UCP Journal *of* Law & Legal Education
Vol. 4, Issue 1 (January – June 2026)

Redefining Data Protection Standards: The Vitality of User Consent in Data Privacy Regulations and Legal Challenges

***Amayal Chaudhary*[*], *Faryal Chaudhary*[**]**

Abstract

Rapid global digitisation has created tensions between technological innovation and the protection of individual privacy rights. User consent has emerged as a central issue on this front. This paper reviews the effectiveness of existing consent mechanisms, assesses the confounding factors posed by emerging technologies, and discusses the ethical and legal ramifications of data privacy laws premised on consent. It investigates how technology influences user consent and offers recommendations to mitigate the identified harms. The research methodology is doctrinal, involving analysis of relevant legislative documents, leading case law, applicable enforcement frameworks, along with several secondary sources. The underlying ethical principles meant to inform consent compliance regimes are part of the review as well. The assessment has revealed a number of implementation deficits in existing consent frameworks. These include consent desensitisation, unclear or ineffective disclosure of algorithmic decisions, the rise of dark patterns, etc., which inhibit the ability of users to make truly free and autonomous decisions. Emerging technologies like Artificial Intelligence (AI) and the Internet of Things (IoT) exacerbate these problems and further strain user perception. The paper, therefore, recommends standardising data protection mechanisms with an emphasis on behavioural insights. It mandates the implementation of privacy-by-design principles and the elevation of enforcement measures to a level where user consent is treated as a substantive right.

[*] Director, Media & Press, Cyber & IP Association (CIPA), Lahore, Pakistan. Email: amayalch@gmail.com
[**] President, Pakistan Law Students Association (PLSA), Lahore, Pakistan. Email: faryalch339@gmail.com
Article History: Received: 08-05-2025; Received in revised form: 29-03-2026; Accepted: 03-08-2026.
Available online: 26-10-2026
DOI: https://doi.org/10.24312/ucp-jlle.04.01.545
OPEN ACCESS

Keywords: Data Privacy, User Consent, Data protection, Technological Innovation, Legal Challenges

Introduction

Across the Western world, writers consistently uphold privacy as a paramount asset, indispensable for a life of value. Decades ago, Charles Fried asserted that without privacy, we forfeit "*our very integrity as persons*" (Fried, 1968, p. 477), a sentiment that has since been widely echoed. Scholars broadly agree that privacy is deeply engaged with our sense of personhood (Wilkowska et al., 2022). It is also commonly observed that this fundamental right is under siege in modern society. Commentators depict these dangers in stark terms, warning that violations of privacy could usher in a world of horror, compromise our very humanity, or even pave the way for totalitarianism (Del Re, 2024). Hence, legal safeguards concerning privacy are often framed as critical to securing fundamental liberties.

Consent management evolved from being a checkbox exercise to a vital aspect of global data protection compliance. The European legislator defined the consent of the data subject as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*" (Directive 95/46/EC of the European Parliament and of the Council of Europe, 2023, Art. 2(h)). This vital consent framework holds various elements of data protection, such as freedom, specificity, and informed consent (Custers et al., 2018). The principle of autonomy reflects the legal idea of the connection between individuals and control over their own lives (Custers et al., 2014). For consent to be valid, it must be informed (Custers et al., 2018), which is a concept known as informational self-determination (Custers et al., 2013). Initially introduced in resolution (73) 22 by the Council of Europe in 1973, the concept acts as a safeguard against unlawful intrusions into an individual's privacy and family life. The concept of "authorised use" was also established in this resolution. It was perceived in a wider sense to involve a licence from an authoritative body or general legal permission (Council of Europe, 1973). For example, in the 2007 case of *Copland v. the United Kingdom* (European Court of Human Rights, 2007, para. 44), it was determined that the unauthorised

collection and storage of personal information related to an individual's telephone, email, and internet usage constitutes a breach of his/her right to privacy as outlined in Article eight of the European Convention on Human Rights (Council of Europe, 1950, Art. 8). Regulations like the General Data Protection Regulation of European Union, and other similar measures worldwide, aim to put users in driver's seat when it comes to their personal information. The legal and moral standards included in these frameworks, like the New York City Automated Decision Systems, the Net Neutrality Principle, and again the GDPR, have momentous effects on the global data management community. They promote the idea of building data management systems on a foundation of responsible individual protections, rather than isolating them. However, there exist a number of barriers that reduce the real efficacy of such regulations.

A significant challenge lies in ensuring that consent mechanisms are efficient and user-friendly. Traditional consent dialogues continuously underperform in fulfilling their intended goals. This culminates in user confusion and deviance from privacy regulations. Given the sheer volume of personal information, smartphones prove to be the prime targets for data theft. The prevalent use of Android devices and their ancillary services has catalysed global data collection and sharing (Guaman et al., 2021). Users generally consent to privacy policies when they install applications, overlooking the serious implications (Felt et al., 2012). Service providers offer sprawling and impenetrable terms and conditions, privacy policies, or similar documents during the registration process. Due to this, users encounter multiple consent requests and oftentimes struggle to comprehend these documents (Custers et al., 2014). This situation leaves them with little option but to consent, as declining may lead to restricted services or total exclusion from digital platforms. Application permissions, standardly obtained at the point of registration, act as a primary method for acquiring user consent. Post-approval, they allow ongoing permission to user data (Custers et al., 2013), even when the app is not in active use.

This growing intrusion upon our digital activity has created the urgent need for online consumers to become more aware of the processing of their personal data. If such a progressive erosion of privacy remains unaddressed, individuals will likely be subjected to

corporate surveillance without their knowledge. Consequently, digital ecosystems, rather than regulatory organisations, will redefine digital privacy, potentially leading to an abuse of power. Therefore, to achieve its primary research objective, the study aims to identify the level of effectiveness reached by regular data privacy frameworks in helping users offer meaningful consent. It assesses the extent of difficulties faced by standard user consent procedures because of the integration of new technologies like Artificial Intelligence and the Internet of Things. It further evaluates key moral values which can be used by consent management systems to ensure that users understand their data tracking processes. It highlights the impact of "consent fatigue" on user decision-making, and methods which can be used to mitigate its effects.

In addressing these queries, this article starts with the premise of delineating the methodology adopted and providing a literature review that assimilates seminal works on user consent. Succeeding segments evaluate the efficacy of extant regulatory frameworks in tandem with enforcement mechanisms and accountability systems. Friction points arising from new technologies and ethical principles of present-day data practices are evaluated as well. In its final analysis, recommendations for optimising consent-based frameworks are provided whilst recapping the principal findings and their relevance for future studies.

Research Methodology

The methodology adopted is predominantly qualitative and doctrinal, based on a comprehensive analysis of statutory laws, legal precedents, and academic literature. Different regulatory frameworks are compared to evaluate their effectiveness in safeguarding users' consent in relation to privacy. Relevant court rulings and major International and Regional Legal Instruments are selected as primary sources. They encompass the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the ePrivacy Directive. Selection of these instruments is based on their substantial global influence, relevance to regulation, and thoroughness. Their central role in defining modern data protection principles on user consent is also given considerable value. To add historical and normative perspective,

foundational tools like the OECD Privacy Guidelines are evaluated. Court rulings are shortlisted based on their canonical status, especially those revolving around the validity and scope of consent. Additionally, ethical dilemmas are reviewed together with compliance barriers and the effects of decisions made by algorithms. Scholarly articles, policy reports, and expert opinions serve as secondary sources. Their inclusion is predicated on relevance and merit, and their contribution to the prevailing debates. This work prioritised the use of peer-reviewed scholarship, based primarily on journal outputs from distinct legal, technological, and interdisciplinary databases but also drawing on seminal works where appropriate. In general, the study is organised within a legal-doctrinal paradigm, giving prominence to logical arguments and normative analysis.

Literature Review

The privacy risks in the collection and use of user data have been well-documented (Yang et al., 2023). Technical solutions must address the need to protect privacy and the utility of data applications in light of the substantial disagreement about consent withdrawal procedures and the spatial domain of the *right to be forgotten.* An important strand of the literature is focused on the legal reaction to such hardships, such as the General Data Protection Regulation (GDPR). It introduced momentous reforms by revising data privacy laws and network platforms (European Parliament & Council of the European Union, 2016). The GDPR's impact on website pageviews, revenue, data sharing online, and market concentration among technology vendors was studied to evaluate the economic and unintended consequences of the regulation. It was found that these developments led to the implementation of updated procedures in online consent systems, which helped fulfil the changing privacy requirements and regulatory criteria. (Degeling et al., 2019). Nevertheless, such changes have added complications in consent management systems that require deeper investigation.

Beyond regulatory developments, existing research highlights the ethical and practical challenges associated with the management of consent across different domains. The analysis of data protection standards, along with consent acquisition methods and participant anonymity, reflects the importance of ethical

research (Ashley et al., 2002). At the same time, uncertainty about smartphone research through sensor mobile apps causes anxiety due to a lack of awareness. Similar concerns are found in the ethical data management of mobile health (mHealth) apps through privacy statement reviews, security, and sharing practice evaluations that focus especially on women's health applications (Colangelo & Maggiolino, 2019). Bearing out the theory, users are unaware of their privacy expectations and rights to user information. There exists a communication gap which has not been sufficiently addressed by regulations.

Accepting this mantle, innovation-led measures aimed at improving consent management are also explored in the literature. Organisations encounter growing challenges because they need to handle a bunch of different privacy regulations; on the other hand, users want free access to services and their data with full transparency (Khatiwada et al., 2024; Olca & Can, 2022). To address this, studies have produced advanced consent management platforms (CMPs) which simplify consent procedures while adhering to legal requirements (Nouwens et al., 2020; Toth et al., 2022). For example, the unalterable records created by blockchain enable better trust and transparency in consent management (Kakarlapudi & Mahmoud, 2021). Similarly, the User-Managed Access (UMA) framework allows users to handle consent operations with a standardised architecture in order to overcome current consent methods (Maler, 2015). Furthermore, mobile location-based advertising providers build strategies to minimise users' sense of intrusiveness. These efforts increase customer confidence and meet data protection requirements (Gutierrez et al., 2019). Similarly, customised consent management software is essential for many domains, including healthcare and IoT applications, since these sectors aim to fulfil the unique privacy requirements of their users. For example, Merlec et al. (2021) created a smart contract-based system that enables users to maintain control of their personal data from its initial generation until its termination.

Regardless of these breakthroughs, the literature still notes limitations in practice. The analysis suggests that consent procedures in current fitness applications are deficient in two essential areas: the grant of permanent consent and vagueness in consent protocols (Alhajri et al., 2022). Therefore, it is contended

that the efficacy of user consent is largely compromised by interface design rather than regulatory deficiency alone.

Studies also suggest that many consent banners employed by websites set the stage for "*dark patterns,*" which manipulate user choices and subvert informed consent (Almeida & Monteiro, 2021; Gray et al., 2021). Once the importance of interdisciplinary factors in consent management is taken into account, frameworks that have been put forth for evaluating consent procedures come to the forefront (Human et al., 2022). Similarly, the need for a user-centric approach to consent management that follows the legal standards and also enhances user experience and conception is brought to light (Jesus & Pandit, 2022).

It is summarised that the issue of user consent, for all intents and purposes, is a complex one. It occurs where the requirements of legal compliance and the requirements of system and user interface overlap. There are three components: granular assessment of data protection frameworks, management systems and privacy provisions, which have the potential to mitigate privacy risks when correlated. Although there have been a variety of enhancements in the regulations for data protection, their implementation lacks uniformity in legal, technical and user experience aspects. Existing literature is bereft of a harmonised approach and a thorough analysis of the interrelation of these variables. This paper seeks to fill this gap, exploring the concept of consent through a dual legal and analytical lens, and thus contributing to a broader understanding of the utility of consent in the global digital domain.

The Efficacy of Existing Frameworks: Their Relevance and Adaptability

Contemporary data protection laws, such as General Data Protection Regulation (GDPR) (2016) (European Union), California Consumer Privacy Act (CCPA) (2018) (United States), Personal Information Protection and Electronic Documents Act (PIPEDA) (2000) (Canada), Lei Geral de Proteção de Dados (LGPD) (2018) (Brazil), Protection of Personal Information Act (POPI) (2013) (South Africa), Act on the Protection of Personal Information (APPI) (2003) (Japan) etc., are mainly designed for digital interfaces (ambient sources like touch sensing, IoT devices, and cameras). They work together to maintain the autonomy of the

user and provide legal data processing. However, their ways of approaching consent and data protection show pronounced variance between jurisdictions.

The GDPR, introduced in 2018, is a global and comprehensive picture of data protection. It was enacted to establish the necessary conditions that would encourage EU citizens to have faith in digital systems. It applies extraterritorially, and for that reason the European Data Protection Supervisor labelled it as the "*gold standard*" for safeguarding personal information (Buttarelli, 2016). Even though it imposes consent requirements on consumer IoT devices, it provides alternative lawful bases for data processing. After the initial year of the GDPR's enforcement, the UK Information Commissioner's Office indicated that people were gaining more control over their data. For instance, from 25 May 2018 to 1 May 2019, the commissioner obtained 14,000 personal data breach reports, four times more than the office received previously (Information Commissioner's Office, 2019)**.** Similarly, regulatory bodies from 11 countries in the European Economic Area already imposed fines under the GDPR totalling around *€56 million* (European Data Protection Board, 2019). This clearly indicates its contribution to increased reporting of data breaches and stronger regulatory enforcement. Key provisions in the regulation concerning data privacy and protection include: users' right to revoke consent at any time (European Parliament & Council, 2016, Art. 7(3)); establishment of legal grounds for processing personal data (European Parliament & Council, 2016, Art. 6(1)); users' entitlement to transparent information about their personal data (European Parliament & Council, 2016, Art. 12); users' right to access their personal information, including how it's obtained, processed, and shared (European Parliament & Council, 2016, Art. 15); the right to be forgotten, allowing for prompt erasure (European Parliament & Council, 2016, Art. 17); users' ability to control and easily transfer their personal data between service providers (European Parliament & Council, 2016, Art. 20); individuals' right to oppose personal data processing for marketing or non-service-related purposes(European Parliament & Council, 2016, Art. 21); implementation of reasonable data protection measures by design or default in company development and processing systems (European Parliament & Council, 2016, Art. 25); prompt notification to users of data breaches that may

jeopardise their rights; requirement for a data protection officer to ensure company compliance (European Parliament & Council, 2016, Art. 34); and penalties for non-compliance with the regulation (European Parliament & Council, 2016, Art. 37). Even though it is argued to be a very comprehensive and effective regulation, it's not without limitations. The substantial expenses that organisations face to comply with specific requirements related to data mapping, cross-border data transfers, and various data processing activities necessitate significant financial investment. Furthermore, the regulation does not apply to EU member states' national security activities or law enforcement data. It is also not applicable when data is processed for personal or household purposes without commercial or economic intent. (European Parliament & Council of the European Union, 2016, Recital 18).

On the other hand, the California Consumer Privacy Act (CCPA), which has been in effect since 2020, focuses more on the personal information of the residents of California; for example, they are allowed to opt out of data-selling practices instead of requiring prior consent. It is said to be based on three important principles: accountability, control, and transparency. One of its crucial aspects is broadening the definition of personal information. This expansion includes geolocation data, personal identifiers, and inferential data from previously mentioned information, which contributes to the formulation of a profile that reflects users' preferences and behaviours. Additionally, it includes data related to the user's internet browsing and search history. The development of this regulation represents an important move toward protecting the privacy rights of individual citizens regarding sensitive personal information. It also gives consumers control over the gathering, use and sale of their personal data by firms that offer such services.

With that said, there is a missing connection between the spirit of the law and the practical application. Even though these frameworks have raised the bar for data protection, challenges remain in their implementation and enforcement. They still rely heavily on consent as a primary legal basis. This reliance is problematic in "algorithmic societies" where data processing is continuous and ecosystemic. Research on diverse privacy methods in the area of big data confirms that frameworks must strike a balance between the benefits of making decisions through data

using individuals' privacy and data-driven techniques (Dangal, 2023).

Reference can also be made to the ePrivacy Directive, which is a part of the European legal framework on electronic communications and focuses on the processing of personal data and the protection of privacy in this sector (European Parliament & Council of the European Union, 2002). The Directive has entrusted a pivotal role to consent of the user and/or the subscriber, which is encountered in several instances: with regard to the confidentiality of communication (European Parliament & Council, 2002, art. 5), to traffic data (European Parliament & Council, 2002, art. 6), to location data (European Parliament & Council, 2002, art. 9), to the elimination of the temporary denial or absence of consent in emergencies (European Parliament & Council, 2002, art. 10), to directories of subscribers (European Parliament & Council, 2002, art. 12) and to unsolicited communications (European Parliament & Council, 2002, art. 13). This sector-specific focus complements the broader GDPR framework by operationalising consent in technologically intensive environments such as cookies and online tracking. With that being said, its reliance on repetitive requests for consent, especially in the field of cookie banners, contributes to user fatigue and daily acceptance habits, thereby undermining the quality of consent in reality. This leans towards a broader regulatory barrier: even if regulations tighten the net around consent, application in the digital space eviscerates user-driven agency.

In 1978, the Organisation for Economic Co-operation and Development (OECD) established an Expert Group to develop principles on basic rules on cross-border data flow, personal data, and data privacy protection. They primarily sought to promote harmonisation of the national legislation (OECD, 2002). This OECD Expert Group worked in cooperation with the Council of Europe, which was concurrently preparing a CoE Convention. In 1980, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were implemented. These guidelines put forward eight principles to be used at the national level regarding the protection of individual privacy:

- *Collection limitation principle*
- *Data quality principle*
- *Purpose specification principle*

- *Use limitation principle*
- *Security safeguards principle*
- *Openness principle*
- *Individual participation principle*
- *Accountability principle*

While knowledge is deemed the minimum standard of collection of data ("OECD guidelines on the protection of privacy and Transborder flows of personal data," 2002, p. 52), the guidelines do not specify the conditions under which the data subject's awareness of data collection suffices, nor when explicit consent is required. The phrase "where appropriate" also limits the applicability of this provision by shifting the responsibility to the data controller to decide cases where, due to practical or policy reasons, the knowledge or consent of the data subject is not necessary.

It is observed that the existing legal systems of consent, which rely on the concept of autonomous authorisation, although offering several protections, have proven to be inefficient in reality. European Data Protection regulations suggest even more stringent legal requirements for explicit consent. This results in the phenomenon of "consent desensitisation", a situation in which users habitually agree to consent requests without being engaged with or understanding them in their entirety, compromising privacy protection and trust in data processing.

Enforcement Mechanisms and Accountability in Data Protection Laws

The role and characteristics of the institutions that monitor and regulate the processing of personal data also vary widely around the world. Current frameworks are particularly deficient in overcoming the challenges posed by evolving technologies. In Europe, there are numerous bodies such as the *Commission Nationale Informatique et Libertés* in France, the *Hellenic Personal Data Authority* in Greece, the *Garante per la protezione dei dati personali* in Italy, the *Comissão Nacional de Proteção de Dados* in Portugal, the *Agencia Española de Protección de Datos* in Spain, and the *Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte* in Switzerland. They are important in different institutional contexts, as they have patchy performance in

practice depending on the availability of resources, the ability to enforce, and the approach to national implementation.

Whilst regulations such as GDPR and CCPA have bent over backwards to enforce user rights, their delivery and enforcement processes are not built to last (Ehimuan et al., 2024). The present model is blighted by poor privacy policies that are either absent or too knotty for users to comprehend (Galvin & Demuro, 2020). Non-transparency bends the rules on how informed consent is supposed to work, leaving users vulnerable to data abuse. Similarly, innovative approaches such as the "sticky policy" paradigm, although promising and designed to ensure consistent application of privacy preferences across systems, remain unimplemented and ineffective at scale (Ashley et al., 2002). Technological solutions, including federated learning (FL) and blockchain-based systems, together with privacy-enhancing techniques such as multi-party computation and homomorphic encryption, have been proposed for improving both security and privacy (Narkedimilli et al., 2024). However, these solutions remain limited in practice. Federated learning systems remain susceptible to some privacy attacks, and blockchain-based systems experience impediments to mass adoption (Zhu et al., 2026). The EU maintains a faulty data protection framework that produces no positive effects even after passing newly proposed laws. More essentially, even the active consent model does not sufficiently consider mental and environmental elements that determine user behaviour patterns. Individuals who navigate through privacy policies discover that the content they receive differs from what they anticipated in those terms (Martin, 2015). While users prioritise certain aspects of data protection, current policies do not dedicate sufficient attention to these essential points (Custers et al., 2014). Such a mismatch only deteriorates the performance of consent mechanisms and user trust.

Cases in the courts also point towards advances and constraints. As an example, in the Planet49 case, the Court of Justice of the European Union (CJEU) defined preselected check-boxes, which contravene the conditions of "valid consent", requiring active and unambiguous consent. The decision underlined that the consent of the users has to be expressed in separate explicit statements (Court of Justice of the European Union, 2019). Likewise, Orange Romania led the Court of Justice of the European Union to develop the principles in place into particular active

consent conditions (Court of Justice of the European Union, 2020). It was held that consent becomes invalid in case a pre-ticked box has been checked by the data controller prior to a contract being signed. Besides, consent is never deemed to be freely given when the terms of the contract mislead users about their ability to proceed without agreeing to data processing. The resulting confusion caused by forcing customers to fill in another form if they want to reject consent also violates the right of the customers to clear and transparent information (Court of Justice of the European Union, 2020). By beefing up the absolute nature of "valid consent" as a legal basis for data processing, the decision lays down a precedent that national courts are obliged to adhere to, shaping data protection practices in Europe. Plus, a much-anticipated European interpretative ruling on consent-related issues emerged in the well-known German Facebook (now Meta Platforms) case, where the Bundeskartellamt (German Federal Cartel Office) imposed tight curbs on Facebook's data processing practices (Bundeskartellamt, 2019). The precedent establishes vital standards for methods through which user data gets processed while focusing on social media platforms that apply targeted advertising models.

This points to an ironic problem of enforcement where the provisions of "valid consent" have been clarified by the courts, and yet organisations still carry on with fraudulent design processes with little to no ramifications. It is not an issue of legal ambiguity; the legal rule is explicit, but design-based manipulation is in a compliance grey area. This finding addresses the first research query that present frameworks are of little avail to users in offering meaningful consent. The primary reason for that is not legislative loopholes but sparse implementation measures. Regulatory bodies exist, but their mechanisms are powerless to avert the exploitation of users through malformed or incomprehensible privacy policies.

Regulatory Hurdles and Challenges Posed by Emerging Technologies

Modern AI processing techniques and machine learning algorithms have added a layer of challenges to data privacy. Several issues arise because these systems need extensive personal information to perform optimally. Differential privacy and the release of private data demonstrate the necessity to develop

analysis-friendly algorithms which safeguard individual privacy during data mining operations (Mohammed et al., 2011). The opacity of algorithms often leaves users in the dark regarding the utilisation of their data, which results in substantial erosion of user trust and autonomy. At present, it is essential to handle the ethical problems linked to computerised decision capabilities since they threaten users' fundamental rights. Big data requires a privacy norm-based access control system that functions to guide collaborative decision-making processes (Ulusoy & Yolum, 2020).

Furthermore, the field of behavioural economics alongside cognitive sciences has carefully studied "Legal design" as an engineering system that nudges users towards specific choices (Tversky & Kahneman, 1974). However, state and national lawmakers across Europe share present-day concerns regarding the potential misuse of such nudges (Alemanno, 2016). Operators are facing scrutiny regarding their adoption of these procedures since they use them mainly for self-benefit without holding regard for user needs or the welfare of the general population (Di Porto & Egberts, 2023). Frequently, the elements that contribute to the creation of a poorly designed web interface stem from deliberate decisions aimed at exploiting user cognitive biases, thereby enhancing the profits of service providers (Brignull, 2025). Such a detrimental objective is incompatible with the principles of equitable legal digital design. Instead, it should prioritise human rights, including the right to self-determination, through a commitment to substantial transparency and adherence to ethical and normative standards.

Moreover, the concept of informed consent morphs into a double-edged sword amid algorithmic complexities (Giannopoulou, 2020). Classic notions of consent no longer fit the purpose, since users are often deficient in grasping the concept of data practices. Some of these very common challenges faced globally include;

- The rapid expansion and sheer volume of data in our technology-centric society present a plethora of hurdles in managing billions of data points (Siddiqa et al., 2016).
- Discrepancies in the definitions of key concepts such as data privacy, user consent, withdrawal of consent, and the right to erasure can impede organisations' decisions

regarding which data privacy law to implement for their users (Tyler, 2022).

- Numerous data analysts have singled out human error as a primary obstacle in data privacy (Amoresano & Yankson, 2023). For instance, insufficient awareness among employees can severely compromise an organisation's data privacy and protection framework. This vulnerability may manifest through practices such as the use of weak passwords or susceptibility to phishing attacks, ultimately exposing user data to risks and potential loss.
- The financial repercussions of rectifying a data breach can be substantial, leading to significant revenue losses for the organisation, which may also incur severe regulatory fines (Tosun, 2021).

In relation to the second research query, the study finds that technological advancement has outpaced regulatory capacity. The combination of these technologies has rendered "informed consent" almost unachievable since the tracking of data becomes omnipresent and invisible (Zimmeck et al., 2024). The ambient nature of IoT collection, data thirstiness of AI systems, and complexity of algorithm processing are all conditions under which the traditional notion of consent cannot be adequately implemented.

Ethical Implications of Data Privacy

Transparency is one of the integral principles of data protection, yet it is rarely observed in practice (Belcheva et al., 2023). The issues of autonomy, consent, and potential exploitation remain a central concern. The relationship between individual privacy decisions and the societal impact of data sharing in general needs to be understood (Meier and Krämer, 2022). In the data economy, there are three phases of data processing: *information reception, approval and initial use, and secondary use (reuse)*. Each phase presents risks to individual control (Van Nortwick & Wilson, 2021). Privacy threats extend beyond personal decisions and data, including shared private information with others. A soft privacy matching mechanism that allows for controlled relaxation of privacy preferences to align with service providers' policies was proposed (Alom et al., 2019). Enhancing user experience through this method generates potential ethical problems because users

receive minimal information about the consent's meaning. To properly use AI in data processing, the ethical concerns need thorough evaluation. Algorithmic models continue to face challenges because of their biases and discrimination, while having unclear responsibility protocols. Similarly, the design of consent banners has also come under scrutiny, with the use of "dark patterns" that manipulate user consent (McGarrigle et al., 2026). In the context of cookie consent management, such usage can undermine the validity of consent under Article 5(3) of the ePrivacy Directive. The German data protection supervisory authorities have identified certain practices as inadmissible "nudging" ("DSK: Neue Orientierungshilfe für Anbieter:innen von Telemedien," 2022), where design elements steer users toward granting consent rather than making a truly voluntary choice. Reports like the *OH Telemedien 2021 Guidance* and other regulatory documents have criticised deceptive tactics ("DSK: Neue Orientierungshilfe für Anbieter:innen von Telemedien," 2022). Many consent banners are designed to encourage users to accept data collection rather than providing clear options for opting out. This raises ethical concerns about the transparency and fairness of such practices (Gray et al., 2021).

The *privacy paradox* is also worth mentioning here, which refers to the phenomenon where individuals express concern about their privacy yet engage in behaviours that compromise it. When this paradox is explored from a configurational perspective, the need for a deeper understanding of the factors influencing privacy decision-making becomes prominent (Yang et al., 2023). Addressing the privacy paradox is essential for developing effective consent management strategies that empower users. Felt et al. (2012) conducted two studies revealing that Android permissions fail to effectively inform users about resource accessibility. Issues related to user comprehension, including confusing caption headings, difficulty connecting resource-based alerts to consequences, inability to reason about permission absence, and alert fatigue were identified (Felt et al., 2012). Consent requests during registration are often ineffective due to complex, lengthy forms, and big data can render consents obsolete. If a comparison is made between "informed consent with user expectation" and "consent based on criteria from literature and privacy policies", it will become obvious that not all consents are crucial to users; the

most important ones are typically included in privacy policies (Custers et al., 2018).

In addressing the third research query, it is noted that ethical issues such as dark patterns, manipulative design, and the privacy paradox must be incorporated into consent frameworks to ensure that consent is genuinely meaningful. Transparency, autonomy, and fairness must be operationalised using design requirements which extend beyond formal legal compliance to address the actual user experience.

Recommendations for Harmonising Data Protection Standards

A coherent approach to data protection standards must give primacy to user consent as a cardinal rule. To actually and truly address the concerns raised herein, there is a dire need for a thorough conception of privacy decision-making that incorporates insights from psychology and behavioural economics (Dinev et al., 2015). The law requires that withdrawing consent should be as straightforward as providing it (Resta, 2000). Ideally, a user should be able to access the same withdrawal mechanism at any time. Conversely, in practice, many businesses fail to implement this requirement effectively (Jha et al., 2023). The imperative for affirmative action to indicate an informed and voluntary decision is reinforced by the very terminology used in consent mechanisms. Different visual techniques (such as colour schemes) highlight options like “Agree” or “Allow” while de-emphasising alternatives like “Reject” or “Block”. These practices compromise the authenticity of consent by nudging users toward acceptance, which then contributes to consent fatigue, where individuals habitually agree without fully engaging with the information presented (Helberger et al., 2021). Hence, the fourth research question obtains a concrete response that the issue of consent fatigue severely deteriorates the decision-making ability of users. To mitigate its effects, Estonia serves as a great example; it has introduced an innovative consent service that enables individuals to authorise the sharing of their personal data (including sensitive information like health records) from state-managed registries to private sector entities. This digital solution, developed by the Estonian Information System Authority (RIA), aims to facilitate the provision of personalised services by allowing private companies to

access data with the explicit consent of the individual. By integrating these perspectives, as mentioned above and below, policymakers can develop frameworks that enhance user agency and promote informed consent;

- Inclusion of privacy agents that can assist users in making informed decisions regarding their personal information could enhance user autonomy and improve compliance with data protection regulations (Bernsmed et al., 2012).
- User education and awareness are critical components of effective consent management. The impact of privacy fatigue on decision-making behaviour increases the need for clear and accessible privacy information. By improving user education, organisations can empower individuals to make informed choices regarding their personal data (Liu et al., 2024).
- Technological solutions like the development of methods that preserve individual privacy in the context of big data can play a pivotal role in enhancing data privacy. By utilising, in a positive manner, the advancements in technology, organisations can implement privacy-preserving measures that align with regulatory requirements.
- Implementing a permission model that automatically revokes all the permissions given after a particular time frame can also be considered an innovative approach towards protection and enhancing data privacy standards.
- Enforcing context-awareness and privacy-by-design principles in the specification of information systems has also been proposed as a way to enhance data privacy and user consent.

Conclusion

In conclusion, a paradigm shift is needed, one that views consent as a design challenge requiring culturally-informed consideration. The vitality of user consent is in its ability to maintain individual autonomy over systemic exploitation. The traditional model shifts the burden of privacy protection onto the individual, who is often the least equipped to manage it. This paper finds that the current consent frameworks fail to realise their full potential due to serious implementation gaps. They consider

consent as a regulatory compliance artefact but not as a substantive mechanism. New technologies such as AI and IoT contribute to these issues by creating opacity, enlarging the scope of data processing beyond initial authorisation, and exceeding regulatory adaptations. Besides, existing frameworks do not properly regulate ethical issues, which undermine real user autonomy. The results also reveal that mitigation of "consent fatigue" is a problem that needs regulatory consistency and user-centric technology solutions. It is imperative that organisations adopt state-of-the-art solutions so that user autonomy is ring-fenced without neglecting the existing data privacy regulations. Practically, the recommendations, which are presented in this research, can be used to offer advice to the policymakers, regulators and organisations that aim to improve the efficacy of consent. A comprehensive solution to the stipulated problems is the blending of technological protection, user-centred design principles, and ethical guidelines. The redefined standards of data protection are impossible to reach without avoiding the concept that consent, which is once legally acquired, will inherently protect the interests of the users. Academically, the research is a part of the widening agreement that privacy self-management is no longer adequate in the data world of the twenty-first century. It expands the field of data protection scholarship by combining legal analysis, assessment of technological feasibility, and study of behavioural psychology to transform the concept of user consent into an interdisciplinary issue, instead of a purely legal one. The findings can contribute to the re-conceptualisation of consent as an ongoing process demanding continuous engagement, adaptation, and opportunities for reconsideration. Such an understanding of consent has material undertones for legal theory and system design. Research on consent's technical and legal aspects helps professionals and researchers develop transparent systems for preserving privacy, which give people total control of their personal information. A sustained partnership between policy-makers and representatives representing both industry and academic researchers must exist to create flexible regulatory frameworks that respond to quickly changing data-based technological advancement. In the future, it is recommended that empirical and cross-cultural research be conducted to assess the efficacy of consent, user comprehension, and contextual differences. Technological research should be done to integrate privacy-

preserving tools and consent mechanisms, whereas longitudinal studies will be required to monitor changing user behaviour over time. Besides, research on cross-jurisdictional implementation of dark pattern bans should be increased in order to provide uniform protection across nations. The role of "data visceralisation" in making data sharing more meaningful also warrants further exploration. The implementation of a holistic method requiring multiple participants enables the creation of modern privacy protection standards that maintain consent principles at the same time.

References

Act on the Protection of Personal Information, Act No. 57 of 2003 (Japan). https://www.japaneselawtranslation.go.jp/en/laws/download/130/09/h15Aa000570101en1.0_h15A119.pdf

Alhajri, M., Salehi Shahraki, A., & Rudolph, C. (2022). Privacy of fitness applications and consent management in blockchain. *Australasian Computer Science Week 2022*, 65-73. https://doi.org/10.1145/3511616.3513100

Almeida, F., & Monteiro, J. A. (2021). Exploring the effects of GDPR on the user experience. *Journal of Information Systems Engineering and Management*, 6(3), em0140. https://doi.org/10.21601/jisem/10957

Alom, M. Z., Carminati, B., & Ferrari, E. (2019). Adapting users' privacy preferences in smart environments. *2019 IEEE International Congress on Internet of Things (ICIOT)*, 165-172. https://doi.org/10.1109/iciot.2019.00036

Alemanno, A. (2016). Nudge and the European Union. In *Edward Elgar Publishing eBooks* (pp. 271–284). https://doi.org/10.4337/9781785367854.00016

Amoresano, K., & Yankson, B. (2023). Human error - a critical contributing factor to the rise in data breaches: A case study of higher education. *HOLISTICA – Journal of Business and Public Administration*, *14*(1), 110–132. https://doi.org/10.2478/hjbpa-2023-0007

Ashley, P., Powers, C., & Schunter, M. (2002). From privacy promises to privacy management. *Proceedings of the 2002*

workshop on New security paradigms - NSPW '02. https://doi.org/10.1145/844107.844110

Belcheva, V., Ermakova, T., & Fabian, B. (2023). Understanding Website Privacy Policies—A longitudinal analysis using natural language processing. *Information*, *14*(11), 622. https://doi.org/10.3390/info14110622

Bernsmed, K., Tøndel, I. A., & Nyre, Å. A. (2012). Design and implementation of a CBR-based privacy agent. *2012 Seventh International Conference on Availability, Reliability and Security*, 317-326. https://doi.org/10.1109/ares.2012.60

Brignull, H. (2025). Exploiting vulnerabilities in decision-making (Ch. 6). In *Deceptive design*. Testimonium Ltd. https://deceptive.design/book/contents/chapter-6/

Bundeskartellamt. (2019). *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing (B6-22/16)*. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, *6*(2), 77–78. https://doi.org/10.1093/idpl/ipw006

California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (2018). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&chapter=20.&part=4.&lawCode=CIV

Court of Justice of the European Union. (2020). *Orange România SA v. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* (Case C-61/19). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CJ0061

Court of Justice of the European Union. (2019). *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Case C-673/17, ECLI:EU:C:2019:246).https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0673

Colangelo, G., & Maggiolino, M. (2019). Antitrust Uber Alles. Whither competition law after Facebook? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3362428

Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms.* https://www.echr.coe.int/documents/d/echr/convention_ENG

Council of Europe. (1973). *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.* https://rm.coe.int/1680502830

Custers, B., Dechesne, F., Pieters, W., Schermer, B., & Van der Hof, S. (2018). *Consent and privacy. The Routledge Handbook of the Ethics of Consent*, 247-258. https://doi.org/10.4324/9781351028264-23

Custers, B., Van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet*, 6(3), 268-295. https://doi.org/10.1002/1944-2866.poi366

Custers, B., van der Hof, S., Schermer, B., Appleby-Arnold, S., & Brockdorff, N. (2013). Informed consent in social media use – The gap between user expectations and EU personal data protection law. *Scripted*, 10(4), 435-457. https://doi.org/10.2966/scrip.100413.435

Dangal, S. (2023). Data privacy and security in big data: A comparative analysis. *International Journal of scientific research in engineering and management*, 07(09). https://doi.org/10.55041/ijsrem25590

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy ... Now take some cookies. *Informatik Spektrum*, 42(5), 345-346. https://doi.org/10.1007/s00287-019-01201-1Del Re, E. (2024). Technologies of data protection and institutional decisions for data sovereignty. *Information*, *15*(8), 444. https://doi.org/10.3390/info15080444

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). Official Journal of the European Communities, L 281, 31–50. https://eur-lex.europa.eu/eli/dir/1995/46/oj

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—Informing privacy research through information systems, psychology, and behavioural

economics: Thinking outside the "APCO" box. *Information Systems Research*, 26(4), 639-655. https://doi.org/10.1287/isre.2015.0600

Di Porto, F., & Egberts, A. (2023). The collective welfare dimension of dark patterns regulation. *European Law Journal*, *29*(1–2), 114–141. https://doi.org/10.1111/eulj.12478

DSK: Neue Orientierungshilfe für Anbieter:innen von Telemedien. (2022). *Datenschutz und Datensicherheit - DuD*, 46(2), 76. https://doi.org/10.1007/s11623-022-1564-0

Ehimuan, B., Chimezie, O., Ob, O. V. A., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. World Journal of Advanced Research and Reviews, 21(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

European Data Protection Board. (2019). *2019 annual report: Working together for stronger rights. https://share.google/lZaVOx2NpvHiQShfB*

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Court of Human Rights. (2007). *Copland v. the United Kingdom* (Application No. 62617/00, Judgment of 3 April 2007). https://hudoc.echr.coe.int/eng?i=001-79996

European Parliament & Council of the European Union. (2002). Directive 2002/58/EC of 12 July 2002 *concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1-14. https://doi.org/10.1145/2335356.2335360

Fried, C. (1968). Privacy. *The Yale Law Journal*, 77(3), 475. https://doi.org/10.2307/794941

Galvin, H. K., & DeMuro, P. R. (2020). Developments in privacy and data ownership in mobile health technologies, 2016-

2019. *Yearbook of Medical Informatics*, 29(01), 032-043. https://doi.org/10.1055/s-0040-1701987

Giannopoulou, A. (2020). Algorithmic systems: Is consent in the details? *Internet Policy Review*, *9*(1). https://doi.org/10.14763/2020.1.1452

Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1-18. https://doi.org/10.1145/3411764.3445779

Guaman, D. S., Del Alamo, J. M., & Caiza, J. C. (2021). GDPR compliance assessment for cross-border personal data transfers in Android apps. *IEEE Access*, 9, 15961-15982. https://doi.org/10.1109/access.2021.3053130

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behaviour*, 95, 295-306. https://doi.org/10.1016/j.chb.2018.09.015

Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M., & Strycharz, J. (2021). EU consumer protection 2.0: Structural asymmetries in digital consumer markets. *BEUC* (*The European Consumer Organisation*). https://www.beuc.eu/brochure/eu-consumer-protection-20-structural-asymmetries-digital-consumer-markets-0

Human, S., Pandit, H. J., Morel, V., Santos, C., Degeling, M., Rossi, A., Botes, W., Jesus, V., & Kamara, I. (2022). Data protection and consenting communication mechanisms: Current open proposals and challenges. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 231-239. https://doi.org/10.1109/eurospw55150.2022.00029

Information Commissioner's Office. (2019). *GDPR: One year on.* https://ico.org.uk/media/about-the-ico/documents/2616187/gdpr-one-year-on.pdf

Jesus, V., & Pandit, H. (2022). Consent receipts for a usable and auditable web of personal data. *IEEE Access*, 10, Article 3157850. https://doi.org/10.1109/access.2022.3157850

Jha, N., Trevisan, M., Mellia, M., Irarrazaval, R., & Fernández, D. (2023). I refuse if you let me: Studying user behavior with privacy banners at scale. *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*, 1–9. https://doi.org/10.23919/TMA58422.2023.10198936

Kakarlapudi, P., & Mahmoud, Q. (2021). A systematic review of blockchain for consent management. *Healthcare*, 9(2), 137. https://doi.org/10.3390/healthcare9020137

Khatiwada, P., Yang, B., Lin, J., Mugurusi, G., & Underbekken, S. (2024). A reference design model to manage consent in data subjects-centered Internet of Things devices. *IoT*, 5(1), 100–122. https://doi.org/10.3390/iot5010006

Lei Geral de Proteção de Dados Pessoais [LGPD], Lei No. 13.709, de 14 de agosto de 2018 (Brazil). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Liu, Z., Iqbal, U., & Saxena, N. (2024). Opted out, yet tracked: Are regulations enough to protect your privacy? *Proceedings on Privacy Enhancing Technologies*, 2024(1), 280–299. https://doi.org/10.56553/popets-2024-0016

Maler, E. (2015). Extending the power of consent with user-managed access: A standard architecture for asynchronous, centralizable, internet-scalable consent. *2015 IEEE Security and Privacy Workshops*, 175-179. https://doi.org/10.1109/spw.2015.34

Martin, K. (2015). Privacy Notices as Tabula Rasa: An Empirical Investigation into how Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online. *Journal of Public Policy & Marketing*, *34*(2), 210–227. https://doi.org/10.1509/jppm.14.139

McGarrigle, J., Torrance, J., Quigley, M., & Dymond, S. (2026). Consent banners, dark patterns, and GDPR infringements in online gambling: Evidence from a systematic audit and online experiment. *Computers in Human Behavior Reports*, *23*, Article 101270. https://doi.org/10.1016/j.chbr.2026.101270

Meier, Y., & Krämer, N. C. (2022). The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels. *Communication Research*, 51(2), 178-202. https://doi.org/10.1177/00936502221102101

Merlec, M., Lee, Y., Hong, S., & In, H. (2021). A smart contract-based dynamic consent management system for personal data usage under gdpr. *Sensors*, 21(23), 7994. https://doi.org/10.3390/s21237994

Mohammed, N., Chen, R., Fung, B. C., & Yu, P. S. (2011). Differentially private data release for data mining. *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, 493-501. https://doi.org/10.1145/2020408.2020487

Narkedimilli, S., Sriram, A. V., & Raghav, S. (2024). *FL-DABE-BC:* A privacy-enhanced, decentralized authentication, and secure communication for federated learning framework with decentralized attribute-based encryption and blockchain for IoT scenarios. *arXiv*. https://doi.org/10.48550/arXiv.2410.20259

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent Pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-13. https://doi.org/10.1145/3313831.3376321

Siddiqa, A., Hashem, I. a. T., Yaqoob, I., Marjani, M., Shamshirband, S., Gani, A., & Nasaruddin, F. (2016). A survey of big data management: Taxonomy and state-of-the-art. *Journal of Network and Computer Applications*, *71*, 151–166. https://doi.org/10.1016/j.jnca.2016.04.008

Olca, E., & Can, O. (2022). DICON: A domain-independent consent management for personal data protection. *IEEE Access*, 10, 95479-95497. https://doi.org/10.1109/access.2022.3204970

OECD guidelines on the protection of privacy and Transborder flows of personal data. (2002). https://doi.org/10.1787/9789264196391-en

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Canada). https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Protection of Personal Information Act 4 of 2013 (South Africa). https://www.gov.za/documents/protection-personal-information-act

Resta, G. (2000). Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali. *Rivista Critica del Diritto Privato*, 2000, 299–320.

Toth, M., Bielova, N., & Roca, V. (2022). On dark patterns and manipulation of website publishers by CMPs. *Proceedings on Privacy Enhancing Technologies*, 2022(3), 478–497. https://doi.org/10.56553/popets-2022-0082

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

Tyler, A. R. B. (2022). *Can we still archive? Privacy and social science data archiving after the GDPR* (Publication No. 29999086) [Doctoral dissertation, University of Michigan]. Deep Blue Documents. https://deepblue.lib.umich.edu/handle/2027.42/175592

Ulusoy, O., & Yolum, P. (2020). Norm-based access control. *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, 35-46. https://doi.org/10.1145/3381991.3395601

Van Nortwick, M., & Wilson, C. (2021). Setting the bar low: Are websites complying with the minimum requirements of the CCPA? *Proceedings on Privacy Enhancing Technologies*, 2022(1), 608-628. https://doi.org/10.2478/popets-2022-0030

Wilkowska, W., Offermann, J., Colonna, L., Florez-Revuelta, F., Climent-Pérez, P., Mihailidis, A., Poli, A., Spinsante, S., & Ziefle, M. (2022). Interdisciplinary perspectives on privacy awareness in lifelogging technology development. *Journal of Ambient Intelligence and Humanized Computing*, *14*(3), 2291–2312. https://doi.org/10.1007/s12652-022-04486-5

Yang, R., Chen, X., & Fu, S. (2023). Unlocking privacy paradox in social media from a configurational perspective. *Proceedings of the Association for Information Science and*

Technology, 60(1), 1197-1199. https://doi.org/10.1002/pra2.990

Zhu, L., Zhao, B., & Peng, R. (2026). Blockchain-enabled federated learning: A survey on system design, key challenges, and future directions. *Electronics*, *15*(8), 1572. https://doi.org/10.3390/electronics15081572

Zimmeck, S., Goldelman, D., Kaplan, O., Brown, L., Casler, J., Jean-Charles, J., Champeau, J., & Harkous, H. (2024). Website data transparency in the browser. *Proceedings on Privacy Enhancing Technologies*, *2024*(2), 211–234. https://doi.org/10.56553/popets-2024-0048