory of Relationship Dynamics," *Journal of Marketing*, 77 (1), 1–30.

Palmatier, Robert W., and Kelly D. Martin (2019), *The intelligent marketer's guide to data privacy: The impact of big data on consumer trust*. Springer International Publishing.

Parasuraman, Ananthanarayanan, Valarie A. Zeithaml, and Leonard L. Berry (1994), "Reassessment of Expectations as a Comparison Standard in Measuring Service Quality: Implications for Further Research," *Journal of Marketing*, 58 (1), 111–24.

Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis (2018), "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions," *Journal of Cybersecurity*, 4 (1), tyy001.

Rasoulian, Shahin, Yany Grégoire, Renaud Legoux, and Sylvain Sénécal (2017), "Service Crisis Recovery and Firm Performance: Insights from Information Breach Announcements," *Journal of the Academy of Marketing Science*, 45 (6), 789–806.

Rasoulian, Shahin, Yany Grégoire, Renaud Legoux, and Sylvain Sénécal (2023), "The Effects of Service Crises and Recovery Resources on Market Reactions: An Event Study Analysis on Data Breach Announcements," *Journal of Service Research*, 26 (1), 44–63.

Reeck, Crystal, Nathaniel A. Posner, Kellen Mrkva, and Eric J. Johnson (2023), "Nudging App Adoption: Choice Architecture Facilitates Consumer Uptake of Mobile Apps," *Journal of Marketing*, 87 (4), 510–27.

Reich, Brandon J., Troy Campbell, and Robert Madrigal (2020), "Who Deserves Faulty Products? How Blaming the Victim Prevents Consumer Punitive Action," *Journal of Consumer Psychology*, 30 (1), 60–76.

Reidenberg, Joel R. (1993), "Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms," *Harvard Journal of Law & Technology*, 6 (2), 287–306.

Reuters (2024), "AT&T Announces $1 Bln Fiber Deal with Corning," (October 28), www.reuters.com/business/media-telecom/att-announces-1-bln-fiber-deal-with-corning-2024-10-28/.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti (2011), "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management*, 30 (2) 256–86.

Rundle, James (2021), "Regulators Tighten Scrutiny of Data Breach Disclosures by Companies," (August 31), www.wsj.com/articles/regulators-tighten-scrutiny-of-data-breach-disclosures-by-companies-11630402201.

Rust, Roland T., William Rand, Ming-Hui Huang, Andrew T. Stephen, Gillian Brooks, and Timur Chabuk (2021), “Real-Time Brand Reputation Tracking using Social Media,” *Journal of Marketing*, 85 (4), 21–43.

Salisbury, Linda Court, Gergana Y. Nenkov, Simon J. Blanchard, Ronald Paul Hill, Alexander L. Brown, and Kelly D. Martin (2023), “Beyond Income: Dynamic Consumer Financial Vulnerability,” *Journal of Marketing*, 87 (5), 657–78.

Satariano, Adam (2023), “Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules,” (May 22), www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html.

Schlosser, Ann E., Tiffany Barnett White, and Susan M. Lloyd (2006), “Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions,” *Journal of Marketing*, 70 (2), 133–48.

Schwartz, Barry (2004), *The paradox of choice: Why more is less*. ECCO.

Scott, Maura L., Sterling A. Bone, Glenn L. Christensen, Anneliese Lederer, Martin Mende, Brandon G. Christensen, and Marina Cozac (2024), “Revealing and Mitigating Racial Bias and Discrimination in Financial Services,” *Journal of Marketing Research*, 61 (4), 598–618.

Siebert, Anton, Ahir Gopaldas, Andrew Lindridge, and Cláudia Simões (2020), “Consumer Experience Journeys: Loyalty Loops versus Involvement Spirals,” *Journal of Marketing*, 84 (4), 45–66.

Shao, Wei, Jordan W. Moffett, Sara Quach, Jiraporn Surachartkumtonkun, Park Thaichon, Scott K. Weaven, and Robert W. Palmatier (2022), “Toward a Theory of Corporate Apology: Mechanisms, Contingencies, and Strategies,” *European Journal of Marketing*, 56 (12), 3418–52.

Smith, N. Craig, and Elizabeth Cooper-Martin (1997), “Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability,” *Journal of Marketing*, 61 (3), 1–20.

Solove, Daniel J. (2002), “Identity Theft, Privacy, and the Architecture of Vulnerability,” *Hastings Law Journal*, 54 (1227), 1–47.

Solove, Daniel J. (2004), *The digital person: Technology and privacy in the information age.* New York University Press.

Statista (2025), “Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2024,” (accessed June 13, 2025), www.statista.com/statistics/273550/ data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

Stewart, Emily (2022), “Companies Lose Your Data and Then Nothing Happens,” (April 21), vox.com/the-goods/23031858/data-breach-data-loss-personal-consequences.

Tang, Jie, Umair Akram, and Wenjing Shi (2021), “Why People Need Privacy? The Role of Privacy Fatigue in App Users’ Intention to Disclose Privacy: Based on Personality Traits,” *Journal of Enterprise Information Management*, 34 (4), 1097–120.

Thompson, Craig J., Paul C. Henry, and Fleura Bardhi (2018), “Theorizing Reactive Reflexivity: Lifestyle Displacement and Discordant Performances of Taste,” *Journal of Consumer Research*, 45 (3), 571–94.

Thompson, Debora Viana, Rebecca W. Hamilton, and Roland T. Rust (2005), “Feature Fatigue: When Product Capabilities Become Too Much of a Good Thing,” *Journal of Marketing Research*, 42 (4), 431–42.

Tucker, Catherine E. (2014), “Social Networks, Personalized Advertising, and Privacy Controls,” *Journal of Marketing Research*, 51 (5), 546–62.

Turjeman, Dana, and Fred M. Feinberg (2024), “When the Data are Out: Measuring Behavioral Changes following a Data Breach,” *Marketing Science*, 43 (2), 440–461.

Unilever (2025), “Safeguarding Data,” (accessed June 13, 2025), www.unilever.com/sustainability/responsible-business/safeguarding-data/.

Ursu, Raluca M., Qianyun Zhang, and Elisabeth Honka (2023), “Search Gaps and Consumer Fatigue,” *Marketing Science*, 42 (1), 110–36.

Walker, Kristen L. (2016), “Surrendering Information through the Looking Glass: Transparency, Trust, and Protection,” *Journal of Public Policy & Marketing*, 35 (1), 144–58.

Ward, James C., and Amy L. Ostrom (2006), “Complaining to the Masses: The Role of Protest Framing in Consumer-Created Complaint Web Sites,” *Journal of Consumer Research*, 33 (2), 220–230.

White, Katherine, and Bonnie Simpson (2013), “When Do (and Don’t) Normative Appeals Influence Sustainable Consumer Behaviors?” *Journal of Marketing*, 77 (2), 78–95.

Weinberg, Neal (2023), “Best and Worst Data Breach Responses Highlight the Do’s and Don’ts of IR,” (March 2), www.csoonline.com/article/574649/data-breaches-some-of-the-best-and-worst-among-recent-responses.html.

Westin, Alan F. (2003), “Social and Political Dimensions of Privacy,” *Journal of Social Issues*, 59 (2), 431–53.

Wood, Stacy L., and John G. Lynch Jr. (2002), “Prior Knowledge and Complacency in New Product Learning,” *Journal of Consumer Research*, 29 (3), 416–26.

Wooldridge, Jeffrey M. (2021), “Two-Way Fixed Effects, the Two-Way Mundlak Regression, and Difference-in-Differences Estimators,” (published online August 17), dx.doi.org/10.2139/ssrn.3906345.

Zimmermann, Johanna, Kelly D. Martin, Jan H. Schumann, and Thomas Widjaja (2024), “Consumers’ Multistage Data Control in Technology-Mediated Environments,” *International Journal of Research in Marketing*, 41 (1), 56–76.

Zhang, Jonathan Z., and Chun-Wei Chang (2021), “Consumer Dynamics: Theories, Methods, and Emerging Directions,” *Journal of the Academy of Marketing Science*, 49, 166–196.

Zhang, Jonathan Z., George F. Watson IV, Robert W. Palmatier, and Rajiv P. Dant (2016), “Dynamic Relationship Marketing,” *Journal of Marketing*, 80 (5), 53–75.

Zhu, John JianJun, Ling Tuo, Yanfen You, Qiang Fei, and Matthew Thomson (2024), “A Preemptive and Curative Solution to Mitigate Data Breaches: Corporate Social Responsibility as a Double Layer of Protection,” *Journal of Marketing Research*, 61 (4), 778–801.

Zeithaml, Valarie A., Arun Parasuraman, and Arvind Malhotra (2002), “Service Quality Delivery through Web Sites: A Critical Review of Extant Knowledge,” *Journal of the Academy of Marketing Science*, 30 (4), 362–375.

Zou, Yixin, and Florian Schaub (2019), “Beyond Mandatory: Making Data Breach Notifications Useful for Consumers,” *IEEE Security & Privacy*, 17 (2), 67–72.

Customer Privacy Journey Web Appendix

Web Appendix A: AT&T Data Breach Longitudinal Field-Based Insights 53

Web Appendix B: AT&T YouGov BrandIndex Data Analysis 62

References 66

These materials have been supplied by the authors to aid in the understanding of their paper. The AMA is sharing these materials at the request of the authors.

Web Appendix A: AT&T Data Breach Longitudinal Field-Based Insights

We conducted a three-wave longitudinal survey to assess changes in AT&T customers' privacy experiences following the AT&T data breach[2] announced on July 12, 2024 (FitzGerald and Furman 2024). Participants were recruited via Prolific using filters and screening questions to verify their AT&T customer status. Of the 521 recruited, 506 were verified customers, and 490 completed the first survey (M_{Age} = 38.37 years; 63.3% female, 37.9% male, 1.6% non-binary, and .2% other), launched 12 days after the breach was announced. Completing the first survey was required for eligibility in Wave 2 (*n* = 315; 64% response rate), and those who completed Wave 2 were invited to Wave 3 (*n* = 211; 67% response rate), administered approximately two and four months later. Each survey remained open for one week, with participants receiving reminder messages to encourage completion. In their review of survey-based studies, Hulland, Baumgartner, and Smith (2018) report an average response rate of 37.7% (SD = 21.6; Median = 33.3%), indicating that the response rates in this study are comparatively strong. Participants varied in income (Min_{Income} = less than $25,000, Max_{Income} = $150,000 or more), education (.8% = some high school or less, 26.3% = high school diploma or GED, 12.4% = associate's or technical degree, 43.9% = bachelor's degree, 16.5% = graduate or professional degree), and tenure as AT&T customers ($Min_{Customer}$ = less than one year, $Max_{Customer}$ = more than 10 years).

Procedure and Analysis

We used open-ended questions in all three waves to explore evolving customer feelings related to AT&T, their use of customer data, and the breach. Although the first survey followed the breach announcement, participants were prompted to reflect on their pre-breach views (i.e., "How did you feel about your data privacy with AT&T before you learned about this recent data breach?"). Across all three waves, participants described how they felt at the time of each survey and were encouraged to provide as much detail as they wished. In Wave 2, after completing the open-ended portion, participants completed a

---

[2] We use the terms "data breach" and "breach" interchangeably. Similarly, we use the terms "customer privacy journey" and "privacy journey" interchangeably.

matching task, categorizing their feelings of privacy vulnerability, privacy violation, and privacy fatigue across points in the privacy journey: before learning about the breach, immediately after, and at the time of the survey (i.e., approximately two months after the breach disclosure). The matching item was presented after the open-ended items to reduce demand effects and facilitate triangulation of psychological reactions. Finally, we collected demographic information.

Once data were collected, we applied the human–LLM (large language model) methodology introduced by Arora, Chakraborty, and Nishimura (2025). Specifically, we leveraged the LLM to process open-ended survey responses from the three wave, using targeted prompts to extract thematic insights, then probed further for illustrative quotes. We provided all definitions for the key constructs. Table W1 outlines this process, including the prompts, probes, and generated text sequence. Our goal was to assess if and how the responses aligned with or illuminated distinct psychological responses proposed in our privacy journey conceptual framework. We detail key insights and themes, beginning with the pre-breach stage.

As the final phase of the hybrid human–LLM analysis (Arora, Chakraborty, and Nishimura 2025), two independent coders reviewed the alignment between LLM-generated responses, prompts, and original survey data. Working separately, they cross-checked outputs against source material through multiple readings—neither identified issues in the LLM–human interaction, reinforcing confidence in the findings. Any discrepancies in quote categorization were resolved through discussion, ensuring analytic rigor.

Table W1. Insights from the Longitudinal AT&T Customer Survey

Panel A: Pre-Data Breach Stage (Wave 1)

Flow	Prompts and Generated Texts
Evidence of privacy vulnerability	We propose that customers feel a sense of vulnerability regarding their data privacy even before a breach occurs. Privacy vulnerability is defined as a customer's susceptibility to harm arising from the firm's collection, access, or use of their personal data. Did participants report feeling a sense of vulnerability before the AT&T breach?
LLM answer	The survey responses suggest that a significant portion of participants reported feelings related to vulnerability even before the specific AT&T data breach was announced, alongside those who felt secure or indifferent. This indicates that vulnerability was a pre-existing sentiment for many customers, often stemming from a general awareness of risks in the digital age, prior experiences with breaches (either AT&T's or other companies'), or a fundamental skepticism about the privacy practices of large corporations.
LLM probe	Can you extract the illustrative quotes that support your reasoning?
LLM additional answer	"I did not feel particularly safe about my data privacy but also felt like I couldn't do much about it," "I don't find any security with any high tech data companies," "My data and privacy [were] vulnerable," "I did not feel my data was protected very well to begin with," "I did not feel it was very secure, it could be accessed by too many store employees," "My data before learning about the data breach was always at risk," "I wasn't super confident that they were taking measures to be secure."

Panel B: Data Breach Stage (Wave 1)

Flow	Prompts and Generated Texts
Evidence of privacy violation	We propose that customers feel a sense of violation regarding their data privacy when a breach occurs. Privacy violation is defined as a customer's feelings of anger and betrayal, arising from the belief that the firm failed to uphold its responsibility to protect their personal data. Did participants report feeling a sense of violation during the AT&T breach?
LLM answer	Yes, based on the sources, many participants explicitly reported feeling a sense of violation, betrayal, or used other terms indicating a strong negative reaction to their data privacy being compromised after learning about the AT&T data breach.
LLM probe	Can you extract the illustrative quotes that support your reasoning?
LLM additional answer	"I felt violated. I hate that people I do not know now have access to my personal phone information," "I personally feel violated...my data could possibly be on the black market somewhere! It's also a bit scary not knowing what criminals can do with my information," "I felt betrayed. I felt that my privacy had been violated and that I need[ed] to be more protected," "I feel disappointed and violated. I feel that a better job should have been done to ensure privacy was being maintained," "Betrayed."

Panel C: Post-Data Breach Stage (Wave 2)

Flow	Prompts and Generated Texts
Evidence of privacy fatigue	We propose that customers feel a sense of privacy fatigue after a breach occurs. Privacy fatigue is defined as a customer's exhaustion with ongoing data privacy issues, manifesting in emotional exhaustion and/or cynicism. Did participants report feeling a sense of privacy fatigue after the AT&T breach?
LLM answer	Yes, participants frequently reported feelings consistent with privacy fatigue after the AT&T data breach, characterized by widespread emotional exhaustion and cynicism. This fatigue manifested as forgetting about the breach, becoming desensitized to such incidents, and expressing resignation or distrust regarding data security and corporate accountability.
LLM probe	Can you extract the illustrative quotes that support your reasoning?
LLM additional answer	"My data has been breached too many times to count," "There are so many data breaches in [so] many companies that I just don't care anymore," "It is a pretty hopeless situation that is unavoidable," "I feel like I [don't] have any privacy at all anymore. I feel like I don't have any control [over my privacy]," "I don't really care much about it at this point because so many people are suffering the same," "I don't really feel like there is anything I can do these days but let all these companies fumble my information and expect a $5 apology," "I still feel that my data could constantly be at risk of being breached," "These days your data being leaked seems like a fact of life," "Unfortunately it's hard to care about data breaches at this point especially when there's so little I can do to combat them."

Table W1. Insights from the Longitudinal AT&T Customer Survey (continued)

Panel D: Continuity Loop (Wave 3)

Flow	Prompts and Generated Texts
Evidence of privacy vulnerability and privacy fatigue	Do customers feel a renewed sense of privacy vulnerability and lingering privacy fatigue? Privacy vulnerability is a customer's susceptibility to harm arising from the firm's collection, access, or use of their personal data. Privacy fatigue is defined as a customer's exhaustion with ongoing data privacy issues, manifesting in emotional exhaustion and/or cynicism.
LLM answer	Yes, the results suggest a renewed sense of vulnerability, as customers continue to feel their personal data is at risk and experience tangible impacts like increased spam calls. However, this vulnerability is deeply shaped by lingering privacy fatigue, manifesting as a resigned acceptance that data breaches are normal and unavoidable. This leads to emotional desensitization and a perceived powerlessness, transforming their vulnerability into a more passive, cynical outlook rather than an active alarm.
LLM probe	Can you extract the illustrative quotes that support your reasoning?
LLM additional answer	"I have been getting more spam calls and texts...I feel scared and I know my info is out on the dark web now," "I'm still feeling a bit uneasy about my data privacy with AT&T," "It makes me question how vulnerable my information really is, especially when stored on third-party cloud platforms," "It's hard not to wonder if this could happen again, or whether they truly have the necessary protections in place to prevent further incidents," "Data breaches are an expected and normal part of life because it seems to be near impossible to maintain security," "I am still frustrated it took place, but I have accepted that it happened and don't dwell on it," "At this point, I assume my data has been leaked by just about every company that has it," "Data privacy won't exist in the next few years. This was just the beginning."
Evidence of privacy fatigue dynamics	Do customers feel increasing privacy fatigue with time across the three survey waves?
LLM answer	Yes, the sources provide strong evidence of increasing privacy fatigue across the rounds of the survey. This fatigue is marked by emotional desensitization, resignation, indifference, and the tendency to forget about the breach over time. Even prior to the data breach, several respondents already expressed signs of early fatigue. Some believed that breaches were inevitable, viewing companies as inherently vulnerable to cyberattacks. Others admitted to feeling indifferent or rarely thinking about their data privacy at all. A number of participants voiced concern about the frequency of data breaches in general, while others revealed they were already desensitized due to the sheer number of incidents across companies. By the second round, signs of privacy fatigue became more widespread. Many respondents openly stated they had become desensitized to breaches because they happen so frequently. The perception of breaches as an "inevitability," a "fact of life," or something "normal" was repeatedly expressed. A number admitted they had forgotten about the breach by this point. Feelings of helplessness ("there's nothing you can really do") and resignation ("my info is simply out there") were common. In the third round, the signs of fatigue deepened. Forgetting about the breach became even more common, and many respondents described themselves as feeling indifferent. Breaches were widely labeled as an "expected and normal part of life," a "fact of life," or simply "just the norm." The sense of powerlessness persisted, with several noting that "there's nothing a consumer can do."
LLM probe	Can you extract the illustrative quotes that support your reasoning?
	"It feels like there's not much else customers can do but accept this reality," "I assume my data has been leaked by just about every company that has it," "Data privacy doesn't exist in today's society. AT&T was one of many companies who have breached my data," "I feel like I get news of a data breach almost every month so unfortunately I feel desensitized by it," "It seems like there are always data breaches everywhere so it almost feels normal," "I have become very desensitized to data breaches."

Pre-Data Breach Stage Field-Based Insights

Although the first wave of our survey was launched shortly after the AT&T breach became public, we explicitly asked participants to reflect on their feelings before the incident. To capture insights into the pre-breach phase, we asked, “How did you feel about your data privacy with AT&T before you learned about this recent data breach?” Respondents were encouraged to be as descriptive as possible.

We posit that customers experience privacy vulnerability pre-breach, specifically upon learning that a firm has collected or will collect their data. We analyzed the open-ended responses using a human–LLM methodology to provide external evidence supporting this proposition. Table W1, Panel A presents the prompts and representative responses related to the pre-breach stage collected in Wave 1. First, we asked the LLM whether customers experience a sense of vulnerability regarding data privacy before learning about the breach. The model summarized the responses as follows:

> The survey responses suggest that a significant portion of participants reported feelings related to vulnerability even before the specific AT&T data breach was announced, alongside those who felt secure or indifferent. This indicates that vulnerability was a pre-existing sentiment for many customers, often stemming from a general awareness of risks in the digital age, prior experiences with breaches (either AT&T’s or other companies’), or a fundamental skepticism about the privacy practices of large corporations.

We then prompted the model for illustrative quotes. It returned examples such as: “I did not feel particularly safe about my data privacy but also felt like I couldn't do much about it,” and “I did not feel my data was protected very well to begin with.” Table W1, Panel A provides additional quotes. The results offer qualitative support and conceptual grounding for privacy vulnerability as a meaningful construct in the pre-breach phase.

Data Breach Stage Field-Based Insights

To assess shifts in feelings in the breach stage, we asked participants to reflect on their immediate responses to the incident in Wave 1. Specifically, we posed the open-ended question: “How did you personally feel considering your data privacy immediately after learning about the AT&T data breach?” We then asked the LLM whether customers experience a sense of violation regarding data privacy during a breach (Table W1, Panel B). The model summarized the responses as follows:

> Yes, based on the sources, many participants explicitly reported feeling a sense of violation, betrayal, or used other terms indicating a strong negative reaction to their data privacy being compromised after learning about the AT&T data breach.

We then probed for illustrative quotes. The model returned examples including: "I felt violated. I hate that people I do not know now have access to my personal phone information," and "I felt betrayed. I felt that my privacy had been violated and that I need[ed] to be more protected." Table W1, Panel B reports additional quotes, underscoring the role of privacy violation in the breach stage of the privacy journey.

Post-Data Breach Stage Field-Based Insights

To assess shifting feelings in the post-breach stage, we asked participants in Wave 2 of the survey, launched approximately two months after the breach disclosure, to reflect on their feelings over time. Specifically, we posed the open-ended question: "Now that two months have passed since AT&T announced the data breach, how do you currently feel about your data privacy with AT&T?" We asked the LLM whether customers experience a sense of privacy fatigue regarding data privacy after a breach (Table W1, Panel C). The model summarized the responses as follows:

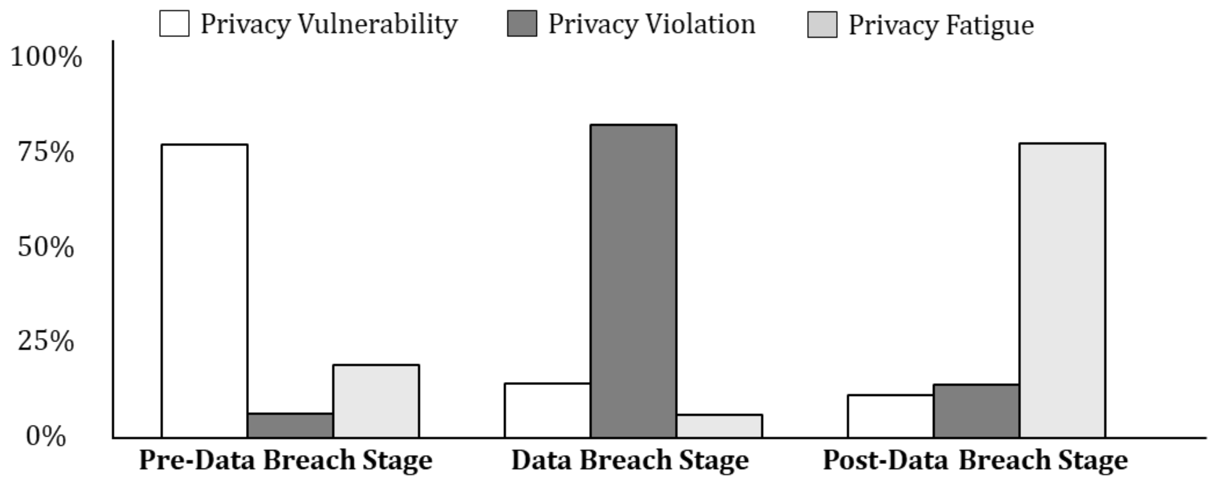
> Yes, participants frequently reported feelings consistent with privacy fatigue after the AT&T data breach, characterized by widespread emotional exhaustion and cynicism. This fatigue manifested as forgetting about the breach, becoming desensitized to such incidents, and expressing resignation or distrust regarding data security and corporate accountability.

Illustrative quotes we probed for included: "My data has been breached too many times to count," and "I don't really feel like there is anything I can do these days but let all these companies fumble my information and expect a $5 apology." Table W1, Panel C reports additional quotes.

Following the open-ended questions in Wave 2, participants were asked to match specific feelings to each stage of the privacy journey. The options included a sense of vulnerability ("vulnerable or susceptible"), violation ("violated or taken advantage of"), and privacy fatigue ("exhausted or desensitized"). The stages were defined as: before learning about the breach, immediately after the breach, and at the time of the survey (approximately two months after the breach disclosure). As shown in

Figure W1, most participants associated vulnerability with the pre-breach stage (75%), violation with the breach stage (80%), and privacy fatigue with the post-breach period (75%), lending support to our framework.

Figure W1. Matching Question Results (Wave 2)



Notes: This figure shows how participants in the second survey wave matched emotions to stages of the customer privacy journey; *n* = 315.

Customer Privacy Journey Continuity Loop Field-Based Insights

Our framework suggests the privacy journey loops rather than ends, as a customer reenters the data exchange relationship, with a renewed sense of privacy vulnerability and lingering privacy fatigue from their prior privacy experiences. We conducted Wave 3 of the longitudinal survey approximately four months after AT&T disclosed the breach. This survey used open-ended questions asking participants to assess their data privacy with AT&T at the time of the survey. Specifically, we asked, "Now that a few months have passed since AT&T announced the data breach, how do you currently feel about your data privacy with AT&T?" We used the LLM to understand if the survey responses align with our theorizing, asking if the results suggest a renewed sense of privacy vulnerability shaped by lingering privacy fatigue (Table W1, Panel D). The LLM responded:

> Yes, the results suggest a renewed sense of vulnerability, as customers continue to feel their personal data is at risk and experience tangible impacts like increased spam calls. However, this vulnerability is deeply shaped by lingering privacy fatigue, manifesting as a resigned acceptance that data breaches

> are normal and unavoidable. This leads to emotional desensitization and a perceived powerlessness, transforming their vulnerability into a more passive, cynical outlook rather than an active alarm.

We probed for illustrative quotes and the LLM returned those that corresponded to feelings of privacy vulnerability, such as: “I have been getting more spam calls and texts...I feel scared and I know my info is out on the dark web now,” and “It makes me question how vulnerable my information really is, especially when stored on third-party cloud platforms.” The LLM also extracted quotes that aligned with privacy fatigue, including: “Data breaches are an expected and normal part of life because it seems to be near impossible to maintain security,” and “At this point, I assume my data has been leaked by just about every company that has it.” Table W1, Panel D reports additional quotes.

Leveraging the survey’s longitudinal design, we applied the LLM to assess whether participants exhibited increasing feelings of privacy fatigue over time across the three survey waves (Table W1, Panel D). This design enabled us to track changes and provide deeper insight into how customer feelings evolve across a privacy journey. The LLM reported a clear increase in privacy fatigue across the three waves of the survey. According to the model, this privacy fatigue manifested as emotional desensitization, resignation, and a growing tendency to forget about the breach over time. The LLM also noted early signs of privacy fatigue even before the breach, with some participants viewing such incidents as inevitable. By the second wave, the model identified an intensification of privacy fatigue, and by the third wave, the model noted that these sentiments persisted, with many participants describing breaches as a normal part of life and expressing a sense of resignation. Illustrative quotes included: “It feels like there’s not much else customers can do but accept this reality,” and “I feel like I get news of a data breach almost every month so unfortunately I feel desensitized by it,” Table W1, Panel D reports the complete LLM response and additional quotes.

In sum, the longitudinal survey design lends support to the proposed privacy journey framework, highlighting distinct, dominant psychological reactions at each stage. The findings also indicate that privacy fatigue festers quietly and intensifies over time, emerging as a psychologically salient force in the post-breach stage and carrying forward into subsequent privacy experiences. Crucially, this accumulated privacy fatigue appears to erode customers' psychological resilience, amplifying how vulnerable they feel as they reenter data exchange relationships.

Web Appendix B: AT&T YouGov BrandIndex Data Analysis

We use secondary data to assess changes in brand advocacy following AT&T's public confirmation of its breach in July 2024. Our analysis uses a two-way fixed effects heterogeneous treatment effects difference-in-differences (DID) approach (Wooldridge 2021), where AT&T serves as the treated group and the breach disclosure marks the start of the treatment period. The data come from YouGov's Brand Metrics (Klostermann et al. 2025; Moorman, Sorescu, and Tavassoli 2024), which continuously tracks customer attitudes toward telecommunications brands in the U.S., including AT&T, T-Mobile, Verizon Wireless, US Cellular, Lumen Technologies, and Xfinity Mobile. This data set enables us to benchmark shifts in AT&T's brand advocacy relative to those of its competitors. The sample consists of a balanced panel with 234 weekly observations across the six telecommunications brands, covering the period from April 8, 2024, to January 5, 2025. This includes three months of pre-treatment data and six months of post-treatment data relative to the public disclosure of AT&T's data breach. Table W2 reports descriptive statistics and correlations.

Table W2. YouGov data descriptive statistics and correlations

Variable	Mean	SD	1	2	3
1 Brand advocacy	61.30	19.30	1.00		
2 Advertising awareness	58.44	18.30	.27	1.00	
3 WOM exposure	49.89	17.14	.43	.42	1.00

Note: SD = Standard deviation. WOM = Word-of-mouth.

Measures

Brand advocacy. Our outcome of interest is brand advocacy, measured using YouGov's BrandIndex likelihood to recommend metric, which gauges brand advocacy through the question: "Would you recommend this brand to friends and family, or tell them to avoid it?" YouGov surveys approximately 5,000 respondents daily, randomly selected from a 7-million-member online panel. To reduce selection bias, samples are stratified and weighted by age, race, gender, education, and region, using U.S. Census benchmarks, ensuring national representativeness. This real-time tracking allows for robust, week-over-week brand comparisons (Rust et al. 2021). Our analysis focuses on customers of each brand, rather than the general population.

Control variables. To account for alternative influences on brand advocacy, we include controls for advertising awareness and word-of-mouth (WOM) exposure, both of which may independently affect outcomes. Advertising awareness is measured by the item, "Have you seen advertising for this brand in the past two weeks?" WOM exposure is assessed via the question, "Have you talked about this brand in the past two weeks?" Both measures are expressed as percentages. Including these covariates allows us to more precisely isolate the effect of the breach. We also incorporate brand fixed effects to control for time-invariant brand-specific characteristics, such as baseline consumer perceptions or ongoing marketing strategies. Week fixed effects are included to adjust for time-varying shocks that could influence all brands simultaneously, such as seasonal patterns, industry-wide events, or macroeconomic fluctuations.

Estimation and Results

We use a two-way fixed effects (TWFE) model to estimate the average treatment effect on the treated (ATT), controlling for brand-specific and week-specific unobserved heterogeneity (Wooldridge 2021). This model structure accounts for constant confounding factors within brands over time or common across brands each week. We also include advertising awareness and WOM exposure as time-varying covariates to refine our treatment effect estimation further. The TWFE model allows us to examine the dynamic evolution of treatment effects across time, highlighting how customer responses to the breach change weekly. By leveraging within-brand variation, the model mitigates potential omitted variable bias and strengthens causal inference. The Wooldridge (2010) test indicates no significant first-order autocorrelation in the panel data model residuals (F-statistic = 3.815, $p = .108$).

The results, reported in Table W3, indicate a significant negative ATT for AT&T following the data breach (ATT = –20.13, $p = .047$), suggesting a decline in brand advocacy linked to the breach. However, this effect dissipates in subsequent weeks, with ATT estimates becoming statistically indistinguishable from zero. Later periods show a rebound in brand advocacy, with notable positive effects in August (ATT = 35.57, $p = .010$) and September (ATT = 20.49, $p = .008$), likely driven by favorable public sentiment surrounding potential union agreements between AT&T and its workers (CWA 2024; Hyde 2024). Another significant positive effect occurs in the week of October 28 (ATT = 20.50, *p* = .041), coinciding with AT&T's announcement of a $1 billion supply agreement with Corning (Reuters 2024). A subsequent decline is observed in mid-November (ATT = –18.88, *p* = .050), which aligns with media coverage of the hacker's arrest (Franceschi-Bicchierai 2024; Murphy and Platt 2024), possibly reactivating concerns related to the breach.

Parallel trends. Our estimation approach relies on the assumption of parallel trends, which posits that the treatment and control groups would have followed the same trends without a data breach announcement. We compared the pretreatment trends for AT&T and the industry to test this assumption. The results showed no significant difference (F(4, 5) = .89, *p* = .530), suggesting that pretreatment differences between the two groups do not drive our findings.

Table W3. Average Treatment Effect on the Treated following the AT&T Data Breach

Weeks post breach	ATT	SE	t–statistics	*p* –values	95% CI
1	5.31	26.35	.20	.848	[−62.42, 73.04]
2	−12.31	24.14	−0.51	.632	[−74.36, 49.74]
3	−20.13	7.70	−2.62	.047	[−39.92, −0.35]
4	−29.84	27.30	−1.09	.324	[−100.00, 40.33]
5	8.87	4.21	2.11	.089	[−1.96, 19.70]
6	.95	6.61	.14	.891	[−16.05, 17.96]
7	35.57	8.79	4.05	.010	[12.98, 58.17]
8	1.69	12.49	.14	.898	[−30.42, 33.79]
9	−13.33	5.94	−2.25	.075	[−28.59, 1.93]
10	3.73	8.11	.46	.665	[−17.12, 24.58]
11	−.49	8.30	−0.06	.955	[−21.82, 20.84]
12	20.49	4.74	4.32	.008	[8.30, 32.68]
13	−7.59	13.28	−0.57	.593	[−41.74, 26.56]
14	−5.96	12.65	−0.47	.657	[−38.48, 26.56]
15	13.27	8.59	1.54	.183	[−8.82, 35.36]
16	.82	8.01	.10	.922	[−19.77, 21.41]
17	20.50	7.47	2.74	.041	[1.29, 39.72]
18	−5.89	5.91	−1.00	.364	[−21.08, 9.29]
19	−18.88	7.35	−2.57	.050	[−37.78, 0.01]
20	−35.74	15.80	−2.26	.073	[−76.35, 4.88]
21	−1.98	9.46	−0.21	.842	[−26.31, 22.34]
22	−6.59	7.84	−0.84	.439	[−26.74, 13.56]
23	−5.13	5.36	−0.96	.382	[−18.91, 8.64]
24	−6.37	6.51	−0.98	.373	[−23.11, 10.37]
25	−.02	1.76	−0.01	.993	[−4.54, 4.51]
26	−10.22	5.72	−1.79	.134	[−24.92, 4.48]

Notes: ATT = Average treatment effect on the treated. SE = Standard error. CI = Confidence interval. ATT is computed using advertising awareness and word–of–mouth covariates. Pre-treatment period includes three months. Robust standard errors are reported.

References

Arora, Neeraj, Ishita Chakraborty, and Yohei Nishimura (2025), “AI–Human Hybrids for Marketing Research: Leveraging Large Language Models (LLMs) as Collaborators,” *Journal of Marketing*, 89 (2), 43–70.

CWA (2024), “CWA and AT&T Enter Federal Mediation as Southeastern Strike Continues Over Unfair Labor Practices,” (August 21), https://cwa-union.org/news/releases/cwa-and-att-enter-federal-mediation-southeastern-strike-continues-over-unfair-labor.

FitzGerald, Drew, and Sadie Gurman (2024), “AT&T Says Hacker Stole Cell, Text Data on Nearly All Its Wireless Customers,” (July 12), www.wsj.com/business/telecom/at-t-says-hacker-stole-data-on-nearly-all-its-wireless-customers-32d6969d.

Franceschi-Bicchierai, Lorenzo (2024), “Snowflake Hackers Identified and Charged with Stealing 50 billion AT&T Records,” (November 12), https://techcrunch.com/2024/11/12/ snowflake-hackers-identified-and-charged-with-stealing-50-billion-att-records/.

Hulland, John, Hans Baumgartner, and Keith Marion Smith (2018), “Marketing Survey Research Best Practices: Evidence and Recommendations from a Review of *JAMS* Articles,” *Journal of the Academy of Marketing Science*, 46 (1), 92–108.

Hyde, Marlon (2024), “AT&T Reaches Deal with Union Telecom Workers, Ending Southeast Strike,” (September 16), www.wabe.org/att-reaches-deal-with-union-telecom-workers-ending-southeast-strike/.

Klostermann, Jan, Anne Mareike Flaswinkel, Chris Hydock, and Reinhold Decker (2025), “The Effect of Company Size on Aggregate Word of Mouth Valence,” *Journal of Marketing* (published online February 6), doi.org/10.1177/00222429251320603.

Moorman, Christine, Alina Sorescu, and Nader T. Tavassoli (2024), “Brands in the Labor Market: How Vertical and Horizontal Brand Differentiation Impact Pay and Profits through Employee–Brand Matching,” *Journal of Marketing Research*, 61 (2), 204–24.

Murphy, Margi, and Brian Platt (2024), “Canada Arrests Man Suspected of Hacks of Snowflake Customers,” (November 4), www.bloomberg.com/news/articles/2024-11-05/hacker-said-to-be-behind-breach-of-snowflake-customers-arrested.

Reuters (2024), “AT&T Announces $1 Bln Fiber Deal with Corning,” (October 28), www.reuters.com/business/media-telecom/att-announces-1-bln-fiber-deal-with-corning-2024-10-28/.

Rust, Roland T., William Rand, Ming-Hui Huang, Andrew T. Stephen, Gillian Brooks, and Timur Chabuk (2021), “Real-Time Brand Reputation Tracking using Social Media,” *Journal of Marketing*, 85 (4), 21–43.

Wooldridge, Jeffrey M. (2010), *Econometric analysis of cross-section and panel data*. MIT Press.

Wooldridge, Jeffrey M. (2021), “Two-Way Fixed Effects, the Two-Way Mundlak Regression, and Difference-in-Differences Estimators,” (published online August 17), http://dx.doi.org/10.2139/ssrn.3906345.