social sciences

MDPI

Article

Experiencing Digital Sovereignty: Exploring Associations Among Perceived Personal Data Controllability, Trust, and Anxiety in Social Media

Maisoon Alsebaei * and Shuaa Aljasir

Department of Journalism & Digital Media, Faculty of Communication and Media, King Abdulaziz University, Jeddah 22254, Saudi Arabia; shaljasir@kau.edu.sa
* Correspondence: malsebaei@kau.edu.sa

Abstract

Social media platforms collect, process, and monetise personal data on a scale that has made control over personal information a central concern for users and regulators. Research on digital sovereignty has largely addressed this concern at the level of states and institutions, leaving the individual user's experience of control comparatively unexamined. This study examines how perceived personal data controllability, an affordance of platform interfaces, is associated with control-based privacy beliefs, trust in the platform, and anxiety. A scenario-based survey was conducted with 308 Saudi participants, who evaluated a simulated social networking platform designed to emphasise privacy and user control. Digital sovereignty was conceptualised as users' claim to self-determination over their data on platforms, with control-based privacy beliefs as one psychological expression of this claim. Stronger perceived controllability was positively associated with control-based privacy beliefs and trust and negatively associated with anxiety. Control-based privacy beliefs moderated the association between controllability and anxiety, which was stronger among participants who held these beliefs less strongly, but did not moderate the association with trust. Control-based privacy beliefs thus function as a boundary condition for users' affective—but not evaluative—responses to platform design.

Keywords: digital sovereignty; personal data controllability; privacy beliefs; platform trust; anxiety; social media; platform design; cognitive–affective mechanisms

1. Introduction

The conditions of interpersonal communication, information dissemination, and identity formation have changed in modern society due to the proliferation of social media. These platforms have evolved into hubs for collecting, processing, and monetising personal data, thereby interweaving users into complex systems of surveillance, algorithmic decision-making, and datafication (van Dijck et al. 2018; Zuboff 2019). Scholarly work has focused on the informational power within platform ecosystems and the extent to which individuals generate, share, and use personal information. In this context, digital sovereignty is a pertinent topic for addressing issues of control, self-determination, and authority in the digital realm (Floridi 2020; Pohle and Thiel 2020).

However, most work treats digital sovereignty as a matter for states and institutions, with scarce consideration of its personal, experiential dimension: how social media users understand and respond to authority over their personal data in everyday platform use (Couture and Toupin 2019; Mueller 2020). This gap matters because control is central to

Check for updates

Academic Editor: Qiang Chen

Received: 9 September 2026
Revised: 29 October 2026
Accepted: 1 November 2026
Published: 4 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

how people relate to digital technology. It remains unclear how platform characteristics relate to users' beliefs about control over personal information and to their psychological responses (Masur 2018; Trepte 2021)—particularly how the controllability of personal data that a platform affords relates to these beliefs (Cho et al. 2020; Trepte 2021). Trust and anxiety, two central outcomes of social media use, have rarely been examined together within a single account of how users experience control over their data. Digital sovereignty therefore remains loosely linked to the psychological processes through which individuals evaluate their participation on social media platforms.

The present study aims to examine how perceived personal data controllability is associated with users' control-based privacy beliefs, trust in the platform, and anxiety, as well as whether control-based privacy beliefs moderate the associations with trust and anxiety. Following Evans et al. (2017), controllability is treated as an affordance: the possibility of controlling one's personal data that users perceive in their relationship with a platform's privacy features. Digital sovereignty is theorised as a unifying concept that refers to users' claim to self-determination over their personal data within platform settings. Control-based privacy beliefs—the conviction that one's privacy on a platform depends on control and autonomy over one's personal information—are one psychological expression of this broader concept and reflect how users experience digital sovereignty during daily interactions with social media platforms (Tan et al. 2023). This study also assumes that greater perceived controllability is associated with greater trust in the platform and lower anxiety. Trust and anxiety are cognitive and emotional outcomes through which digital sovereignty takes on experiential significance in social media contexts.

This paper makes three key contributions to the existing literature: First, it contributes to the growing human-centred strand of digital sovereignty research (Behera et al. 2026) by examining perceptions and experiences of informational control at the individual level. Second, it draws on and corroborates prior studies on privacy affordances, control-based privacy beliefs, trust, and emotional responses under a single theoretical framework. Third, it provides an empirical perspective on the psychological implications of privacy-centric and data management platform architectures in existing debates on the design of digital environments that promote user autonomy and meaningful participation in data-driven societies.

2. Theoretical Background

2.1. Digital Sovereignty in the Platform Economy

Initially, digital sovereignty was defined as a nation-state's ability to assert control over digital infrastructures, data flows, and technological resources. For example, Couture and Toupin (2019) and Mueller (2020) have examined state control over data infrastructure and competing territorial sovereignty in relation to cross-border data transfers, as well as geopolitical conflict concerning technological dependency and strategic autonomy. However, recent studies have viewed digital sovereignty as a multidimensional concept involving overlapping claims in the political, economic, and social spheres (Floridi 2020; Pohle and Thiel 2020). Digital sovereignty is a dynamic discourse in which states, corporations, and individuals attempt to legitimise their governance of digital environments and data practices (Adler-Nissen and Eggeling 2024). Building on the work of Pohle and Thiel (2020), this study defines digital sovereignty as the capacity of an actor—whether a state, an organisation, or an individual—to exercise self-determination over data, digital infrastructure, and digital practices. The present study addresses the individual level of this capacity, which provides the overarching framework for understanding users' experiences of agency and control in social media spaces.

The growing significance of platform-based economic models has further eroded traditional notions of sovereignty in the digital era. Content moderation mechanisms and data-driven content recommendation algorithms influence the regulatory authority of

platforms, shaping patterns of visibility, participation, and communication (Srnicek 2017; Törnberg 2023). This concentration of infrastructural power has led to the emergence of the concept of virtual sovereignty, whereby private companies assume governance functions operating in parallel with—or in conflict with—existing state-backed mechanisms of oversight and accountability (Kelton et al. 2022). Similarly, the collection and manipulation of behavioural data have given rise to increasingly novel methods of creating economic value based on the prediction and presumption of human behaviour. This has led to surveillance-related techniques penetrating daily social life (Zuboff 2019) and a renewed focus on the principle of informational self-determination, which refers to an individual's ability to decide the conditions under which their personal data are collected, processed, and disclosed (Floridi 2020; Pisani 2024). In this model, sovereignty refers to the extent to which citizens can control their digital identity and "informational boundaries". Therefore, understanding digital sovereignty requires an analytical focus on how platforms' architecture, governance models, and design enable or limit end users' capacity to control their personal data (Pisani 2024). This personal aspect of digital sovereignty underpins current research on perceived and experienced control on social media. Studies have focused particularly on privacy management, platform governance, and the ways in which user autonomy is reflected in psychological responses to platform use.

Digital sovereignty can therefore be claimed at three levels: At the state level, it concerns jurisdiction over data flows and digital infrastructure (Couture and Toupin 2019; Mueller 2020). At the platform level, it concerns the governance functions that private platforms exercise over visibility, participation, and data use, sometimes termed virtual sovereignty (Kelton et al. 2022; Törnberg 2023). At the individual level, it concerns informational self-determination, i.e., users' capacity to decide what is known about them and by whom (Floridi 2020; Pisani 2024); this level is the focus of a growing human-centred strand of research (Behera et al. 2026). The present study addresses the individual level; it nonetheless connects the levels: the controllability of personal data is what the platform level makes available to users, and trust is users' judgement of how the platform level will behave.

Privacy, in its classic formulation, is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967, p. 7). Digital sovereignty takes a holistic view of individuals' digital footprints, while informational self-determination, privacy concerns, and privacy self-efficacy reflect specific aspects of the relationship with personal data. Informational self-determination relates to legal and normative rights concerning data collection and processing. Privacy concern relates to perceived threats and risks caused by data practices. Privacy self-efficacy relates to confidence in one's ability to control privacy settings or protective behaviours. Although digital sovereignty can be viewed as a technical ability, it also includes governance institutions and the perception of autonomy among users in digitally mediated settings. Thus, control-based privacy beliefs are conceptualised as the experiential form that the individual claim to digital sovereignty takes in users' daily use of platforms, rather than as digital sovereignty itself.

2.2. Platform Privacy and Data-Control Features

The technical architecture through which individuals interact with digital platforms plays an important role in determining their level of digital sovereignty. Adopting an affordance theory perspective helps us to understand the influence of the architecture on opportunities for user agency. Affordances, which originate in ecological psychology, are the possibilities for action that emerge from the relationship between an actor and their environment (Gibson 1979). Design studies research has emphasised that these possibilities depend on users' perceptions and interpretations of available functionalities, as well as the

objective properties of technological artefacts (Norman 2013). Therefore, it can be argued that affordances are the action possibilities that a user believes are available within a digital space based on the features of the platform and their own goals, intentions, and abilities (Evans et al. 2017).

In this study, the affordance examined is perceived personal data controllability, defined as the extent to which users perceive that a platform enables them to set, adjust, and restrict how their personal information is collected, displayed, and shared. Research on social media affordances has identified visibility, persistence, editability, and association as affordances shared across platforms (Treem and Leonardi 2013), and scales of perceived affordances include privacy and control over interaction among their dimensions (Fox and McEwan 2017). Evans et al. (2017) proposed three criteria for an affordance, namely that it is not the feature itself, it is not an outcome of use, and it varies in degree. Controllability meets all three, as it is distinct from the features that support it (privacy settings, consent options, data-deletion tools) and from its outcomes (beliefs about control, trust, anxiety), and it varies, since a platform can make control over personal data more or less possible.

Controllability is central to digital sovereignty because it determines the means available to users for controlling the collection, dissemination, and management of their personal data. Specifically, granular privacy controls, multi-factor authentication systems, and data access and deletion management methods provide practical ways for users to establish and maintain informational boundaries (Stach and Mitschang 2014; Wang et al. 2021). This is consistent with the Privacy by Design principle, which advocates integrating privacy into the core design of technological systems rather than adding it afterwards or attempting to mitigate it. Adopting a Privacy by Design approach proactively embeds privacy protections into technological systems from the outset (Cavoukian 2011). A key tenet of this approach is that privacy should be the default state, so that users can enjoy protection without having to scour complex configurations or perform numerous manual interventions (Pisani 2024). In this respect, the architectural designs of platforms become normatively significant due to the extent to which they afford or deny privacy in their setups (van Dijck et al. 2018).

Providing privacy-preserving modes of operation does not ensure the effectiveness of digital sovereignty. Rather, the usefulness that users derive from such mechanisms is significantly influenced by their usability, comprehensibility, and prominence in the interface. Empirical findings from the usable privacy literature show that privacy notices, consent mechanisms, and control interfaces are only effective when they engage with users' cognitive capabilities and decision-making processes while minimising the effort involved in assessing and managing privacy-related choices (Angulo et al. 2012; Schaub et al. 2015). Similarly, research in the fields of management and information systems has focused on the strategic importance of privacy features, such as platforms that clearly demonstrate a commitment to user privacy, provide easily accessible and comprehensible control features, enhance their reputation, and generate competitive advantages by communicating responsible information practices (Kuan and Lee 2023). However, interface designs that deliberately influence behaviour in a way that deters or discourages privacy-protective actions jeopardise the conditions for individual digital sovereignty (Tan et al. 2023). Such designs are referred to as "dark patterns" and exploit cognitive biases and information asymmetries to direct users towards outcomes that conflict with their preferences or interests (Gray et al. 2018; Mathur et al. 2019). Such design features prevent users from making independent and informed choices on the platforms, undermining the control and trust necessary for sustainable user–platform relationships.

2.3. Control-Based Privacy Beliefs

Control has long been central to conceptions of privacy. Westin (1967) defined privacy as a claim of individuals to determine for themselves how information about them is

communicated to others, and Malhotra et al. (2004) identified control as a core dimension of internet users' privacy beliefs, that is, the conviction that privacy depends on individuals' control and autonomy over decisions about how their personal information is collected, used, and shared. In this study, control-based privacy beliefs refer to the extent to which users hold this conviction with respect to a specific platform. These beliefs differ from perceived control, which is users' subjective sense that they actually exercise control over their information (Xu et al. 2011). Perceived control concerns whether users feel in control, whereas control-based privacy beliefs concern how much users consider control to matter for their privacy on the platform. From a digital sovereignty perspective, control-based privacy beliefs express the individual-level claim to informational self-determination (Floridi 2020; Pisani 2024). Like other control-related perceptions, they are likely to be context-dependent, varying with the nature of the content and with the privacy cues embedded in platform interfaces (Shulman and Meyer 2022).

The empirical evidence on control in privacy research is extensive. For example, Xu et al. (2011) found that a sense of control mitigates privacy concerns and strengthens the response to institutional privacy assurances. Similarly, Paliszkiewicz and Koohang (2016) found that a sense of control positively predicted individuals' attitudes towards social media platforms and their intention to share information, while Smith et al. (2011) found that perceived control predicted disclosure behaviours and privacy concerns. However, Brandimarte et al. (2013) showed that an increase in perceived control can lead to higher rates of disclosure of sensitive information, even when the objective risk remains unchanged, noting the presence of a control paradox. More recent studies have called these relationships into question: For example, Feng et al. (2024) found no significant relationship between perceived control and intentions to quit social media. This suggests that perceptions of control should be explored under certain conditions in platform environments. According to affordance theory, accessible privacy controls, clear disclosure of privacy practices, and options for managing the flow of information can enhance user trust and control over their data. Similarly, research on privacy interfaces has shown that transparency and user-centred design are strongly associated with users' perceptions of control over their data (Angulo et al. 2012; Wang et al. 2025). When a platform makes control over personal data visibly possible, it also makes control salient as the standard by which privacy on that platform is judged. Users who perceive greater controllability may therefore be more inclined to frame their privacy on the platform in terms of control, that is, to hold stronger control-based privacy beliefs. Based on this, the present study proposes the following hypothesis:

H1. *Perceived personal data controllability is positively associated with control-based privacy beliefs.*

2.4. Trust as a Foundational Construct in Digital Platform Engagement

Trust is central to consumers' interactions with online platforms, particularly social media; it has been identified as a precursor to engagement in digitally mediated interactions (Bansal et al. 2016) and is associated with privacy and security concerns, as well as a lack of transparency regarding the treatment of user data (Zhang and Gupta 2018). According to the seminal definition by Mayer et al. (1995), trust involves exposing vulnerability in the expectation that another party will respond favourably in controlled or uncontrolled environments. This conceptualisation has been widely applied in digital communication and social media research, where trust is associated with continued use despite uncertainties and the risks of self-disclosure and interaction online (Dombrowski and Trepte 2026; Hansen et al. 2018; Krasnova et al. 2010).

In digital contexts, the concept of trust transcends interpersonal trust to include users' assessment of the platform. According to McKnight et al. (2002), and later validated by

Koohang et al. (2021), platform trust is defined by three dimensions: integrity, benevolence, and competence. Integrity is defined as users' trust that a platform will fulfil its promises regarding the protection and privacy of the data that it handles. Benevolence is defined as users' perception that a platform is acting in their best interests, while competence is defined as users' perception of a platform's ability to protect information effectively. These dimensions are strongly related to data governance practices, where the integration of privacy measures comprises integrity, meaningful opportunities for user agency (perceived as benevolence), and the effectiveness of technical safeguard measures (competence). Therefore, trust is associated with various outcomes, such as the willingness to share personal information, satisfaction with platform use, continued usage, acceptance of platform-generated content, and responsiveness to algorithm-generated placements (Eveleth et al. 2024; Grandhi et al. 2021; Xu and Chen 2025); it is also considered essential for maintaining relationships on social media (Koohang et al. 2021).

The widespread use of algorithmic systems and personalised services has led to increased scholarly interest in the factors that influence platform trust. Such digital platforms are becoming increasingly important, as they are the main method of accessing information, conducting commercial transactions, and engaging in social life. This makes it crucial for users to assess whether these systems are transparent and provide autonomy (Xu and Chen 2025). Due to concerns about large-scale data collection, the secondary use of individual data, unintelligible algorithms, and the potential misuse of data, trust has become a key factor in the long-term sustainability of platform ecosystems (Dombrowski and Trepte 2026; Krasnova et al. 2010; Zhang and Gupta 2018). As noted by Zhang and Gupta (2018), trust is more influenced by users' perceived control over their own data than by actual technical security measures; it is also influenced by users' prior experience with online scams and their sensitivity to security cues. This suggests that users' subjective perception of control over their personal information is more important than technical security measures in building trust.

Research has shown that personal data controllability is associated with greater trust in platform providers (Eveleth et al. 2024; Hansen et al. 2018; Krasnova et al. 2010). Control is a governance mechanism that helps to establish cooperative relationships and trust in online environments (Krasnova et al. 2010). Dombrowski and Trepte's (2026) meta-analysis showed that perceived control is consistently associated with users' privacy behaviours, including their use of privacy-protective measures. The study's findings regarding social networking also emphasise the importance of control mechanisms in establishing trust. Krasnova et al. (2010) found that granular privacy settings and robust control processes were better predictors of trust than distributive justice and proactive privacy warnings. This suggests that features that give users more control over the information that they share on social media are important for building trust.

Social cognitive theories that emphasise the importance of beliefs related to control in determining evaluative judgements provide further support for this relationship. Eveleth et al. (2024) found a positive correlation between trust in platform-provided information and knowledge of privacy protection practices. Similarly, Hansen et al. (2018) examined 318 social media users and found that both perceived behavioural control and trust affected behavioural intentions, that trust significantly moderated the development of perceptions of control and users' intent to take risks, and that perceived ease of use significantly moderated the effect of behavioural control on users' intent to use. This indicates that perceived control and trust are correlated and mutually reinforcing, thereby influencing users' reactions to digital platforms.

These insights have been further explored in recent research on algorithmically mediated environments. Xu and Chen (2025) found a positive correlation between the sense of

control experienced when interacting with the system and subsequent satisfaction with—and trust in—the system. In both experimental studies, perceived control, influenced by platform fit and choice visibility, led to evaluations related to trust. The authors also found that these effects depended on users' locus-of-control orientation, with the restriction of visible choices having a more negative impact on those oriented towards internal control. This indicates the importance of designing environments that do not compromise users' perception of autonomy and that offer non-arbitrary opportunities.

Therefore, control is a prerequisite for trust, as well as a process through which privacy can become psychologically relevant to users' judgements of—and interactions with—social media platforms. Users who regard control as central to their privacy may also weigh a platform's controllability more heavily when judging whether it can be trusted. Accordingly, the following hypotheses are proposed:

H2. *Perceived personal data controllability is positively associated with trust in the platform.*

H3. *Control-based privacy beliefs moderate the positive association between perceived personal data controllability and trust in the platform.*

2.5. Anxiety and Privacy-Related Emotional Responses in Social Media Environments

Anxiety has been recognised as influencing experiences in social media environments (Brailovskaia and Margraf 2021). Several studies have found that privacy and data-control features influence users' cognitive, emotional, and behavioural responses to digital environments (Cho et al. 2020; Hajli and Lin 2016). Hajli and Lin (2016) found that perceived control over personal information was negatively correlated with privacy risk perceptions. These perceptions influenced the attitudes, intentions, and disclosures of social networking users. Importantly, the authors distinguished between actual behavioural control and perceived control, emphasising that users' perceptions of control may influence behaviour more than what is actually available to them. This distinction indicates that privacy affordances (such as customisable settings) that are available and usable by users can positively affect their sense of agency, while the actual processing of data remains unchanged.

Further studies have shown that the perception of privacy and control has emotional implications. Based on cognitive appraisal theory, Cho et al. (2020) demonstrated that negative emotions resulting from privacy concerns (e.g., anger, frustration, regret, and anxiety) have distinct mechanisms that influence coping responses. Emotion-focused coping strategies (e.g., disengagement and acceptance) were associated with anxiety and fear, whereas problem-focused strategies (e.g., modifying privacy settings and restricting information disclosure) were associated with frustration and regret. There was no significant decrease in negative emotional reactions with privacy self-efficacy, and a positive correlation was found with regret. Thus, while stronger beliefs about coping with privacy-related uncertainty may not alleviate emotional distress, they may highlight missed opportunities in certain situations.

Additional findings are available regarding the psychological importance of perceived control. Brailovskaia and Margraf (2021) investigated social media use during the COVID-19 pandemic and found that a sense of control mediated the relationship between perceived burden and addictive social media use. Furthermore, they found that anxiety moderated this relationship, such that reduced control was associated with problematic social media use among individuals experiencing moderate-to-high levels of anxiety. The results indicated that a reduced level of control, when paired with high levels of anxiety, may act as a coping mechanism, leading users to become dependent on social media, in a manner similar to that described by Keeton et al. (2008), who found that feelings of low perceived control were associated with anxiety and depressive symptoms when individuals were faced with uncertainty and stress. Overall, these findings suggest that perceived control is a significant

psychological resource in digital environments and plays a central role in how users perceive, cope with, and engage with social media platforms (Brailovskaia and Margraf 2021; Cho et al. 2020; Hajli and Lin 2016). The weight that users place on control may therefore shape how much reassurance they draw from a platform's controllability. Accordingly, the following hypotheses are proposed:

H4. *Perceived personal data controllability is negatively associated with anxiety.*

H5. *Control-based privacy beliefs moderate the negative association between perceived personal data controllability and anxiety.*

2.6. Theoretical Integration

This study draws on theories that originated before the spread of social media but have since been reformulated for digital communication. Affordance theory originated in ecological psychology (Gibson 1979), was extended to designed objects and interfaces by Norman (2013), and was reformulated for communication technologies by Evans et al. (2017), who treat affordances as relational properties that emerge between users and platform features; it is this relational formulation that the present study applies.

Westin's (1967) account of privacy as control over personal information was operationalised for online settings by Malhotra et al. (2004), whose control dimension is used here, and was integrated into the social media privacy model by Trepte (2021), in which perceived control and trust are central to how users regulate their privacy. Perceived control has recently been examined in algorithmic platform environments by Xu and Chen (2025). Similarly, Mayer et al.'s (1995) model of organisational trust was translated to the online environment by McKnight et al. (2002) and validated for social media by Koohang et al. (2021), and cognitive appraisal accounts of emotion were applied to social media privacy by Cho et al. (2020).

Together, these frameworks specify the model tested in this study. The relational view of affordances is the reason that this study measures perceived controllability rather than objective platform features; the social media privacy model positions control-related appraisals as the link between these features to users' responses; and the trust and appraisal frameworks distinguish two kinds of response: an evaluative judgement about the platform, and an affective state regulated by users' own resources. Digital sovereignty supplies the overarching framework, in which control-based privacy beliefs are treated as the experiential, individual-level expression of the broader concept.

3. Methods

3.1. Research Design

This study used a scenario-based survey design, in which participants were first exposed to a simulated social media platform. This design was used to explore the associations between participants' perceptions and platform features, rather than their causal effects, as the study did not include a control group.

This design follows comparable studies of users' responses to platform features. Xu and Chen (2025) presented participants with a recommendation scenario before measuring perceived control and trust, while Cho et al. (2020) used survey-based measurement to capture users' privacy appraisals and emotional responses on social media. Unlike Xu and Chen (2025), who manipulated platform features across experimental conditions, the present study used a single condition, which supports associational rather than causal inference.

Participants were shown a mock-up of a platform interface with elements designed to convey transparency, autonomy, and control over personal information. After reviewing

this, they completed a questionnaire assessing their perceptions of the platform and their psychological responses to it. The design aimed to capture the relationships among perceived personal data controllability, control-based privacy beliefs, trust in the platform, and anxiety. Therefore, the present study focuses on the experience of digital sovereignty in a platform environment and its connection with users' evaluative and affective reactions.

3.2. Participants

A total of 308 Saudi participants took part in the study. Data were collected online between 22 April 2026 and 31 August 2026, after ethical approval had been granted [9 March 2026]. Participants were recruited voluntarily through social media advertisements using convenience sampling, and no financial or other incentives were offered. Saudi Arabia was chosen as the study setting for two reasons: First, the Personal Data Protection Law (SDAIA 2021) came into force in September 2023, and its one-year compliance period ended in September 2024; data collection therefore took place under a fully enforceable system of individual data rights. Second, social media use in Saudi Arabia is exceptionally widespread: Internet use is near-universal (99.0%), and social media user identities were equivalent to 111% of the population in late 2025 (Kemp 2025). Saudi Arabia is therefore a setting in which users can be expected to attend to how platforms present privacy and data controls.

To be eligible, participants had to be Saudi nationals aged 18 years or older and active users of at least one social media platform. Saudi nationality ensured that the participants shared the cultural and regulatory context of the study and were fluent in Arabic, the language in which the simulated platform was presented; nationality approximated, rather than strictly measured, exposure to the Saudi regulatory context. The minimum age ensured legal capacity to give informed consent, and active use ensured that participants could evaluate the simulated platform against first-hand experience of comparable platforms. No further criteria were applied, so as not to restrict the range of the study variables in the sample.

A sensitivity power analysis conducted in G*Power 3.1 (Faul et al. 2009) indicated that, with N = 308, $\alpha = 0.05$, and power = 0.80, the study could detect effects as small as $f^2 = 0.026$ for a single regression coefficient, including the interaction terms in the moderation models, which corresponds to a small effect (Cohen 1988). The sample comprised 147 men (47.7%) and 161 women (52.3%), aged 18–56 years (M = 29.76, SD = 9.12); as a convenience sample, it is not representative of the Saudi population. Most of the participants reported using social media daily (71.1%, Table 1).

Table 1. Participant characteristics ($N = 308$).

Characteristics	*n*	%
Gender: male	147	47.7
Gender: female	161	52.3
Age: 18–24	113	36.7
Age: 25–34	119	38.6
Age: 35–44	50	16.2
Age: 45–56	26	8.4
Social media use: daily	217	71.1
Social media use: several days a week	56	18.4
Social media use: twice a week	25	8.2
Social media use: once a week	7	2.3

Note: Age: M = 29.76, SD = 9.12. Percentages for social media use are based on n = 305 because of three missing responses.

3.3. Stimulus Materials

The platform stimulus was a mock social media interface, named Moments (Arabic لحظات), designed specifically for this study. Privacy and personal data control were highlighted as important and salient features that were easily accessible to users. The platform was set up with clear privacy options and detailed controls over post visibility and data sharing; it also provided clear explanations of data handling and consent-driven data usage options, as well as options to review, edit, manage, and delete personal information. These features were described on successive screens, on each of which the participants selected every option to confirm that they had read it before they could continue, in order to simulate an environment in which users could experience informational self-determination. The simulation was limited to interface-level privacy and data-control features (visibility settings, consent options, and review and deletion of account-linked data) and did not represent open-source governance, interoperability, or data portability. Eight example screens, translated into English, are provided in Supplementary Material S1.

3.4. Procedure

This study was conducted in accordance with the ethical principles set out in the 1975 Declaration of Helsinki (revised in 2013). Ethical approval for the research was obtained before data collection. All procedures involving human participants complied with institutional, national, and international ethical standards.

After accessing the online survey, participants completed the following steps in a fixed order (example screens are provided in Supplementary Material S1):

1. Information and Consent: Participants read information on the purpose of the study, the voluntary nature of participation, their right to withdraw at any time, and the anonymous and confidential handling of their responses, and they gave informed consent electronically.
2. Instructions: Participants were asked to imagine that they were creating an account on, and using, a new social media platform, as well as to examine each screen carefully, including its settings, information display, and control options.
3. Welcome and Account Setup: Participants viewed the welcome screen and the account setup screen on which a username and a profile picture were selected.
4. Introduction to Data and Privacy Controls: A screen explained how the platform handles personal data and introduced the controls available to users.
5. Privacy and Data-Control Screens: Participants viewed, in turn, the post-visibility controls, the information-sharing controls, the account-information management screen, and the privacy-settings screen, which included consent options for data use and the review, editing, and deletion of account-linked data. On each of these screens, participants selected every option to confirm that they had read it before they could proceed.
6. Feed and Profile: Participants viewed the main feed and the profile page, which displayed their account information with an option to edit it, after which a closing screen directed them to the questionnaire.
7. Questionnaire: Participants completed the measures described in Section 3.5, followed by demographic questions.
8. Debriefing: Participants were informed of the focus of the research.

No personally identifying information was collected beyond the demographic variables required for the study. Survey responses were anonymised before analysis and stored on password-protected institutional systems, which were only accessible to the research team. Data were retained in accordance with the university's research data management policy and then securely deleted.

3.5. Measures

3.5.1. Demographic Variables

Participants were asked to report demographic information, including age, gender, and frequency of social media use.

3.5.2. Perceived Personal Data Controllability

Perceived personal data controllability was assessed with two items developed for this study and administered in Arabic: "This platform gives users strong control over their personal information", and "This platform makes privacy settings clear and manageable" (English translations; all items are listed in Appendix A). Both items describe what the platform enables users to do, in line with the definition of an affordance as a possibility for action rather than a feature (Evans et al. 2017), and they correspond to the platform's account-information management and privacy-settings screens and to its post-visibility and information-sharing screens, respectively (Supplementary Material S1). Participants rated each item on a 7-point scale (1 = strongly disagree, 7 = strongly agree), and the ratings were summed (possible range 2–14), with higher scores indicating greater perceived controllability.

A third item, "This platform is transparent about how user data are managed", was administered but excluded from the index because it describes a state of the platform rather than a possibility for action available to users. The two retained items are treated as reflective indicators of a single construct. They were strongly correlated ($r = 0.70$), and the Spearman–Brown coefficient, the recommended reliability estimate for two-item scales (Eisinga et al. 2013), was 0.82. As this study used a single-condition design, the items were not used as a manipulation check. The index measured participants' subjective evaluations of the platform and served as the independent variable in all analyses.

3.5.3. Control-Based Privacy Beliefs

Control-based privacy beliefs were measured using the three items of the control dimension of the Internet Users' Information Privacy Concerns (IUIPC) scale (Malhotra et al. 2004), adapted minimally to refer to the simulated platform (e.g., "Users' privacy on this platform depends on having control and autonomy over decisions about how personal information is collected, used, and shared"; see Appendix A). Responses were recorded on a 7-point Likert scale ranging from 1 = strongly disagree to 7 = strongly agree. The item scores were summed (possible range 3–21), with higher scores indicating stronger control-based privacy beliefs. Internal consistency was acceptable for a three-item scale ($\alpha = 0.76$; Table 2). The items capture the importance that participants attach to control for their privacy on the platform rather than their sense of exercising control, and the construct is labelled accordingly.

Table 2. Reliability of measures.

Construct	Reliability	Number of Items
Perceived personal data controllability	0.82 [a]	2
Control-based privacy beliefs	0.76	3
Trust	0.95	11
Anxiety	0.84	6

Note: Values are Cronbach's α except where marked. [a] Spearman–Brown coefficient, reported instead of Cronbach's α for the two-item scale (Eisinga et al. 2013).

3.5.4. Trust in the Platform

Trust in the platform was measured using the Trusting Beliefs scale developed by McKnight et al. (2002), which assesses three dimensions—benevolence (3 items), integrity (4 items), and competence (4 items)—totalling 11 items. The items were adapted minimally so that they referred to the simulated platform rather than the original website context. The scale demonstrated high reliability (Cronbach's $\alpha = 0.95$). Responses were recorded on a 7-point Likert scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*. The item scores were summed (possible range 11–77), with higher scores indicating greater trust.

3.5.5. Anxiety

Anxiety was measured using the six-item short form of the State Anxiety Scale from the State-Trait Anxiety Inventory (STAI-6), which was developed by Marteau and Bekker (1992) and captures participants' current state of anxiety. Participants were asked to indicate how they felt at that very moment, and their responses were recorded on a 4-point scale ranging from 1 = *not at all* to 4 = *very much so*. The items indicating an absence of anxiety were reverse-coded before scoring, and the item scores were averaged (possible range 1–4), with higher scores indicating greater state anxiety. The reliability of the six-item scale was good ($\alpha = 0.84$).

3.6. Data Analysis

The data were analysed using IBM SPSS Statistics 27 and the PROCESS macro (Hayes 2022) to test the study's hypotheses. Before hypothesis testing, the data were screened for completeness and accuracy of coding, as well as for potential entry errors. Descriptive statistics were computed for all study variables, and preliminary analyses were performed to examine distributions, central tendencies, and variability. Bivariate correlations were examined to assess initial relationships between the focal variables.

To test H1, H2, and H4, simple linear regression analyses were performed to examine whether perceived personal data controllability was associated with control-based privacy beliefs (H1), trust in the platform (H2), and anxiety (H4). All five models were also re-estimated with age, gender, and frequency of social media use as covariates. Throughout, "predict" and "predictor" refer to terms of the statistical models and carry no causal implication.

The moderation hypotheses (H3 and H5) were tested using PROCESS Model 1 (Hayes 2022), with control-based privacy beliefs as the moderator. Because the Breusch–Pagan test indicated heteroskedasticity in the model for trust, both moderation models were estimated with heteroskedasticity-consistent standard errors (HC3), for consistency and robust inference.

In both models, the two variables were mean-centred before the interaction term was computed, so that lower-order coefficients represented conditional associations at the mean of the other variable, and the interaction term was used to determine whether the association between controllability and the outcome varied with control-based privacy beliefs.

Conditional effects were examined at low, medium, and high levels of the moderator, corresponding to the 16th, 50th, and 84th percentiles of control-based privacy beliefs generated by PROCESS. This made it possible to interpret how the association between perceived controllability and each outcome changed across levels of the moderator.

All statistical tests were evaluated at a 95% confidence level and an α level of 0.05. Regression coefficients, standard errors, test statistics, p-values, and confidence intervals (CIs) were reported for all analyses. The assumptions of regression analysis, such as linearity, independence of errors, homoscedasticity, and lack of multicollinearity, were examined before the results were interpreted.

4. Results

4.1. Preliminary Analyses

Descriptive statistics for the main study variables are presented in Table 3. Across the 308 participants, the mean score for perceived personal data controllability was 10.74 (SD = 2.29), the mean score for control-based privacy beliefs was 16.00 (SD = 3.24), the mean trust score was 60.42 (SD = 10.97), and the mean anxiety score was 1.83 (SD = 0.72). The distributions of the variables were examined using skewness and kurtosis values and did not indicate severe deviations from normality. These findings suggest that the data were appropriate for subsequent analyses.

Table 3. Descriptive statistics for the main study variables.

Variable	N	Min	Max	M	SD	Skewness	Kurtosis
Controllability	308	4.00	14.00	10.74	2.29	−0.68	−0.29
Control-based beliefs	308	7.00	21.00	16.00	3.24	−0.53	−0.33
Trust	308	27.00	77.00	60.42	10.97	−0.65	−0.03
Anxiety	308	1.00	3.67	1.83	0.72	0.32	−1.29

4.2. Correlation Analysis

Pearson's product–moment correlation coefficients were computed to examine the bivariate associations among the main study variables. As presented in Table 4, perceived personal data controllability was positively and significantly associated with control-based privacy beliefs ($r = 0.66$, $p < 0.001$) and trust in the platform ($r = 0.80$, $p < 0.001$), and negatively and significantly associated with anxiety ($r = -0.48$, $p < 0.001$). Control-based privacy beliefs were also positively and significantly related to trust in the platform ($r = 0.67$, $p < 0.001$) and negatively and significantly associated with anxiety ($r = -0.34$, $p < 0.001$). Finally, trust in the platform was negatively and significantly associated with anxiety ($r = -0.46$, $p < 0.001$).

Table 4. Pearson correlations among the main study variables.

Variable	1	2	3	4
1. Controllability	—			
2. Control-based beliefs	0.66 ***	—		
3. Trust	0.80 ***	0.67 ***	—	
4. Anxiety	−0.48 ***	−0.34 ***	−0.46 ***	—

Note: *** $p < 0.001$.

4.3. Hypothesis Testing

H1. *Perceived personal data controllability is positively associated with control-based privacy beliefs.*

A simple linear regression analysis was performed to examine the association between perceived personal data controllability and control-based privacy beliefs. Before interpreting the regression model, the relevant assumptions were assessed. The histogram and normal P–P plot of standardised residuals indicated approximate normality, with minor deviations. The scatterplot of standardised residuals against standardised predicted values suggested no serious violations of linearity or homoscedasticity. Although a few studentised deleted residuals exceeded the conventional cutoff of ±3 (range −4.27 to 3.12), Cook's distance remained below 1 (maximum = 0.086), indicating that no single observation had an undue influence on the model. The results showed that the model was statistically significant

($F(1, 306) = 237.61$, $p < 0.001$, $R^2 = 0.437$). Perceived personal data controllability was a significant positive predictor of control-based privacy beliefs (b = 0.936, SE = 0.061, β = 0.661, t = 15.42, $p < 0.001$, 95% CI [0.816, 1.055]).

H2. *Perceived personal data controllability is positively associated with trust in the platform.*

A simple linear regression analysis was performed to examine the association between perceived personal data controllability and trust. Before interpretation, regression assumptions were examined. The histogram and normal P–P plot of standardised residuals indicated that they were approximately normal, with only minor deviations. The scatterplot of standardised residuals against standardised predicted values showed no violation of linearity, although the spread of residuals narrowed slightly at higher predicted values, reflecting the upper limit of the trust scale; given the strength of the association, this does not affect the inference. Although a few studentised deleted residuals exceeded the conventional cutoff of ±3 (minimum = −4.18), Cook's distance values remained well below 1 (maximum = 0.105), indicating that no observation exerted undue influence on the regression model.

A simple linear regression analysis revealed that the model was statistically significant ($F(1, 306) = 545.87$, $p < 0.001$, $R^2 = 0.641$). Perceived personal data controllability was a significant positive predictor of trust (b = 3.839, SE = 0.164, β = 0.800, t = 23.36, $p < 0.001$, 95% CI [3.516, 4.163]).

H3. *Control-based privacy beliefs moderate the positive association between perceived personal data controllability and trust in the platform.*

PROCESS Model 1 was used to examine whether control-based privacy beliefs moderate the association between perceived personal data controllability and trust in the platform. Preliminary diagnostic analyses based on the Breusch–Pagan test indicated heteroskedasticity ($\chi^2(3) = 14.39$, $p = 0.002$); therefore, the moderation model was estimated using HC3, which offers a more reliable estimate in the presence of heteroskedasticity.

The overall model was statistically significant ($F(3, 304) = 190.65$, $p < 0.001$), explaining 67.5% of the variance in trust ($R^2 = 0.675$). Because the model was estimated with HC3 standard errors, the reported F is a heteroskedasticity-robust statistic and is not algebraically equivalent to the OLS F implied by R^2. Perceived personal data controllability was a significant positive predictor of trust (b = 3.141, HC3 SE = 0.238, t = 13.19, $p < 0.001$, 95% CI [2.672, 3.609]), as were control-based privacy beliefs (b = 0.841, HC3 SE = 0.173, t = 4.87, $p < 0.001$, 95% CI [0.501, 1.181]); however, the interaction between controllability and control-based privacy beliefs was not statistically significant (b = 0.053, HC3 SE = 0.056, t = 0.93, $p = 0.351$, 95% CI [−0.058, 0.163]). Therefore, H3 was not supported.

H4. *Perceived personal data controllability is negatively associated with anxiety.*

A simple linear regression analysis was performed to examine the association between perceived personal data controllability and anxiety levels. Before interpretation, regression assumptions were assessed. The histogram and normal P–P plot of standardised residuals indicated approximate normality, with a slight positive skew. The scatterplot of standardised residuals against standardised predicted values showed no curvilinear pattern; the residuals were bounded from below at low predicted values, reflecting participants who scored at or near the minimum of the anxiety scale, and the Breusch–Pagan test in the corresponding moderation model indicated no heteroskedasticity. Although the largest studentised deleted residual (3.48) slightly exceeded the conventional cutoff of ±3, Cook's distance values

remained well below 1 (maximum = 0.053), indicating that no observation exerted undue influence on the model.

The results showed that the model was statistically significant ($F(1, 306) = 91.71$, $p < 0.001$, $R^2 = 0.231$) and that perceived personal data controllability was a significant negative predictor of anxiety ($b = -0.153$, SE = 0.016, $\beta = -0.480$, $t = -9.58$, $p < 0.001$, 95% CI [−0.184, −0.121]), supporting H4.

H5. *Control-based privacy beliefs moderate the negative association between perceived personal data controllability and anxiety.*

PROCESS Model 1 was used to test whether control-based privacy beliefs moderate the association between perceived personal data controllability and anxiety. Collinearity diagnostics were acceptable (VIF = 1.24–1.91). The residuals were approximately normally distributed (skewness = 0.44, kurtosis = −0.17), there were no highly influential cases (largest studentised residual = 3.35, Bonferroni-corrected $p = 0.280$), and the Breusch–Pagan test revealed no evidence of heteroskedasticity ($\chi^2(3) = 0.93$, $p = 0.819$); HC3 standard errors were nevertheless used for consistency with the model for trust.

The overall model was statistically significant ($F(3, 304) = 34.78$, $p < 0.001$), explaining 24.9% of the variance in anxiety ($R^2 = 0.249$). At the mean of the other variable, perceived controllability was significantly negatively associated with anxiety ($b = -0.129$, HC3 SE = 0.022, $t = -5.94$, $p < 0.001$), whereas control-based privacy beliefs were not ($b = -0.004$, HC3 SE = 0.016, $t = -0.25$, $p = 0.803$). The interaction between controllability and control-based privacy beliefs was statistically significant ($b = 0.012$, HC3 SE = 0.005, $t = 2.33$, $p = 0.020$, 95% CI [0.002, 0.022], $\Delta R^2 = 0.018$). Conditional effects analysis showed that the negative association between controllability and anxiety was strongest at low levels of control-based privacy beliefs (16th percentile: $b = -0.165$, $p < 0.001$), weaker at the median ($b = -0.129$, $p < 0.001$), and weakest—though still significant—at high levels (84th percentile: $b = -0.093$, $p = 0.002$).

Re-estimating all five models with age, gender, and frequency of social media use as covariates ($n = 305$, because of three missing responses on frequency of use) did not change the direction or significance of any hypothesised association (H1: $\beta = 0.596$; H2: $\beta = 0.792$; H4: $\beta = -0.464$, all $p < 0.001$; H3 interaction: $b = -0.027$, $p = 0.603$; H5 interaction: $b = 0.014$, $p = 0.010$; Supplementary Table S1).

Overall, four of the five hypotheses were supported (Table 5). Perceived personal data controllability was positively associated with control-based privacy beliefs (H1) and with trust in the platform (H2), and negatively associated with anxiety (H4). Control-based privacy beliefs moderated the association between controllability and anxiety, which was strongest among participants with weaker control-based privacy beliefs (H5), but did not moderate the association between controllability and trust (H3).

Table 5. Summary of hypothesis tests.

Hypothesis	Test	b	95% CI	*p*	Result
H1. Perceived personal data controllability is positively associated with control-based privacy beliefs.	Simple linear regression	0.936	[0.816, 1.055]	<0.001	Supported
H2. Perceived personal data controllability is positively associated with trust in the platform.	Simple linear regression	3.839	[3.516, 4.163]	<0.001	Supported

Table 5. *Cont.*

Hypothesis	Test	b	95% CI	*p*	Result
H3. Control-based privacy beliefs moderate the positive association between perceived personal data controllability and trust in the platform.	PROCESS Model 1 (HC3)	0.053	[−0.058, 0.163]	0.351	Not supported
H4. Perceived personal data controllability is negatively associated with anxiety.	Simple linear regression	−0.153	[−0.184, −0.121]	<0.001	Supported
H5. Control-based privacy beliefs moderate the negative association between perceived personal data controllability and anxiety.	PROCESS Model 1 (HC3)	0.012	[0.002, 0.022]	0.020	Supported

Note: b = unstandardised coefficient; for H3 and H5, b is the coefficient of the controllability × control-based privacy beliefs interaction term. H3 and H5 were estimated with heteroskedasticity-consistent (HC3) standard errors. The positive interaction coefficient for H5 indicates that the negative association between controllability and anxiety weakened as control-based privacy beliefs strengthened.

5. Discussion and Conclusions

This research was based on affordance theory, the conception of privacy as control, and the digital sovereignty framework. These theories were used to analyse the association of perceived personal data controllability with control-based privacy beliefs, trust in the platform, and anxiety within a simulated social media environment; four of the five hypotheses were supported. Perceived controllability was positively associated with control-based privacy beliefs (H1) and trust in the platform (H2) and negatively associated with anxiety (H4). Control-based privacy beliefs were also found to moderate the controllability-anxiety association (H5). Only H3 was not supported, as there was insufficient evidence that control-based privacy beliefs moderate the controllability-trust association. Therefore, the results indicate that perceived controllability is associated with users' cognitive evaluations and affective responses, and that control-based privacy beliefs operate as a boundary condition within the affective pathway rather than the evaluative one.

Support for H1 is consistent with the relational view of affordances outlined in Section 2.6 (Evans et al. 2017; Gibson 1979; Norman 2013), in which interface elements serve as interpretive resources that guide how people act in digital environments. When a platform makes control over personal data visibly possible, users appear more inclined to judge their privacy on that platform in terms of control. This is consistent with Westin's (1967) definition of privacy as a claim to control over personal information—a notion supported by the privacy literature (Malhotra et al. 2004; Xu et al. 2011). Because the items capture the importance that users attach to control rather than their sense of exercising it, H1 indicates that controllability is associated with the salience of control as a privacy standard, not necessarily with a feeling of being in control. Recent evidence from social media platforms supports this, showing that stronger privacy governance mechanisms enhance users' control over their personal data (Xiao 2025). These results corroborate the finding of Van Ooijen and Vrabec (2019) that effective control cannot be achieved solely through legislation but can be partially realised through interface design.

The affordance–trust relationship (H2) was supported, extending previous studies on procedural control and trust formation. In terms of the frameworks outlined in Section 2.6, this result links the relational view of affordances to the online trust model (McKnight et al. 2002): visible privacy and data-control features appear to serve as cues to the plat-

form's integrity, benevolence, and competence. In terms of the levels distinguished in Section 2.1, trust is thus a user-level judgement about how digital sovereignty is exercised at the platform level.

Although affordance theory has traditionally centred on action affordances (Gibson 1979; Norman 2013), this finding indicates a communicative aspect, whereby the affordance of action is communicated to users via visible cues that convey integrity, competence, and benevolence before their interaction with an interface (Koohang et al. 2021; McKnight et al. 2002). This aligns with the idea that affordances are significant trust indicators that may inform the evaluative perceptions in initial impressions, providing an elaboration of affordance theory with direct implications for platform design. Recent evidence supports this interpretation, with clearly communicated privacy policies being found to be associated with higher user trust and platform engagement (Xiao 2025).

Contrary to the idea that control-based privacy beliefs would strengthen the controllability-trust association, H3 was not significant. Previous studies have linked control to trust, either as a direct predictor (Krasnova et al. 2010) or as a mediating mechanism between platform design and trust (Xu and Chen 2025); however, these studies have not considered control-related beliefs as a conditioning factor. The present result is consistent with these models. Perceived controllability was directly and independently associated with control-based privacy beliefs and trust in the platform, indicating a simpler structure than anticipated in H3. In this context, trust appears to be formed based on what the platform makes visible, rather than on how much weight users place on control, meaning that the evaluative pathway operates uniformly across users.

Perceived personal data controllability was negatively associated with anxiety (H4), indicating that participants who perceived more opportunities to control their personal data reported lower levels of anxiety. This finding is consistent with the view that privacy affordances are factors that mitigate anxiety (Cho et al. 2020; Hajli and Lin 2016). Cho et al. (2020) found that threat appraisals and the perceived severity of privacy risks were strongly associated with anxiety and fear. The present findings suggest that visible privacy affordances may be linked to lower perceived severity that users attribute to these risks. Interview evidence points to the same mechanism, with perceived control helping to explain fear and feelings of helplessness following privacy-invasive experiences on algorithmic social media platforms (Kang et al. 2026). Meanwhile, qualitative work has shown that social media affordances are implicated in users' emotional regulation processes more generally (Peng et al. 2024).

The moderating role of control-based privacy beliefs was supported for anxiety (H5). The negative association between controllability and anxiety was stronger among participants who held weaker control-based privacy beliefs and weaker among those who held stronger beliefs. One interpretation is that users who place less weight on control rely more on what the platform signals, so that visible controllability is most reassuring for them, whereas users who regard control as central to their privacy remain more vigilant and draw comparatively less reassurance from the same features—a pattern that echoes the control paradox discussed below (Brandimarte et al. 2013). The finding is also broadly consistent with that of Zhuang et al. (2023), who found that perceived control moderated users' privacy regulation responses to cross-platform information sharing, suggesting more generally that control-related appraisals condition how users respond to platform practices. The contrast between this result and the non-significant moderation observed for trust (H3) is informative from a theoretical perspective, as the same moderator behaved differently across the two outcomes. Trust is a judgement about the platform, formed by what the platform makes visible (Mayer et al. 1995; McKnight et al. 2002), whereas anxiety is a user state regulated by users' own resources and dispositions (Cho et al. 2020). Control-based

privacy beliefs are one such disposition, which is consistent with their moderating role for the emotional response but not for the evaluative one. This contrast corresponds to the distinction drawn in Section 2.6 between an evaluative judgement about the platform and an affective state regulated by users' own resources.

These associations should also be read critically: Brandimarte et al. (2013) showed that increasing users' sense of control can lead them to disclose more sensitive information even when objective risks remain unchanged—a pattern that they termed the control paradox. In the present study, the controllability associated with stronger control-based privacy beliefs, greater trust, and lower anxiety derived from interface-level controls; this simulation did not show the participants how their data would actually be processed. Greater trust and reduced anxiety may therefore reflect reassurance rather than protection and, on real platforms, could lower users' vigilance towards data practices that visible controls do not govern. From a digital sovereignty perspective, the experiential dimension examined here is thus necessary but not sufficient: perceived controllability is meaningful only insofar as it corresponds to users' actual capacity to determine how their data are used (Hajli and Lin 2016; Van Ooijen and Vrabec 2019).

These findings are meaningful within the Saudi context. The Personal Data Protection Law (SDAIA 2021) has increased awareness of data rights and platform accountability among a population with near-universal Internet use and very high social media use (Kemp 2025). Users who are already attentive to how platforms handle their data are likely to trust those with visible privacy controls, which may help explain the strength of the affordance–trust relationship observed here.

Although digital sovereignty is the overarching theoretical framework of this study, it was not used as an independent empirical construct. Instead, this study investigated a user-specific experiential aspect of digital sovereignty: control-based privacy beliefs and the perceived controllability of personal data. From this perspective, the results can be understood not as measures of digital sovereignty itself but as preliminary empirical findings on a way in which users can gain more control over digital platforms. Future research should therefore focus on developing and testing multidimensional measures of digital sovereignty that better account for legal, technical, governance, and psychological elements.

Furthermore, as only one test condition was used, the results of this study support inferences of predictive rather than causal relationships. Although the simulated platform allowed participants to evaluate privacy and data control in a controlled environment, future studies incorporating multiple conditions and random assignment will be required in order to understand causal effects. The moderation findings should also be replicated using larger, more diverse samples to establish whether the significant interaction observed for anxiety and the non-significant interaction observed for trust remain stable in different settings.

In addition, the generalisability of the findings is limited in three respects. First, the sample was a convenience sample recruited through social media advertisements and is not representative of Saudi social media users. Second, the study was conducted in a single country, operating under a single data protection regime, and participants evaluated a single hypothetical platform. The associations observed may therefore reflect the regulatory and cultural context of Saudi Arabia and the design of this particular interface, and they should be tested across countries and across platforms that differ in design. Third, the sample was predominantly young, as about three-quarters of participants (75.3%) were under 35 years of age. Younger users tend to use social media more extensively (Kemp 2025) and may hold different privacy perceptions from older users; the findings are therefore likely to over-represent their perspective. Although controlling for age did not change the direction or significance of any hypothesised association (Section 4.3; Supplementary Table S1), the findings should be replicated with samples that include more older users.

Participants' education level was also not recorded. This is a limitation for a platform-based study, because education is associated with digital literacy, privacy awareness, and trust in technology, which may shape how users perceive and respond to privacy affordances. Future research should measure education and examine it as a covariate or moderator.

Moreover, the controllability index was short and study-specific, comprising two items after an item describing platform transparency was excluded because it did not refer to a possibility for action. Its strong correlation with trust ($r = 0.80$) indicates close coupling between perceived controllability and evaluations of the platform rather than a relationship between fully independent constructs. In addition, perceived control—users' sense of exercising control over their information—was not measured; the IUIPC items used capture the importance attached to control rather than the experience of it. Future research should develop and validate a fuller, platform-independent measure of perceived personal data controllability and measure perceived control directly alongside control-based privacy beliefs.

The findings of the present study also rest on the evaluation of a simulated platform rather than on observed behaviour on platforms that participants actually use, and there may be a gap between such hypothetical evaluations and real-world behaviour. In particular, the salience of privacy features in the simulation was deliberately high and is unlikely to be matched on commercial platforms. Finally, because the simulation did not include open-source governance, interoperability, or data portability, this study cannot speak to these features, which belong to the technical and structural dimension of digital sovereignty rather than to the experiential dimension examined here. Whether such structural guarantees are associated with trust and anxiety to the same degree as visible controls is a direct question for future research.

The results suggest that the controllability that platforms make visible is associated with users' trust, their beliefs about control, and their emotional responses in simulated platform environments. While these findings offer platform designers and digital communication practitioners' initial insights, they should not be interpreted as evidence that such platform attributes will lead to comparable effects in real-world platforms and user groups (Kuan and Lee 2023). Theoretically, this study contributes to the growing human-centred strand of digital sovereignty research (Behera et al. 2026) by treating control-based privacy beliefs as an experiential expression of the broader concept, and by testing their associations with perceived controllability, trust, and anxiety empirically.

Although the results do not offer a definitive understanding of digital sovereignty, they provide an initial empirical basis for investigating the relationship between perceptions of affordances and feelings of agency and trust in platforms (Floridi 2020; Pohle and Thiel 2020). Overall, the findings suggest that users who perceive greater personal data controllability report stronger control-based privacy beliefs, greater trust, and lower anxiety in a simulated social media environment. Furthermore, control-based privacy beliefs moderate the controllability-anxiety association but not the controllability–trust association. These findings provide preliminary evidence that users' perceptions of platform design may be relevant to discussions of digital sovereignty at the individual level. However, further research is required before broader conclusions can be drawn regarding platform design, governance, or digital policy.

By building on the present study, future research could investigate whether perceived control, measured directly, mediates the association between perceived personal data controllability and platform trust. This would provide further insight into the psychological mechanisms through which platform affordances are associated with users' evaluations. Similarly, this study relied exclusively on self-reported perceptions collected after exposure to a simulated platform. While this approach was suitable for evaluating subjective percep-

tions, it did not capture actual privacy-related behaviour. Future studies could strengthen the ecological validity of their research by incorporating behavioural measures, such as logs of participants' interactions with privacy settings, alongside self-report measures.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/socsci15110767/s1. Supplementary Material S1: Example screens of the simulated platform (Moments); Table S1: Hypothesis tests re-estimated with age, gender, and frequency of social media use as covariates.

Author Contributions: Conceptualization, S.A.; Methodology, S.A.; Software, M.A.; Formal analysis, S.A.; Investigation, M.A.; Resources, S.A.; Writing—original draft, M.A. and S.A.; Writing—review & editing, M.A. and S.A.; Visualization, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by Ethics Committee of the Faculty of Communication and Media at KAU (protocol code FCM-REC-05-2026, 9 March 2026).

Informed Consent Statement: Informed consent was obtained from all participants in the study.

Data Availability Statement: The datasets collected and analysed during this study are available from the corresponding author upon request and subject to institutional ethical approval.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Questionnaire Items

All items were administered in Arabic; English translations are given below. Items in A1 and A2 followed the instruction "Please indicate the extent to which you agree with the following statements about the privacy and data-control features of the platform presented to you."

A1. Perceived personal data controllability (developed for this study; 1 = strongly disagree to 7 = strongly agree)

1. This platform gives users strong control over their personal information.
2. This platform makes privacy settings clear and manageable.

Administered but excluded from the index (see Section 3.5.2): This platform is transparent about how user data are managed.

A2. Control-based privacy beliefs (adapted from the IUIPC control dimension, Malhotra et al. 2004; 1 = strongly disagree to 7 = strongly agree)

1. Control over personal information is an important aspect of privacy on this platform.
2. I believe my privacy would be invaded on this platform if I lost control over how my personal information is collected, used, and shared.
3. Users' privacy on this platform depends on having control and autonomy over decisions about how personal information is collected, used, and shared.

A3. Trust in the platform (adapted from McKnight et al. 2002; 1 = strongly disagree to 7 = strongly agree)

Benevolence: 1. I believe that this platform would act in my best interest. 2. If I required help, this platform would do its best to help me. 3. This platform is interested in my well-being, not just its own.

Integrity: 4. This platform is truthful in its dealings with users. 5. I would characterize this platform as honest. 6. This platform would keep its commitments. 7. This platform is sincere and genuine.

Competence: 8. This platform is competent and effective in doing what it is supposed to do. 9. This platform performs its role very well. 10. Overall, this platform is a capable and

proficient social media platform. 11. In general, this platform is very capable of managing its services effectively.

A4. State anxiety (STAI-6; Marteau and Bekker 1992; instruction: indicate how you feel right now, at this moment; 1 = not at all to 4 = very much so)

1. I feel calm (R). 2. I am tense. 3. I feel upset. 4. I am relaxed (R). 5. I feel content (R). 6. I am worried.

Note: (R) = reverse-coded before scoring.

References

Adler-Nissen, Rebecca, and Kristin Anabel Eggeling. 2024. The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *Journal of Common Market Studies* 62: 993–1011. [CrossRef]

Angulo, Julio, Simone Fischer-Hübner, Erik Wästlund, and Tobias Pulls. 2012. Towards usable privacy policy display and management. *Information Management & Computer Security* 20: 4–17. [CrossRef]

Bansal, Gaurav, Fatemeh Mariam Zahedi, and David Gefen. 2016. Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management* 53: 1–21. [CrossRef]

Behera, Tarun Kumar, Sanjay Misra, Biswajeeban Mishra, and Petter Kvalvik. 2026. Role of human-centric approach toward digital sovereignty: A systematic literature review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 16: e70105. [CrossRef]

Brailovskaia, Julia, and Jürgen Margraf. 2021. The relationship between burden caused by coronavirus (COVID-19), addictive social media use, sense of control and anxiety. *Computers in Human Behavior* 119: 106720. [CrossRef] [PubMed]

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4: 340–47. [CrossRef]

Cavoukian, Ann. 2011. *Privacy by Design: The 7 Foundational Principles*. Toronto: Information and Privacy Commissioner of Ontario.

Cho, Hichang, Pengxiang Li, and Zhang Hao Goh. 2020. Privacy risks, emotions, and social media: A coping model of online privacy. *ACM Transactions on Computer-Human Interaction* 27: 40. [CrossRef]

Cohen, Jacob. 1988. *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. Mahwah: Lawrence Erlbaum Associates.

Couture, Stephane, and Sophie Toupin. 2019. What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society* 21: 2305–22. [CrossRef]

Dombrowski, Jana, and Sabine Trepte. 2026. Taking stock of social media privacy: Meta-analytic evidence on how control, trust, and concerns are associated with social media use, disclosure, and protection. *Journal of Computer-Mediated Communication* 31: zmaf025. [CrossRef]

Eisinga, Rob, Manfred te Grotenhuis, and Ben Pelzer. 2013. The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown? *International Journal of Public Health* 58: 637–42. [CrossRef] [PubMed]

Evans, Sandra K., Katy E. Pearce, Jessica Vitak, and Jeffrey W. Treem. 2017. Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication* 22: 35–52. [CrossRef]

Eveleth, Daniel M., Robert W. Stone, and Lori J. Baker-Eveleth. 2024. Social media users trust in their most frequently used social media site. *Online Journal of Communication and Media Technologies* 14: e202445. [CrossRef]

Faul, Franz, Edgar Erdfelder, Axel Buchner, and Albert-Georg Lang. 2009. Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods* 41: 1149–60. [CrossRef] [PubMed]

Feng, Guangchao Charles, Xianglin Su, and Yiru He. 2024. A Meta-Analytical Review of the Determinants of Social Media Discontinuance Intentions. *Mass Communication and Society* 27: 525–50. [CrossRef]

Floridi, Luciano. 2020. The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology* 33: 369–78. [CrossRef] [PubMed]

Fox, Jesse, and Bree McEwan. 2017. Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale. *Communication Monographs* 84: 298–318. [CrossRef]

Gibson, James J. 1979. *The Ecological Approach to Visual Perception*. Boston: Houghton Mifflin.

Grandhi, Sukeshini A., Linda Plotnick, and Starr Roxanne Hiltz. 2021. By the crowd and for the crowd: Perceived utility and willingness to contribute to trustworthiness indicators on social media. *Proceedings of the ACM on Human-Computer Interaction* 5: 218. [CrossRef]

Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The dark (patterns) side of UX design. Paper presented at the 2018 CHI Conference on Human Factors in Computing Systems, Montréal, QC, Canada, April 21–26; pp. 1–14. [CrossRef]

Hajli, Nick, and Xiaolin Lin. 2016. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics* 133: 111–23. [CrossRef]

Hansen, Jared M., George Saridakis, and Vladlena Benson. 2018. Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior* 80: 197–206. [CrossRef]

Hayes, Andrew F. 2022. Introduction to mediation, moderation, and conditional process analysis. In *A Regression-Based Approach*, 3rd ed. New York: Guilford Press.

Kang, Hyunjin, Jeeyun Oh, Tingting Yang, Eunjoo Jin, and Nazira Banu. 2026. Emotional responses to privacy invasion on algorithmic social media: Insights from in-depth interviews linking agency, emotions, and privacy. *Information, Communication & Society*, 1–20. [CrossRef]

Keeton, Courtney Pierce, Maureen Perry-Jenkins, and Aline G. Sayer. 2008. Sense of control predicts depressive and anxious symptoms across the transition to parenthood. *Journal of Family Psychology* 22: 212–21. [CrossRef] [PubMed]

Kelton, Maryanne, Michael Sullivan, Zac Rogers, Emily Bienvenue, and Sian Troath. 2022. Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs* 98: 1977–99. [CrossRef]

Kemp, Simon. 2025. *Digital 2025: Saudi Arabia*. DataReportal. Available online: https://datareportal.com/reports/digital-2025-saudi-arabia (accessed on 22 February 2026).

Koohang, Alex, Kevin Floyd, Johnathan Yerby, and Joanna Paliszkiewicz. 2021. Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. *Issues in Information Systems* 22: 133–49. [CrossRef]

Krasnova, Hanna, Elena Kolesnikova, and Oliver Guenther. 2010. Leveraging trust and privacy concerns in online social networks: An empirical study. Paper presented at the 18th European Conference on Information Systems (ECIS 2010), Pretoria, South Africa, June 7–9; p. 160.

Kuan, Jennifer, and Gwendolyn Lee. 2023. Governance strategy for digital platforms: Differentiation through information privacy. *Strategic Management Review* 4: 161–91. [CrossRef]

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15: 336–55. [CrossRef]

Marteau, Theresa M., and Hilary Bekker. 1992. The development of a six-item short-form of the state scale of the Spielberger State-Trait Anxiety Inventory (STAI). *British Journal of Clinical Psychology* 31: 301–6. [CrossRef] [PubMed]

Masur, Philipp K. 2018. *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Berlin: Springer. [CrossRef]

Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction* 3: 1–32. [CrossRef]

Mayer, Roger C., James H. Davis, and F. David Schoorman. 1995. An integrative model of organizational trust. *Academy of Management Review* 20: 709–34. [CrossRef]

McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research* 13: 334–59. [CrossRef]

Mueller, Milton L. 2020. Against sovereignty in cyberspace. *International Studies Review* 22: 779–801. [CrossRef]

Norman, Don A. 2013. *The Design of Everyday Things*. Cambridge: The MIT Press.

Paliszkiewicz, Joanna, and Alex Koohang. 2016. *Social Media and Trust: A Multinational Study of University Students*. Santa Rosa: Informing Science Press.

Peng, Lulu, Jinping Wang, Nanxiao Zheng, and Xiaoping Guo. 2024. Traversing emotional spaces: Social media affordances and emotion regulation in times of physical isolation. *Social Media+ Society* 10: 20563051241237273. [CrossRef]

Pisani, Giacomo. 2024. The right to self-determination in the digital platform economy. *Computer Law & Security Review* 53: 105964. [CrossRef]

Pohle, Julia, and Thorsten Thiel. 2020. Digital sovereignty. *Internet Policy Review* 9. [CrossRef]

Saudi Data and Artificial Intelligence Authority (SDAIA). 2021. Personal Data Protection Law. Available online: https://sdaia.gov.sa/en/Research/Pages/DataProtection.aspx (accessed on 2 September 2026).

Schaub, Florian, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. Paper presented at the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), Ottawa, ON, Canada, July 22–24; pp. 1–17.

Shulman, Yefim, and Joachim Meyer. 2022. Degrees of perceived control over personal information: Effects of information relevance and levels of processing. *IEEE Access* 10: 40596–608. [CrossRef]

Smith, H. Jeff, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35: 989–27. [CrossRef]

Srnicek, Nick. 2017. *Platform Capitalism*. Cambridge: Polity Press.

Stach, Christoph, and Bernhard Mitschang. 2014. Design and implementation of the privacy management platform. Paper presented at the 2014 IEEE 15th International Conference on Mobile Data Management, Brisbane, QLD, Australia, July 14–18. [CrossRef]

Tan, Kheng Leong, Chi-Hung Chi, and Kwok-Yan Lam. 2023. Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys* 56: 1–36. [CrossRef]

Törnberg, Petter. 2023. How platforms govern: Social regulation in digital capitalism. *Big Data & Society* 10: 1–13. [CrossRef]
Treem, Jeffrey W., and Paul M. Leonardi. 2013. Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Annals of the International Communication Association* 36: 143–89. [CrossRef]
Trepte, Sabine. 2021. The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory* 31: 549–70. [CrossRef]
van Dijck, José, Thomas Poell, and Martijn de Waal. 2018. *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press. [CrossRef]
Van Ooijen, I., and Helena U. Vrabec. 2019. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy* 42: 91–107. [CrossRef]
Wang, Chong, Nan Zhang, and Cong Wang. 2021. Managing privacy in the digital economy. *Fundamental Research* 1: 543–51. [CrossRef]
Wang, Jia, Qianqian Cao, and Xiaogang Zhu. 2025. Privacy disclosure on social media: The role of platform features, group effects, trust and privacy concern. *Library Hi Tech* 43: 1035–59. [CrossRef]
Westin, Alan F. 1967. *Privacy and Freedom*. Berlin: Atheneum.
Xiao, Yineng. 2025. Transparency and privacy on social media: Privacy policies for enhancing users' control on social media. *International Journal of Human–Computer Interaction* 41: 14228–47. [CrossRef]
Xu, Heng, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12: 798–824. [CrossRef]
Xu, Yan, and Linmin Chen. 2025. Personalized recommendations and consumer trust: The role of perceived control and locus of control. *Acta Psychologica* 261: 105936. [CrossRef]
Zhang, Zhiyong, and Brij B. Gupta. 2018. Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems* 86: 914–25. [CrossRef]
Zhuang, Lei, Rui Sun, Lijun Chen, and Wenlong Tang. 2023. The impact of shared information presentation time on users' privacy-regulation behavior in the context of vertical privacy: A moderated mediation model. *Behavioral Sciences* 13: 706. [CrossRef] [PubMed]
Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Singapore: PublicAffairs.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.