Privacy Rights, Inference, and User Trust in Digital Platform Services

Adebayo Oluwatosin

Obafemi Awolowo University, Nigeria

ARTICLE INFO

Article history:
Received 6 December 2023
Revised 10 January 2024
Accepted 19 February 2024

Key words:
Privacy,
Data security,
Consent,
Profiling,
Data retention,
Trust,
User behavior.

ABSTRACT

Digital services increasingly translate everyday actions into durable data traces that are collected, linked, and interpreted at scale. This literature-based study clarifies how privacy is redefined when personal information is generated continuously through platforms, devices, and connected infrastructures. Privacy is treated as a set of rights and practical conditions: intelligible notice, meaningful consent, limitation of processing purposes, proportional retention, and accountability for automated inferences. The discussion shows that security and privacy are experienced together by users, because breach narratives, authentication frictions, interface defaults, and recovery procedures shape trust and sharing decisions. Individuals negotiate boundaries through selective disclosure, identity separation, permission management, and post-incident adaptations, yet these practices remain vulnerable to inference, aggregation, and third-party data flows. The study synthesizes conceptual arguments on relational privacy, the temporal problem of persistent records, and the epistemic reach of profiling, then connects them to everyday behavioral trade-offs between convenience and self-protection. It concludes that sustainable protection requires aligning system design with human decision limits, reducing hidden secondary uses, and providing usable mechanisms to review, withdraw, and audit data practices. The article contributes an integrated conceptual map that can guide policy drafting, organizational governance, and privacy-respecting product design. Across sectors such as finance, health, education, and employment, these dynamics raise questions of fairness, autonomy, and due process. By articulating boundary principles and behavioral pathways, the study supports more precise evaluation of digital data practices in real-world use.

INTRODUCTION

The pace of digitization places data as a trail that continues to be formed from the simplest activities to sensitive decisions. When someone communicates, transacts, works, studies, or accesses public services, that series of actions produces records that can be identified, matched, and concluded. Privacy can no longer be understood simply as a state of "invisibility," but rather as the right to determine how information about oneself is formed, used, disseminated, and interpreted. At the same time, data security is not merely a technical issue, as incidents of leaks, misuse of access, and identity manipulation touch on the integrity of personal dignity. In the digital space, the boundary between public and private is easily shifted through platform design, sharing habits, and consent procedures that are often skimmed over. How society interprets openness, security, and control over oneself ultimately becomes a matter of knowledge, ethics, and governance, not merely a matter of devices (Verhulst, 2022).

The development of platform-based services shows that privacy is often negotiated for convenience. People tend to trade some control over their data for quick access, personalization, discounts, or a smooth user experience. The study by Gardi and Eddine (2023) shows that the dynamics of this exchange are inextricably linked to complex cybersecurity and personal data protection challenges, which require global collaboration. These choices are rarely made through balanced consideration, because information architecture often directs attention to short-term benefits while obscuring long-term costs. Data processing consent is usually presented as a formality, while the consequences of data aggregation are difficult for ordinary users to imagine. At the social

* *Corresponding author, email address:* ***adebayo.oluwatosin@gmail.com***

level, the habit of sharing location, photos, purchase history, and political preferences is slowly becoming the new norm (Meier, 2023). As norms shift, privacy can be seen as an uncooperative attitude, when what is at stake is personal autonomy. This shift in meaning shapes how individuals understand themselves in relation to digital systems: whether they are sovereign subjects or objects that are constantly being evaluated.

Modern computing technology expands data processing capabilities through cross-device tracking, predictive analytics, and behavioral modeling. Seemingly trivial data, such as typing patterns, walking speed, or active hours, can be used to guess health conditions, stress levels, social relationships, and even ideological preferences. When inference becomes possible, the boundaries of "sensitive" data become blurred, because sensitivity arises from combinations, not from a single element. At this point, privacy is closely related to security: the more data is collected, the greater its economic value, and the greater its appeal to malicious parties (Parrilli & Hernández-Ramírez, 2021). Leaks do not always occur through hacking; they can arise from procedural negligence, configuration errors, or abused internal access. Individuals then face the reality that risks are not always visible, but their consequences can be long-lasting.

In hermeneutic readings of user experiences, privacy often manifests as a sense of being "monitored" that is difficult to prove, while data security manifests as a sense of "vulnerability" that is often only recognized after an incident has occurred. Users interpret signs, such as advertisements that seem too accurate, recommendations that seem to know their secrets, or verification messages that arrive unsolicited. This interpretation shapes behavior: some become more cautious, some choose to resign themselves, and some seek technical solutions that are not always fully understood (Schoenherr, 2022). Here, it appears that technology is not merely a tool, but a medium that reconfigures the relationship between the self, others, and institutions. This change requires a discussion that balances normative and empirical aspects: what should happen according to principles of rights, and what actually happens in everyday practice. This is where a literature review is needed to formulate a map of ideas, terms, and debates that can be accounted for.

At a more specific level, attention is focused on how system design and platform culture shape the concept of privacy and guide individual actions. The concept of privacy becomes layered: there is privacy as control, privacy as access restriction, privacy as confidentiality, and privacy as protection from unfair judgment. Each layer raises different security measures, ranging from encryption and authentication to access management and processing accountability (Benjamin, 2017). Individual behavior is then shaped by a combination of beliefs, digital literacy, past negative experiences, and social pressure to stay connected. Many people are aware of the risks but continue the same practices because the cost of change is considered too high. In such situations, the term "consent" has the potential to become a symbol of administrative compliance rather than a conscious choice. A thorough literature review is therefore needed to organize concepts, explain mechanisms, and assess the ethical implications that accompany the shift in privacy in the digital age.

The main problem arises when individuals' understanding of privacy is not in line with how data is processed in digital systems. Users often think that privacy is ensured when they set their accounts to private or choose not to publish certain information. Data processing, however, goes much further: it involves the collection of metadata, third-party tracking, database merging, and storage that exceeds expectations. The findings of Negara et al. (2022) on privacy violations on social media and their impact on interpersonal trust among young people, for example, confirm that the mismatch between privacy expectations and system practices can undermine social foundations. This misalignment creates a knowledge gap that makes it difficult for individuals to assess risks, make decisions, and demand accountability. At a conceptual level, privacy is a shared term, but its meaning differs between users, service providers, and regulators. These differences in meaning cause normative confusion: privacy violations are considered ethical violations by some, but are considered normal business practices by others. As a result, the protection promised through policy is often not perceived as protection.

The next issue relates to data security as a fragile prerequisite for trust. Secure systems require layered risk management, but practices in the field often reveal a reliance on weak passwords, credential reuse, link-clicking habits, and shared device use. On the other hand, institutions that manage data can face cost pressures, limited human resources, and business priorities that override security improvements. Studies on regulatory effectiveness, such as that conducted by Aziz et al. (2023) in Indonesia's fintech sector, reveal a gap between ideal legal norms and implementation in the field, particularly in creating a secure and accountable system. When incidents occur, individuals bear the burden of recovery: replacing digital identities, dealing with fraud, or restoring reputations. This burden highlights the imbalance

between those who benefit from data collection and those who bear the risk when protection fails. Security issues also intersect with behavior, as overly complex procedures lead people to look for shortcuts, while overly lax procedures open the door to abuse. Without a clear understanding of the relationship between privacy and security, policies can easily become reactive and fragmented.

An examination of data privacy and security is necessary today because digital devices and services have become part of our daily infrastructure. Decisions that were once personal are now recorded as data that can be reprocessed beyond its original purpose. When data forms a profile, that profile can influence access to opportunities, services, and institutional treatment. Individuals may experience automated assessments that are difficult to understand, for example in job selection, credit offers, or content filtering. Therefore, literature such as Baraja et al. (2023) study on the implementation and supervision of the Personal Data Protection Act on online platforms is important for understanding the mechanisms needed for the legal framework to effectively regulate the complex digital ecosystem and prevent injustice. This situation places privacy as an issue of information justice, while data security becomes a requirement so that data-based social processes do not harm the most vulnerable parties. The changing habits of communication also shift the boundaries of social agreements: what is considered reasonable to share, who has the right to know, and when information can be remembered. A literature review allows the author to systematically trace these conceptual changes, showing how terms have evolved and how ethical and legal frameworks have attempted to adapt.

This topic is also important because individual behavior is often shaped by subtle design choices, rather than conscious decisions. Interfaces can encourage openness through share buttons, permissive default settings, or narratives that personalization is synonymous with convenience. At the same time, security is often treated as an afterthought, only addressed when a breach occurs. This pattern results in a culture that normalizes privacy sacrifices and downplays security discipline. This normalization can change how individuals see themselves in the long run: as users who always have to adjust to the system, not as rights holders who can set boundaries. By examining the literature, studies can formulate the relationship between technology, the concept of privacy, and emerging behaviors, so that the discussion does not stop at a list of risks. It can describe how user experiences are understood, how trust is formed or broken, and how digital spaces are reshaping the relationship between freedom, surveillance, and responsibility.

This literature-based study aims to develop a structured conceptual understanding of data privacy and security in the digital age by examining how technology has shifted the definition of privacy from the idea of confidentiality to issues of control, inference, and governance of personal information processing. This research is directed at formulating a theoretical link between system architecture, data collection and aggregation practices, and how individuals interpret their sense of security or surveillance when using digital services. In the theoretical realm, this paper aims to clarify key terms, bring together various definitional approaches, and map the relationship between privacy as a right and security as a prerequisite for protection. In the practical realm, this paper is expected to provide a foundation for the development of digital literacy guidelines, organizational policy design, and service design principles that respect user choices, so that data management is more accountable, proportional, and justifiable.

RESEARCH METHOD

This research uses qualitative literature study with a thematic synthesis orientation to organize, compare, and interpret conceptual findings regarding privacy, data security, and individual behavior in the digital space. The process is aimed at producing a coherent understanding of the shifting meaning of privacy, the relationship between technical mechanisms and social consequences, and the forms of user rationality when dealing with data collection and processing. The synthesis was conducted through critical and interpretive reading of scientific texts, with attention to the terms, assumptions, and operational definitions used by the authors. A systematic review framework was used as a procedural guideline so that the search, selection, and reporting could be retraced, while still allowing room for conceptual analysis that is common in qualitative studies. This approach follows the principles of transparency and traceability recommended in the guidelines for reporting systematic reviews and meta-syntheses (Abid, 2023).

The search strategy was designed in stages: formulation of core keywords and synonyms, combination of Boolean operators, and adjustment of terms according to discipline clusters, such as law, information systems, cybersecurity, and technology ethics. Primary sources include journal articles, proceedings, academic books, and research reports with scientific credibility. Inclusion criteria cover works that explicitly discuss digital privacy and data

security, explain the conceptualization of privacy, describe data processing mechanisms or security risks, and link the discussion to individual behavior or user decisions. Exclusion criteria include popular writings without clear methodology, manuscripts that do not present literature-based arguments, and publications that only contain technical descriptions without relevance to the concepts of privacy or behavior. To maintain consistency, the selection process was carried out by screening titles and abstracts, followed by reading the full text, then recording the reasons for inclusion or exclusion at each stage, as recommended in the guidelines for conducting systematic reviews.

Coding was carried out through a combination of deductive and inductive strategies. Deductively, the initial codes were compiled from categories commonly found in privacy and data security studies, such as information control, consent, tracking, identity, leakage, misuse of access, and trust. Inductively, new codes were added when patterns of argumentation or recurring terms emerged that were not yet covered in the initial codes. The codes are then grouped into themes, and each theme is tested through cross-source comparison to examine consistency, differences, and limitations of application. Quality assurance is carried out through an audit trail in the form of analytical decision records, re-examination of the accuracy of quotations from the original sources, and researcher reflexivity in assessing assumptions made when interpreting the text. The validity of the synthesis is maintained by seeking contradictory evidence, assessing the weight of arguments, and marking areas that are still debated in the literature, in accordance with the principles of qualitative meta-synthesis.

RESULT AND DISCUSSION

Reconstructing the Concept of Privacy in the Digital Technology Ecosystem

Privacy in the digital ecosystem has shifted from the classic understanding of a closed space to one that emphasizes control, process transparency, and restrictions on the use of personal information. When human activities are mediated by platforms, privacy no longer depends on the act of hiding oneself, but rather on the ability to regulate the flow of data that is generated every time someone types, searches, likes, watches, or moves around (Xu & Zhang, 2023). In this order, privacy becomes a relationship between the subject and the system that stores, processes, and links information on a large scale. This relationship is asymmetrical because individuals often face complex procedures, while organizations have analytical tools and the ability to combine data across services. This shift demands a more operational definition of privacy, namely as the right to know what is collected, for what purpose, how long it is stored, with whom it is shared, and how automated decisions are made from the data. Without an operational definition, privacy is easily reduced to a personal preference, when in fact it is directly related to dignity and autonomy.

The reconstruction of the concept of privacy must begin with the understanding that digital data rarely stands alone. Personal information is formed through the aggregation of traces, correlations, and inferences, so that something that initially appears neutral can become a marker of identity or private circumstances when combined with other sources (Inverardi et al., 2023). Privacy is therefore inadequate when understood as protection of predefined "sensitive data." Sensitivity can arise from relationships between variables, such as active time patterns related to work rhythms, locations that indicate beliefs, or shopping preferences that point to health status. A more appropriate concept of privacy must acknowledge this inferential logic: threats to privacy do not always take the form of direct leaks, but rather the formation of new knowledge about a person without their informed consent. When inference becomes a routine part of digital services, privacy becomes a matter of epistemic boundaries, namely the limits of what systems should know about individuals.

In the digital space, privacy is also related to visibility, which is determined by design. Default settings, notifications, and menu layouts can encourage users to grant broader access than they realize. In many services, privacy-preserving options are buried in hard-to-find layers, while sharing options are presented as normal and quick actions. This situation makes privacy dependent on navigation skills, reading patience, and uneven literacy. Arifin and Darmawan (2021) in their study on technology access and digital literacy emphasize that this gap is not only technical, but structural, which also shapes individuals' ability to negotiate privacy. As a result, privacy is not merely a free choice, but rather the result of an interaction between the user's intentions and the structure of the options provided (Vasalou et al., 2015). The reconstruction of the concept of privacy needs to include the dimension of choice design as a normative element: a choice is considered valid if it is understandable, can be rejected without disproportionate penalties, and is not obscured by ambiguous language. Without these principles, consent can become an administrative formality, while real control remains with the service provider.

Privacy as control is often understood individually, but in the digital ecosystem, that control

has limits because a person's data often contains information about other people. Group photos, contact lists, conversations, and recordings of shared activities can link the identities of many parties at once (Falgoust, 2016). In this situation, privacy is relational: one person's decision to upload or grant access can affect others who were not present in the consent process. The reconstruction of the concept of privacy must recognize that the subject of privacy is not a single individual, but a network of relationships recorded in data. Consequently, the measure of "privacy rights" cannot be based solely on individual preferences, but must also take into account the moral obligation not to expose others through seemingly trivial sharing practices. Al Hakim et al. (2021) in their analysis of cultural value transformation in the digital age show that continuous sharing and documentation practices have changed social norms regarding personal and public boundaries. When the relational dimension is ignored, the digital space encourages a culture of continuous documentation, while those who are documented lose the opportunity to determine how they are presented and interpreted.

The shift in the concept of privacy is also evident in the emergence of identity as a data construct. Digital identity is not just an account name, but a set of attributes, scores, and categories compiled from daily interactions (Tikk, 2017). When these categories are used to predict actions or preferences, individuals can be treated based on statistical assumptions rather than fair recognition. At this point, privacy is related to protection from classifications that reduce human complexity to labels. The reconstruction of the concept of privacy needs to include the right not to be excessively profiled, the right to know the basis for profiling, and the right to correct or reject harmful inferences. This is not merely an issue of convenience, but one of procedural justice. A person can lose access, opportunities, or reputation due to incorrect profiling, while the profiling process is often opaque and difficult to challenge.

The relationship between privacy and time also needs to be redefined. In analog experiences, much information is ephemeral: conversations pass, mistakes are forgotten, and social traces fade. In the digital space, cheap storage and automatic archiving make the past easily retrievable. Privacy is therefore linked to the right to be socially forgotten, or at least the right to limit the retention of data that is no longer relevant. Long retention increases the chances of leaks and misuse, but also strengthens the power of institutions to judge individuals based on old records (Jørgensen, 2016). The reconstruction of the concept of privacy needs to place retention as an ethical variable: storage must be proportional to the purpose, and deletion must be a real procedure, not just a promise. Privacy thus includes a temporal dimension, namely control over when information stops circulating and stops being used as a basis for assessment.

Privacy is also related to space, because digital devices bring location tracking to a very detailed level. When location becomes routine data, the boundary between private and public space weakens. People may feel they are in a personal space, but devices transform it into coordinates that can be analyzed, mapped, and compared. The reconstruction of the concept of privacy needs to treat location as data that has the potential to reveal patterns of life, relationships, and habits that are never directly stated. Protecting location privacy is not enough through the "turn off GPS" option, because tracking can take place through networks, sensors, or other signals. A stronger definition of privacy therefore requires restrictions on the collection and accuracy of location data according to service needs. With this principle of proportionality, privacy is not understood as a rejection of technology, but as a reasonable regulation of what the system needs to know.

Within the platform system, privacy is often exchanged for personalization. The personalization of services is claimed to increase convenience, but personalization requires extensive and continuous data. The reconstruction of the concept of privacy needs to test the assumption that personalization always has positive value. Personalization can lead to a narrowing of the information experience, the reinforcement of certain habits, or highly targeted consumption incentives. When personalization works through prediction, individuals can be subtly guided without feeling guided. Therefore, privacy is related to cognitive freedom, namely the freedom to form preferences without overly precise intervention. A definition of privacy that includes cognitive freedom will assess the extent to which the system respects the user's ability to choose, not just accept recommendations. In this framework, privacy is a prerequisite for freedom of expression and freedom to determine identity, because exposure curated by profiles can limit a person's horizon of choice.

The reconstructed concept of privacy must also examine the language of policy and consent practices. Many privacy policies are drafted as lengthy legal documents, making them difficult to understand as ethical communication. When language becomes a barrier, consent loses its substantive meaning. Reconstructing the concept of privacy requires reasonable communication standards: concise explanations, examples of data use, policy change

indicators, and equal choices between accepting or rejecting. Negara and Darmawan (2023) in a study on digital empowerment and legal protection emphasize that a clear and accessible legal framework is the foundation for transforming consent from a formality into an informed choice. Meaningful consent also requires the absence of covert coercion, such as refusal that renders the service completely unusable even though certain processing is not essential. Privacy thus becomes a governance practice, not just a statement. It requires mechanisms that allow users to review permissions, withdraw permissions, and see the consequences of withdrawal without the threat of disproportionate loss of access.

Ultimately, reconstructing the concept of privacy requires a bridge between normative rights and user experience. Privacy rights are often expressed as fundamental or legal rights, but users experience them as a sense of security, trust, or freedom to act without surveillance. When rights are understood only at the level of documents, while experience shows powerlessness, a gap occurs that destroys trust. An appropriate concept of privacy must therefore include three elements: control over data flows, transparency of processing, and accountability in the event of violations. The element of control gives users the capacity to choose; the element of transparency gives users the ability to assess; the element of accountability provides assurance that violations are not normalized. These three elements redefine privacy from a mere moral claim to a relational structure that can be tested in practice, while also serving as a basis for assessing whether the digital ecosystem respects human autonomy.

An analytical summary of this discussion shows that digital technology reshapes privacy through data aggregation, inferential logic, choice design, recorded social relations, and long-term retention that changes the nature of social memory. Privacy, which was originally easily understood as confidentiality, has become a right that demands control, readability, and restrictions on the purpose of processing, including restrictions on profiles formed from behavioral traces. These changes also show that privacy touches on the dimensions of space and time, because location and digital archives can reveal patterns of life that were previously difficult to trace. At the normative level, consent needs to be interpreted as an action that is understood, can be withdrawn, and is not obscured by language that obscures the consequences. At the experiential level, privacy is present as a measure of freedom of action and freedom to form preferences without overly precise intervention. This entire description emphasizes that the reconstruction of the concept of privacy needs to be placed as a framework that can be used to read everyday data processing practices, before moving on to discussions about data security and individual behavior.

Data Security and Individual Behavior in Negotiating Digital Privacy Boundaries

Data security shapes how individuals assess whether digital spaces are trustworthy, because a sense of security stems from the belief that personal information cannot be easily accessed, altered, or used without authorization. In everyday use, individuals rarely separate security as a technical issue and privacy as a value issue. The two are integrated into practical decisions, such as choosing an application for communication, storing identity documents, or linking accounts across services. When reports of leaks are common, individuals interpret that every online activity carries a risk, even though the source of the risk is not always clear (Pascalev, 2017). This assessment influences sharing habits: some people reduce their profile details, limit uploads, or use alternative accounts, while others maintain their old habits because they feel that change does not provide certainty. Here, it appears that data security does not function as a tangible guarantee, but rather as a prerequisite that is silently assessed through cues. These cues can take the form of multi-layered verification, account activity notifications, or transparency of settings, all of which influence decisions to disclose or withhold information.

Weak security conditions shape adaptive behaviors that are often reactive in nature. Individuals typically change their habits after experiencing account takeover, fraud, or witnessing the loss of someone close to them. Before an incident, threats are understood as something distant, whereas after an incident, threats become concrete and personal. Behavioral changes can take the form of changing passwords, activating two-factor authentication, deleting certain applications, or tightening sharing settings (Kovanic & Spáč, 2022). These adaptations are often hampered by cognitive load, however. An analysis of inclusivity in technology-based services by Ramle and Mardikaningsih (2022) emphasizes that the digital skills gap can increase vulnerability, whereby those with lower literacy levels face a higher cognitive load in managing security, making them more prone to taking risky shortcuts. Many people have to manage dozens of accounts, deal with repeated permission requests, and make quick decisions under time pressure. Security is then negotiated as a compromise between digital order and convenience. When security procedures are considered too

cumbersome, individuals tend to look for shortcuts, such as using similar password patterns, storing credentials in unprotected notes, or ignoring updates. This pattern shows that safe behavior requires designs that are aligned with human capabilities, not just normative instructions.

Privacy negotiations often occur at the intersection between security mechanisms and user experience (Serrano-Tellería, 2018). When platforms provide detailed but difficult-to-understand settings, users feel they have illusory control. They can close their profiles to the public, but still do not understand how data is used for internal assessment or behavior modeling. This lack of understanding encourages two extreme patterns: hypervigilance or resignation. Hypervigilance can result in strict settings, but is sometimes accompanied by excessive suspicion of every permission request. Resignation arises when individuals feel they have no realistic choice but to follow the terms of service. Both patterns create unstable privacy boundaries. These boundaries change according to experience, needs, and social pressure. In practice, users often make heuristic-based decisions, such as trusting big brands, trusting apps that their friends use, or trusting apps that appear professional. Such heuristics fill information gaps, but can be misguided when appearance is trusted over an evaluation of actual security procedures.

Data security also influences sharing behavior by creating a sense of risk associated with identity. Threats such as identity theft, account takeover, or profile spoofing make people realize that basic information, such as phone numbers, birth dates, or photos, can be a gateway for attacks (Díaz Ferreyra et al., 2020). This awareness influences decisions about what is considered appropriate to share. Some individuals begin to separate their identities: one identity for professional matters, one identity for social networking, one identity for transactions, and one identity for exploration. This separation aims to reduce cross-activity links, so that if one account is compromised, other accounts are not exposed. Separation of identities requires high discipline and can cause social tension because it is considered inauthentic. On a psychological level, individuals try to balance the need to be socially accepted with the need to protect themselves. Privacy boundaries are therefore the result of both social and security considerations, where feelings of vulnerability can reinforce the decision to limit information, while the need for recognition can encourage repeated openness.

Security habits are often determined by narrative understanding, rather than technical understanding. Individuals learn from stories, such as stories about accounts being hacked after clicking on a link, or stories about data leaks leading to fraud. Stories shape mental maps of what is dangerous and what is safe. This map then guides actions such as checking sender addresses, rejecting verification code requests, or avoiding public networks. Mental maps can also produce a false sense of security, such as the belief that using expensive devices automatically means safety, or the belief that deleting uploads means the data is completely gone. As a result, individuals' behavior may appear consistent, but it is based on false assumptions. Negotiating privacy boundaries here takes place through the interpretation of signs: login notifications, application permission requests, service messages, and overly precise recommendations. When signs are understood as threats, user close access. When signs are understood as normal, users open access. Data security thus functions as a language that is interpreted on a daily basis (Nadon et al., 2018).

Trust in digital institutions is shaped by service experiences and beliefs about accountability (Prettyman et al., 2015), where clear response mechanisms such as account recovery support and complaint procedures form the foundation of perceptions of security and fairness that shape user behavior (Anugroh et al., 2023). However, this trust is also shaped through design signals such as default settings, which guide privacy behavior norms. Furthermore, security practices are strongly influenced by relational norms and social routines (Abdelaziz et al., 2019), such as sharing devices or passwords within families and friendships, where privacy boundaries are negotiated in the context of power and trust relationships between individuals. Thus, security behavior is not merely a personal choice, but a response to the incentive structures of platforms and collective norms that define what is "appropriate" in sharing access in digital spaces.

Data security becomes more complex when individuals use interconnected service ecosystems. A single account can serve as a gateway to other services through single sign-on, device synchronization, or payment integration. This interconnectedness increases convenience, but also magnifies the consequences when a single point of access is compromised. The convenience and practicality offered by this integration, as examined by Kemarauwana and Darmawan (2020) regarding the contribution of perceived ease of use to behavioral intentions in digital payments, is a major driving factor for users to remain connected to various services, even though they are aware of the risks involved. The study shows that pragmatic considerations often dominate over formal security

calculations. Individuals respond to this situation with a variety of strategies. Some focus security on one main account with layered verification, some split accounts so they are not interconnected, and some leave security to password managers. Each strategy requires different knowledge and discipline. When knowledge is low, strategies tend to rely on habits, such as using the same email address for all services. This dependence makes privacy boundaries easy to breach through identity correlation. Negotiating privacy boundaries in a connected ecosystem means determining where connections between services need to be severed, what data needs to be synchronized, and what features should be disabled even if it reduces convenience (Watson et al., 2020). These decisions are rarely based on formal calculations, but rather on pragmatic trade-offs.

Security incidents change behavior through a sense of loss of control. When data is leaked, individuals face the reality that events are beyond their personal control. This can lead to recovery actions such as changing all passwords, freezing payment services, or monitoring account activity. Recovery also leads to fatigue, as these actions are time-consuming and require ongoing attention. In the long term, fatigue can lead to desensitization, a state in which people consider leaks to be normal. Desensitization weakens privacy boundaries because individuals stop believing that small actions yield results. At this stage, sharing behavior may increase again because a sense of futility encourages permissive attitudes. Data security thus influences behavior through two potentially contradictory phases: the post-incident vigilance phase and the risk normalization phase. The negotiation of privacy boundaries is not linear; it moves in rhythm with experience, news, and the perceived burden of recovery. To understand individual behavior, it is necessary to examine how people rebuild trust after losing control.

Security literacy influences how individuals interpret signs and manage choices. Literacy is not merely knowledge of terminology, but rather the ability to connect actions with consequences. Individuals who understand how attacks work tend to be more consistent in their safe habits, such as being wary of social engineering, checking connected devices, and managing app permissions. Literacy itself, however, can breed overconfidence, leading users to feel invulnerable and become careless. Alternatively, individuals who lack understanding may become overly cautious, but in inefficient ways, such as avoiding certain features while neglecting more important actions like system updates. Negotiating privacy boundaries involves the ability to distinguish between real and imagined risks. When imagined risks are perceived as greater, users reduce their digital participation and lose out on the benefits of services. When real risks are underestimated, users open up broad access without protection (Zou et al., 2018).

Security technologies such as encryption, multi-factor authentication, and permission controls can influence behavior through a sense of "protection" (Brough & Martin, 2020). This sense of protection is beneficial, but it can trigger moral hazard in the form of bolder actions. For example, someone feels safe because they use multi-factor authentication, so they log in more often from other people's devices or ignore application warnings. Security measures that interrupt too often can cause annoyance, leading users to disable features or permanently select the "remember me" option. This pattern shows a relationship between user experience and security discipline. Privacy boundary negotiations occur at the moment of interruption: when the system requests access to the camera, microphone, location, or contacts, users weigh the immediate benefits and unseen risks. Because this weighing often takes place quickly, users tend to follow the path of least resistance. A responsible and equitable approach to technology development, as discussed by Radjawane and Mardikaningsih (2022), emphasizes that technology should be designed to empower users with clear and fair choices, rather than trapping them in risky usage patterns for commercial gain. The form of interaction, clarity of explanation, and equal choices become factors that shape habits. In this framework, security cannot be separated from decision ergonomics.

This discussion shows that privacy boundaries are negotiated in complex interactions between social norms, cognitive load, incident experiences, and trust in institutions. Strong sharing norms, as studied by Infante and Mardikaningsih (2022), create social pressure to be open, while individuals respond with improvised information filtering techniques. Ultimately, privacy boundaries are not fixed lines, but rather the result of daily pragmatic decisions that balance comfort, risk, and interpretation of digital signals. Sustainable security practices depend on decision governance and user experiences that enable choices that are easy to understand and implement in the rhythm of digital life.

CONCLUSION

This literature review confirms that privacy in the digital age is no longer adequate when understood as mere confidentiality or the option to withhold information. Privacy has evolved into a right and practical condition that demands control over data

flow, clarity of processing purposes, retention restrictions, and accountability for automated inferences that shape new knowledge about individuals. In everyday use of services, privacy and data security exist as a mutually reinforcing experience: a sense of security arises when users see understandable protection signs, while a sense of vulnerability intensifies when leaks, slow recovery, or confusing settings occur. Individual behavior is shaped by repeated negotiations between the need for convenience and the need for self-protection, including information filtering, identity separation, and application permission management. These negotiations are often limited by cross-service aggregation, profiling, and third-party data flows that are difficult to see. Sustainable protection therefore requires alignment between system design and human decision boundaries.

The conceptual findings in this paper have implications for three areas. In the policy domain, privacy protection needs to be expressed in understandable language, with testable indicators, such as limits on processing purposes, retention periods, and procedures for withdrawing consent. In the realm of organizational governance, data security needs to be treated as a discipline inherent in the entire data lifecycle, from collection to deletion, accompanied by access logging and consistent internal audit mechanisms. In the realm of product design, user privacy decisions should be supported by equivalent choices, careful default settings, and concise explanations linking permissions to possible consequences. For digital literacy, the focus of learning needs to shift from a list of prohibitions to the ability to assess situation-based risks, such as understanding social engineering, cross-account identity correlations, and the meaning of long data retention. Overall, these implications help to position privacy as a condition of freedom of action and security as a prerequisite for restorable trust.

Further literature-based research can deepen the mapping of consent typologies that users truly understand, including variations in communication, transaction, education, and health services, as well as how the form of consent affects sharing behavior. It is also necessary to refine the concept of relational privacy so that protection does not stop at the individual who gives permission, but also includes other parties who are recorded in the data. For practical development, data management organizations should develop easy-to-use mechanisms for reviewing permissions, revoking permissions, and viewing access history at a glance, as these steps reduce the cognitive load on users. Service developers are advised to test default settings and permission flows with comprehensibility tests, so that safer options are not hidden. For educators and digital literacy module developers, materials should emphasize realistic habits such as multi-factor authentication, separating accounts for different needs, being wary of messages requesting codes, and checking devices that are logged in.

REFERENCES

Abdelaziz, Y., Napoli, D., & Chiasson, S. (2019). End-Users and Service Providers: Trust and Distributed Responsibility for Account Security. In *International Conference on Privacy, Security and Trust*, 1-6.

Abid, N. (2023). A Review of Theories Utilized in Understanding Online Information Privacy Perceptions. In *Computer Science On-line Conference, Charm: Springer International Publishing*, 54-67.

Al Hakim, Y. R., Rojak, J. A., & Triono, B. (2021). Transformation of Cultural Values and Social Practices in the Digital Age. *Journal of Social Science Studies*, 1(1), 173-178.

Anugroh, Y. G., Hardyansah, R., Darmawan, D., Khayru, R. K., & Putra, A. R. (2023). Consumer Protection and Responsibilities of E-commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions. *Journal of Social Science Studies*, 3(2), 89-94.

Arifin, S., & Darmawan, D. (2021). Technology Access and Digital Skills: Bridging the Gaps in Education and Employment Opportunities in the Age of Technology 4.0. *Journal of Social Science Studies*, 1(1), 163-168.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, 3(1), 23-28.

Baraja, M. U., Saputra, R., Saktiawan, P., Dirgantara, F., & Waskito, S. (2023). Implementation and Supervision of Personal Data Protection Law on Online Platforms. *Journal of Social Science Studies*, 3(1), 101-108.

Benjamin, G. (2017). Privacy as a Cultural Phenomenon. *Journal of Media Critiques*, 3(10), 55-74.

Brough, A. R., & Martin, K. D. (2020). Critical Roles of Knowledge and Motivation in Privacy Research. *Current Opinion in Psychology*, 31, 11-15.

Díaz Ferreyra, N. E., Kroll, T., Aïmeur, E., Stieglitz, S., & Heisel, M. (2020). Preventative Nudges: Introducing Risk Cues for Supporting Online Self-Disclosure Decisions. *Information*, 11(8), 1-2.

Falgoust, M. (2016). Data Science and Designing for Privacy. *Techné: Research in Philosophy and Technology,* 20(1), 51-68.

Gardi, B., & Eddine, B. A. S. (2023). Cyber Security and Personal Data Protection in the Digital Age: Challenges, Impacts, and Urgency of Global Collaboration. *Bulletin of Science, Technology and Society*, 2(3), 58–63.

Infante, A., & Mardikaningsih, R. (2022). The Potential of Social Media as a Means of Online Business Promotion. *Journal of Social Science Studies,* 2(2), 45-49.

Inverardi, P., Migliarini, P., & Palmiero, M. (2023). Systematic Review on Privacy Categorization. *Computer Science Review*, 49, 1-28.

Jørgensen, R. F. (2016). The Right to Privacy under Pressure. *Nordicom Review*, 37, 165-170.

Kemarauwana, M., & Darmawan, D. (2020). Perceived Ease of Use Contribution to Behavioral Intention in Digital Payment. *Journal of Science, Technology and Society (SICO),* 1(1), 1–4.

Kovanic, M., & Spáč, S. (2022). Conceptions of Privacy in the Digital Era: Perceptions of Slovak Citizens. *Surveillance and Society*, 20(2), 186-202.

Meier, Y. (2023). Raising Awareness for Privacy Risks and Supporting Protection in the Light of Digital Inequalities. In *IFIP International Summer School on Privacy and Identity Management, Charm: Springer Nature Switzerland*, 44-51.

Nadon, G., Feilberg, M., Johansen, M., & Shklovski, I. (2018). In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms. In *Proceedings of the 9th International Conference on Social Media and Society*, 138-149.

Negara, D. S., & Darmawan, D. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13–19.

Negara, D. S., Darmawan, D., & Saktiawan, P. (2022). Privacy Violations on Social Media and Interpersonal Trust Among Young Generations. *Journal of Social Science Studies*, 2(2), 151-156.

Parrilli, D. M., & Hernández-Ramírez, R. (2021). Empowering Digital Users Through Design for Privacy. In *Perspectives on Design and Digital Communication II: Research, Innovations and Best Practices, Cham: Springer International Publishing*, 3-13.

Pascalev, M. (2017). Privacy Exchanges: Restoring Consent in Privacy Self-Management. *Ethics and Information Technology*, 19(1), 39-48.

Prettyman, S. S., Furman, S. M., Theofanos, M. F., & Stanton, B. C. (2015). Privacy and Security in the Brave New World: The Use of Multiple Mental Models. *In International Conference on Human Aspects of Information Security, Privacy, and Trust, Cham: Springer International Publishing*, 160-270.

Radjawane, L. E., & Mardikaningsih, R. (2022). Building Ethical and Fair Technology: Approaches to Responsible Technology Development and Application. *Journal of Social Science Studies*, 2(1), 189-194.

Ramle, N. L. B., & Mardikaningsih, R. (2022). Inclusivity in Technology-Based Services: Access and Skills Challenges. *Journal of Social Science Studies*, 2(2), 225-230.

Schoenherr, J. R. (2022). Whose Privacy, What Surveillance? Dimensions of the Mental Models for Privacy and Security. *IEEE Technology and Society Magazine*, 41(1), 54-65.

Serrano-Tellería, A. (2018). Users' Management of Mobile Devices and Privacy. *Profesional De La Informacion*, 27(4), 822-829.

Susser, D. (2016). Information Privacy and Social Self-Authorship. *Techné: Research in Philosophy and Technology*, 20(3), 1-27.

Tikk, E. (2017). Privacy Online: Up, Close and Personal. *Health Technology*, 7(4), 489-499.

Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy as a Fuzzy Concept: A New Conceptualization of Privacy for Practitioners. *Journal of the Association for Information Science and Technology*, 66(5), 918-929.

Verhulst, S. (2022). Operationalizing Digital Self-Determination. *Data & Policy*, 5, 1-17.

Watson, H., Moju-Igbene, E., Kumari, A., & Das, S. (2020). "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-12.

Xu, H., & Zhang, N. (2023). An Onto-Epistemological Analysis of Information Privacy Research. *Information Systems Research*, 35(3), 1422-1434.

Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). I've Got Nothing to Lose: Consumers' Risk Perceptions and Protective Actions After the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security*, 197-216.

Oluwatosin, A. (2024). Privacy Rights, Inference, and User Trust in Digital Platform Services, *Journal of Social Science Studies,* 4(1), 381 – 390.