frontiers | Frontiers in Political Science

TYPE Conceptual Analysis
PUBLISHED 09 December 2024
DOI 10.3389/fpos.2024.1391755

OPEN ACCESS

EDITED BY
Johanne Kübler,
Vienna University of Economics and Business, Austria

REVIEWED BY
Marc Jacquinet,
Universidade Aberta, Portugal
Ahmad Sururi,
Sultan Ageng Tirtayasa University, Indonesia

*CORRESPONDENCE
Soheil Human
✉ soheil.human@univie.ac.at;
✉ soheil.human@wu.ac.at

RECEIVED 26 February 2024
ACCEPTED 10 September 2024
PUBLISHED 09 December 2024

CITATION
Human S (2024) Humans [plural] in the loop: the forgotten collective aspects of privacy, consenting, controlling, and digital protection. *Front. Polit. Sci.* 6:1391755. doi: 10.3389/fpos.2024.1391755

Humans [plural] in the loop: the forgotten collective aspects of privacy, consenting, controlling, and digital protection

Soheil Human[1,2,3]*

[1]Department of Philosophy, University of Vienna, Vienna, Austria, [2]Sustainable Computing Lab, Institute for Information Management and Control, Vienna University of Economics and Business, Vienna, Austria, [3]Vienna Cognitive Science Hub, Vienna, Austria

The integration of digital technologies into various aspects of life is not only transforming industries and economies but also fundamentally altering human interactions and societal dimensions, raising critical ethical and societal concerns, particularly regarding human agency and human rights. Current approaches for addressing these concerns, particularly in the case of digital privacy, are predominantly "individual-centric", placing an undue burden on individuals who often lack the necessary knowledge and resources to protect their digital rights. This article argues for a paradigm shift toward human-compatible approaches by providing individuals with cognitive, collective, and contextual supports to empower them. The article redefines "humans in the loop" as a collective practice and expands the ongoing debates from "data protection" to the broader discourse of "digital protection." It proposes the establishment of novel sociotechnical mechanisms, such as the "Advanced Data Protection Control (ADPC)", within internet infrastructures to facilitate effective communication between users and stakeholders. This approach addresses the shortcomings of current practices dominated by service providers and advocates for innovative policy-making and technical advancements. By integrating collective supports with automation and other cognitive and contextual supports, the goal is to foster a sustainable and accountable digital future that ensures pluralism, inclusion, and human agency in the continuous co-creation, evaluation, and improvement of digital technologies.

KEYWORDS

human-compatibility, digital protection, data protection, consenting, Advanced Digital Protection Control, cognitive supports, contextual supports, collective supports

1 Introduction

The swift emergence and incorporation of digital technologies, along with other advancements, are revolutionizing various sectors and fundamentally transforming how people live and how environments and societies are structured. This transformation, while offering the promise of improved living standards, raises a plethora of ethical and societal concerns (Human et al., 2019). Central among these are the diminishing human agency and the potential violation of human rights, such as privacy rights, which are crucial in our democratic and decision-making structures (Zuboff, 2015, 2023). The shift in power dynamics poses a significant challenge to the concept of a meaningful human existence, raising critical questions about the role and impact of advanced digital technologies, particularly AI (see, e.g., Schröer et al., 2024), in both civilian and military domains.

Concerns also extend to the diminishing role and relevance of humans in an increasingly automated world, where advanced artificial systems are taking over significant aspects of daily life and decision-making processes. This shift raises profound questions about the safeguarding of human rights in a digital era. Furthermore, the emergence of generative AI and complex systems, along with the vast collection of personal data, has heightened concerns about *hyperpersonalized* targeting (see, e.g., Desai, 2022, for a discussion on hyperpersonalization from a solely marketing perspective). This form of targeting, used in strategies like targeted advertising and personalized content delivery, poses significant risks of manipulating public perception and behavior in relation to digital technologies.

In addressing the aforementioned societal and ethical concerns, it is imperative to recognize that while these issues are inherently *collective* and *societal*, the predominant methods employed to tackle them have been markedly *individual-centric*. This article advocates for *human-compatible* approaches that bolster individual capacity to safeguard their digital rights. These approaches encompass *cognitive*, *collective*, and *contextual* supports (Human and Cech, 2021). We contend that the concept of "humans in the loop" should be re-envisioned as a *collective*, rather than an *individual* practice. This perspective alleviates the undue burden placed on individuals, who often lack the requisite knowledge, expertise, capacity, time, and motivation to protect their digital rights effectively. Furthermore, this discourse should transcend the narrow confines of *data protection*. While integral, *data protection* is but one facet of a broader spectrum of *digital rights protection*.

We further discuss that current practices, which predominantly vest authority and decision-making power over data, procedures, and user interfaces involved in *digital protection* with service providers (referred to as *data controllers* under the European Union's *General Data Protection Regulation*), are inadequate. We then argue that for the implementation of *collective* approaches, it is essential to establish advanced digital protection *controls*[1] (technical specifications). These controls should facilitate innovative internet infrastructures that enable the appropriate and reliable communication of data, information, requests, and decisions between users and various stakeholders. This article explores how such a paradigm shift can influence policy-making in the realm of digital technologies. It emphasizes the importance of balancing *collective supports* with *automation* and other *cognitive supports* to shape a more equitable digital future.

2 Humans in the loop: misapplication in digital privacy and consenting

Privacy is one of the cornerstones of human rights (Council of Europe, 1950). In the realm of academia, digital privacy has garnered considerable attention, with research intensifying since the advent of the internet's commercial and widespread usage. Beyond scholarly pursuits, there has been a significant and continuous evolution in national and international guidelines and legal frameworks (e.g., Organisation for Economic Co-operation and Development, 1980; United States Congress, 1998; United Kingdom Government, 1999), particularly in Europe, where the emphasis is often placed on "data protection" (see, e.g., German Federal Government, 1977; European Parliament and Council of the European Union, 1995). This professional focus has been paralleled by a societal push toward heightened awareness of digital privacy issues. Central to this discourse (at least in Europe) is the concept of "keeping humans in the loop," a principle echoed in pivotal documents like the European Charter of Fundamental Human Rights (European Parliament and Council of the European Union and Commission of the European Communities, 2000) and the European General Data Protection Regulation (European Parliament and Council of the European Union, 2016). These documents underscore the importance of individual autonomy in managing personal data, emphasizing the role of *making decisions and giving consent*, as well as the ability to *revise* or *revoke* these decisions.

Despite these long-standing research and legal efforts, and the acknowledged importance of *human-compatible* approaches, the current state of digital privacy–after decades of interdisciplinary endeavors–is far from satisfactory (Zuboff, 2023; Human et al., 2022). The idea of "humans in the loop" has often been misinterpreted or exploited, leading to flawed privacy management mechanisms. These include the ubiquitous "cookie banners"—pop-ups that often present users with convoluted and misleading options for data collection consent. Such mechanisms frequently employ "dark patterns" designed to coerce consent or present information in a manner that is excessively complex and inaccessible to most users (Gray et al., 2021). This misalignment with the concept of *human-compatible* practices has been a subject of extensive debate in the academic field.

In the following, we first briefly discuss some of the existing challenges in the current practice of *individual management* of digital privacy and consenting, with a focus on the limitations faced by individuals. Next, we reflect on a *human-compatible* perspective toward digital privacy and consenting, accompanied by an overview of its constituent dimensions. We argue that considering the *collective* aspects as one of the crucial dimensions of *human-compatible* privacy and consenting practices—along with *cognitive* and *contextual* aspects—is essential. Approaches designated as "humans in the loop," which fail to adequately address these *collective* aspects and instead focus on "*individuals* in the loop," are insufficient for truly empowering individuals in managing their digital privacy and consenting. Such inadequacies

1 It is important to note that, as reflected in the title of this article, we advocate for the enhancement of *Digital Protection*, which, among other benefits, includes and leads to increased personal digital *control*. *Personal digital controlling* (as a *socio-cognitive-techno-legal* action) is a critical dimension of *digital protection*, emphasizing the empowerment of individuals to have meaningful control over managing their digital lives. However, as will be discussed later, we also explore "Advanced Data Protection *Control*" (ADPC) and other advanced 'control' mechanisms. The specific terminology used in the naming of the ADPC, such as 'control,' aligns with common conventions of naming technical specifications prevalent among computer scientists and privacy engineers. For instance, this usage of 'control' is similarly applied in terms like "Global Privacy Control" (GPC). It is important for the reader to distinguish between the former usage of 'control,' which aligns with common sense and its application in philosophy or social science, and the latter usage prevalent in computer science communities.

may inadvertently position these approaches as part of the prevailing problem rather than a viable solution.

2.1 Challenges of *individual* management of digital privacy and consenting

The current practice of digital privacy is highly *individual-centric*. Perhaps the most prominent example of this is the use of consent-obtaining banners (privacy notices or so-called "cookie banners") that appear when users attempt to visit a website. These consent-obtaining mechanisms typically include a substantial amount of information, often presented in multiple layers and linked to lengthy, legally written privacy policies or terms of use. Users are expected to individually engage with these mechanisms, regardless of their age, level of education or knowledge, attentiveness, or motivation, to make privacy-related decisions. Ideally, this process requires users to perceive the content, comprehend it, possess sufficient background knowledge to determine the best course of action, and make an informed decision (Human and Cech, 2021). However, research has demonstrated that this ideal scenario rarely occurs in practice. Individuals face numerous *highly interconnected* challenges and difficulties when interacting with consent-obtaining mechanisms due to various limitations and reasons, including:

2.1.1 Cognitive and informational factors

Individuals face significant challenges in managing their privacy due to a range of cognitive and informational barriers. Companies often leverage complex data analytics and algorithms that are beyond the comprehension of the average consumer. This complexity is continuously increasing due to the adoption of advanced data collection and processing technologies (such as AI), making it difficult for individuals to grasp how their data is being utilized. Additionally, many data collection practices, such as cookies and tracking pixels, operate without user awareness, complicating efforts to manage privacy effectively.

A major issue is the general lack of understanding among individuals regarding data collection, processing, and usage by organizations. But even when individuals attempt to understand the privacy practices of companies, "Privacy Policies" are typically lengthy and filled with legal jargon, deterring users from reading and understanding them, further diminishing their capacity to protect their privacy (Obar and Oeldorf-Hirsch, 2020). This lack of awareness and understanding about the extent and implications of data collection practices is exacerbated by variations in digital literacy among different demographics, particularly older adults and less tech-savvy individuals. Moreover, persistent surveillance and data profiling undermine individual autonomy by influencing behavior and decision-making. The *privacy paradox* illustrates this issue well: individuals express concerns about privacy but often fail to take actions to safeguard it (Schröer et al., 2024). This behavior should not be misconstrued as an indication that users do not value their privacy (Solove, 2021). However, continuous exposure to privacy threats can lead to *privacy fatigue*, where individuals feel overwhelmed and resign themselves to the inevitability of privacy violations (Choi et al., 2018). Over-reliance on technology and trust in service providers further compounds the problem, leading individuals to overlook potential privacy risks (Taddei and Contena, 2013).

Managing consent across various platforms and services is complex, resulting in consent fatigue and uninformed agreements. The proliferation of IoT devices and augmented and mixed realities in personal spaces increases the risk of privacy intrusions, as these devices often collect data continuously and transmit it to third parties (see, e.g., Zheng et al., 2018). Finally, even with strong personal privacy practices, data breaches and security failures at the organizational level can compromise individual privacy, even when these breaches occur, individuals are often unaware or unable to predict or react to them effectively (Hassanzadeh et al., 2021).

2.1.2 Social and economic factors

The business model of surveillance capitalism (Zuboff, 2023), where companies profit from personal data, inherently conflicts with privacy protection, making it difficult for individuals to manage their privacy. Companies often prioritize data monetization over consumer privacy, leading to practices that exploit user data without adequate transparency or consent. Additionally, social media platforms and employment requirements can pressure individuals to share personal information, while the social desirability of connectivity and networking often outweighs privacy concerns.

Algorithms and targeted advertising exploit behavioral biases, nudging individuals toward actions that benefit data harvesters rather than themselves. Furthermore, increasingly sophisticated social engineering and phishing attacks exploit human psychology, making it difficult for individuals to protect their personal information. While these challenges exist, privacy-enhancing technologies (PETs), which are intended to support users, are often costly and not considered a fundamental infrastructure necessary to enable all individuals to protect their human rights, which should be provided to everyone as a public service, thereby rendering them inaccessible to individuals with lower economic resources (along with those with limited motivation, knowledge, expertise, or awareness).

2.1.3 Regulatory factors

Most privacy and data protection regulations are currently *individual-centric* by nature, leaving users to deal with their privacy on their own despite the cognitive and social factors that limit their ability to practice their digital rights. Additionally, inconsistent data protection regulations across jurisdictions make it challenging for individuals to manage their privacy effectively. Even in regions with robust privacy laws, enforcement is often weak (Chander et al., 2021), leaving individuals vulnerable to privacy invasions and misuse. This regulatory gap exacerbates the difficulties individuals face in protecting their privacy, underscoring the need for comprehensive and enforceable privacy protections worldwide.

In conclusion, individuals face a myriad of cognitive, informational, social, economic, and regulatory challenges in managing their privacy. The interplay of these factors creates a complex environment where maintaining privacy requires not

only personal vigilance but also systemic changes in how data is collected, processed, and protected.

2.2 A perspective toward human-compatible digital privacy and consenting

To conceive a *human compatible* approach to digital privacy and consenting, it is essential to revisit our understanding of "humans"—their needs, perceptions, decision-making processes, and behaviors—in the context of digital technology interaction (Watkins and Human, 2023; Human and Watkins, 2023). Contemporary *cognitive science* perspectives, such as *4E Cognition* (Newen et al., 2018; Varela et al., 2017; Newen et al., 2018), suggest that human cognition, decision-making, and actions are context-dependent, influenced by both *individual* and *collective* factors—among others. This also applies to interactions with digital technologies. For an approach to digital privacy to be truly *human-compatible* and empowering, it must encompass the individual end-user's needs, values, capabilities, expertise, motivation, and limitations, as well as the broader socioeconomic context and the nature of the technology they engage with (see also Human and Cech, 2021). Only by considering these diverse dimensions can we achieve genuine empowerment of individuals in the digital realm (Human et al., 2020). A *human-compatible* approach, therefore, involves integrating the *individual* (*cognitive*) and *social* (*collective* & *contextual*) aspects of users when designing, implementing, evaluating, and maintaining information systems—in this case, privacy management and consent-obtaining mechanisms. Viewing *humans* as *cognitive systems enacting* within their *socio-contextual environments* offers a framework for empowering them, taking into account their *sociocognitive* needs, values, capabilities, and limitations. This perspective is not only crucial in designing new consent-obtaining mechanisms, and supporting mechanisms such as "Personal Data Protection and Consenting Assistant Systems" (see Human et al., 2022) but also provides a benchmark for evaluating existing ones on the internet (see, e.g., Human and Cech, 2021). Without this *human-compatible* lens, which acknowledges the multi-dimensionality of human actions (or enactions), efforts toward developing empowering technologies, including privacy management or consent-obtaining mechanisms, will likely fall short of their intended goals—as it is echoed in numerous scholarly publications that address prevailing challenges in the field.

2.2.1 Cognitive aspects of privacy management and consenting

In the realm of digital privacy and consenting management systems, the cognitive demands placed upon users are multifaceted and substantial. These systems require users to engage in a series of complex cognitive processes (see, e.g., Zhu et al., 2023) including, but not limited to, attention, perception, memory recall, comprehension, anticipation, decision-making, and the articulation of these decisions. The efficacy of these processes is intrinsically tied to an array of personal factors such as the individual's needs, values, attention span, motivation, expertise, capabilities, temporal constraints, and inherent limitations. Given the intricate nature of consent-obtaining mechanisms, one might legitimately question the capacity of an average individual to adeptly navigate these tasks, considering the constraints of finite cognitive resources and limitations in time, expertise, knowledge, and other capacities (Human and Cech, 2021). As subsequent sections will elaborate, the systemic structure inherent in current digital privacy practices further impedes the provision of adequate support to users. This support is crucial for users to fully comprehend privacy-related information, including the nuances of how their personal data is collected, shared, and utilized, and to understand the ramifications thereof for themselves and others. Users should possess the capability, a capability that regrettably remains lacking in prevailing practices[2], to make well-informed decisions regarding privacy requests. Furthermore, they should retain a lucid recollection of these decisions and consents, enabling facile access for future revisions, adjustments, or revocations (Human et al., 2022). In instances where exigency dictates, users ought to be able to *automate* (Human and Wagner, 2018; Human et al., 2022) these tasks or engage the support of peers or expert organizations (i.e., *collective supports*).

2.2.2 Contextual aspects of privacy management and consenting

The process of making privacy decisions and granting consent is inherently context-dependent (Human and Kazzazi, 2021). This context is co-constructed by a confluence of factors, including the prevailing digital technology, the user's surrounding environment, and their mental state. The relevance and legitimacy of privacy decisions and consents are closely tied to the particular circumstances in which they are made. For example, in a situation of urgency, a user may opt to divulge sensitive information, or a decision regarding privacy may be valid only for a specific duration and for a designated purpose. Current practices in the realm of digital privacy often fail to account for the critical aspect of context. The mechanisms employed for facilitating privacy decisions and obtaining consent are usually uniform across varying contexts, lacking *contextual* sensitivity. Moreover, these decisions and consents are rarely linked to a specific context, leading to ambiguities for users concerning the extent and duration of their privacy commitments. Addressing the *contextual* aspects, as well as the cognitive challenges associated with guiding users through these *contextual* complexities, are significant tasks, considering the entrenched systemic structures of privacy management and consent acquisition that are prevalent today. These issues will be discussed further in subsequent sections.

2.2.3 Collective aspects of privacy management and consenting

The *collective* aspect of privacy and consenting, arguably one of the most overlooked dimensions, exhibits significant diversity. This facet merits in-depth exploration, particularly in the context of the interconnected nature of *individual* and *collective* privacy concerns in the digital era. In examining the *collective* aspect

2 This aspect warrants critical examination within the present context.

of privacy and consenting, it is pivotal to consider the inherent social nature of *humans* as *cognitive systems* (Augoustinos et al., 2014). The influence of the social environment on knowledge acquisition, value perception, and behavioral patterns is substantial (Frith, 2008). This influence extends to the realm of privacy perception and decision-making (Granovetter, 2018). Empirical research substantiates the notion that an individual's privacy settings are often aligned with those prevalent in their community or social group. Such findings underscore the significance of social conformity and group norms in shaping privacy-related choices (Das et al., 2015; Emami Naeini et al., 2018).

However, the complexity of privacy extends beyond *individual-centric* notions. Privacy, while ostensibly personal, exhibits numerous *collective* and *socially centered* dimensions. A salient example of this is the sharing of personal data not exclusively owned by the user (Lehtiniemi and Kortesniemi, 2017). Instances where applications request access to a user's contact list illustrate this point. The data shared, such as names, telephone numbers, and email addresses, predominantly belong to third parties. Legally and ethically, the individual sharing this information may lack the requisite authority to make such decisions on behalf of others. This raises profound questions about the ethics of consenting and the boundaries of individual autonomy in the context of digital data sharing.

Moreover, the issue of privacy and consenting acquires additional layers of complexity when considering vulnerable groups such as children or LGBTQIA+ communities (Marwick et al., 2018). In the case of children, the responsibility for decisions regarding online privacy and consenting often falls to parents or guardians. This aspect highlights the *collective responsibility* in safeguarding the digital privacy of minors, a responsibility that extends beyond the immediate family unit to encompass broader societal and legal frameworks.

Finally, the aggregate data collected and the profiles created about individuals have implications that transcend personal boundaries (Human et al., 2019). The potential use of this data to influence behaviors, ranging from consumer habits to political voting patterns, represents a form of *collective impact*. Such phenomena do not merely affect individuals but can shape societal trends and norms.

In conclusion, the discourse on privacy and consenting in the digital era necessitates a comprehensive understanding that encompasses both *individual* and *collective* perspectives. It requires an acknowledgement of the social nature of human beings, the ethical implications of data sharing, the special considerations for vulnerable groups, and the broader societal impacts of data-driven behavioral influence. The exploration of these themes offers fertile ground for further academic inquiry and contributes to a more nuanced understanding of privacy and consenting in the contemporary digital landscape.

2.3 Humans in the loop: solution or part of the problem?

Within the ambit of various ethical and legal frameworks, notably the European Charter of Human Rights (European Parliament and Council of the European Union and Commission of the European Communities, 2000), there exists a fundamental tenet that the rights of individuals–pertaining to privacy, agency, and informed consent–must be safeguarded. This necessitates the empowerment of individuals, enabling them to exercise these rights effectively and to assert control over their privacy and online choices in a substantive manner. Regulations such as the European General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union, 2016) have been promulgated to underpin and facilitate the exercise of these rights. Nevertheless, there are critical shortcomings in the implementation of such regulations. Firstly, these regulations are primarily predicated on an *individual-centric* viewpoint, often neglecting the inherent human nature and the imperative to develop privacy practices that are congruent with human compatibility. Secondly, the vested interests of numerous large technology corporations often clash with the realization of *human-compatible* privacy and consenting practices (Zuboff, 2015, 2019).

As a consequence of these lacunae, the recent years have witnessed the emergence of mechanisms for obtaining consent and managing privacy, such as "cookie banners" (Degeling et al., 2018) and "paywalls" (Morel et al., 2022), which are fraught with problems. While ostensibly acknowledging human agency, these mechanisms frequently employ deceptive designs, coaxing individuals into behaviors that disproportionately benefit these corporations, such as data sharing or acquiescing to profiling, tracking, or data transfers (Santos et al., 2019). This exemplifies a scenario where the intrinsic nature of human decision-making in privacy and consenting, along with the *cognitive*, *collective*, and *contextual* dimensions of these *sociocognitive* actions, are either inadvertently overlooked, deliberately neglected, or exploited (Human and Cech, 2021). Consequently, the inclusion of "humans in the loop" in such processes merely transfers the onus onto individuals who are ill-equipped to navigate and safeguard their privacy and consenting rights adequately (Human et al., 2022).

The forthcoming sections will commence with a reflective analysis of this issue, particularly focusing on its impact on underprivileged populations. The argument will be extended to assert that this challenge transcends the confines of privacy and consenting, representing a broader dilemma in digital protection and control within our society. Subsequently, the discussion will explore potential avenues to reintegrate and maintain "humans in the loop" in manners that are truly *human-compatible*, thereby aligning technological processes with the innate characteristics and needs of individuals.

2.4 Diversity and inclusion matters

Digital technologies are utilized across a broad spectrum of user types, each within varied contexts and environments. This diversity underscores the critical need to address *human-compatible* aspects of privacy and consenting. The urgency of this consideration amplifies when addressing the needs of diverse user groups.

For example, children, from a legal and ethical standpoint, require specific support in terms of privacy and consenting (Brown and Pecora, 2014). However, current digital platforms and the

broader ecosystems in which they are integrated often neglect these rights and needs. Typically, children encounter the same methods for obtaining consent and managing privacy as adults, devoid of any mechanism for guardian involvement. Similarly, elderly individuals and those with disabilities often require assistance in managing their privacy and consenting, yet there is a conspicuous absence of supportive mechanisms tailored to their needs (Tao and Shuijing, 2016; Maaß, 2011). Furthermore, immigrants and individuals lacking proficiency in the language of local websites represent another overlooked group. Given the limitations in human cognitive capacity, knowledge, expertise, motivation, and time, virtually everyone, including experts, needs support in managing privacy and consenting matters.

It is imperative to recognize that different contexts necessitate varying types of support. The prevailing "one-size-fits-all" or, more accurately, 'one-size-fits-always-all,' approach, which lacks *cognitive*, *collective*, and *contextual* adaptability, is evidently inadequate. This underscores a profound need for the adoption of more sophisticated, *human-compatible* data protection and consenting practices.

3 The pressing urgency: from data protection to digital protection

The discourse on data protection and digital privacy is not a novel phenomenon but has a rich and extensive history. Tracing back to the earliest legal frameworks dedicated to privacy concerns, one can highlight the Hessian Data Protection Act of 1970 (Hessian Parliament, 1970) and the German Federal Data Protection Act of 1977 (German Federal Government, 1977) as pivotal moments in formally recognizing the importance of data privacy. The Hessian Act, the first of its kind at a regional level, set the stage for broader legislative efforts, while the 1977 Federal Act, advanced for its time, acknowledged the increasing relevance of personal data in the digital age and set a precedent for many subsequent laws worldwide. Together, these pieces of legislation emphasized the need to regulate the processing of personal data by public and private entities, underlining a growing awareness of the intrinsic value and vulnerability of personal data.

This discourse, however, transcends mere legal frameworks. It extends into the realms of philosophical inquiry, scholarly research, and technological developments. Scholars in fields as diverse as ethics, law, and computer science have long debated the implications of data collection and usage. Philosophical discourses dating back to the early 20th century have pondered the implications of technology on privacy and individuality, reflecting a longstanding engagement with these issues. The rise of the internet and digital technologies has only amplified these concerns. For instance, the development of early encryption technologies in the late 20th century was not merely a technological breakthrough but also a response to the growing need for data security and privacy. These examples serve to illustrate that the concern for data protection and privacy is deeply rooted in a multifaceted historical context.

Particularly in Europe, there has been a pronounced focus on the *data* itself, exemplified by the widespread adoption of the term "data protection". This terminology reflects a certain perspective that prioritizes the safeguarding of data. However, if the ultimate objective of these legal, ethical, scholarly, and technological efforts is the protection of human rights, then a sole focus on data protection may prove insufficient. Human rights encompass a broad spectrum of freedoms and protections, of which *data protection and privacy* is but one aspect. Recognizing the interconnectedness of these rights, it becomes clear that an exclusive concentration on "data protection" could inadvertently neglect other critical human rights concerns.

The importance of protecting personal data to empower individuals to enforce their legal rights and maintain control over their personal information is undeniable. However, it is crucial to acknowledge that the protection of data is not an end in itself but a means to safeguard broader rights. Personal data can be utilized for a range of beneficial or detrimental purposes. Extensive research has demonstrated how personal data manipulation can have adverse effects on both individuals and societies (Zuboff, 2015, 2019). An overemphasis on data protection, while necessary, can obscure the need to address the broader implications of how data is used and its potential to infringe on other rights.

The significance of this discussion is amplified when considering the recent advancements in artificial intelligence, complex modeling, and substantial computational power. With these technologies, companies are now capable of developing detailed profiles and models of individuals, a practice unimaginable in earlier decades. This era is not merely about categorizing individuals into user segments but about creating highly personalized profiles and services (see, e.g., Desai, 2022). Concepts like "digital twins" (de Kerckhove, 2021) illustrate the extent of detail in these practices. While these technologies offer innovative and ethical possibilities, their potential for misuse presents unprecedented challenges, far exceeding the problematic practices of the past.

Furthermore, the application of advanced software and models is part of a broader trend involving the deployment of new technologies in novel environments. From the Internet of Things (IoT) to wearable technology and pervasive computing, humans are increasingly immersed in digital environments. These developments add new dimensions to human interaction with technology, reducing the prevalence of digital-free spaces. The resultant abundance of personal data heightens the potential for new forms of manipulation, challenging the very notion of human agency.

In light of these developments, any discourse focused on keeping humans in the loop of decision-making must acknowledge that addressing these issues requires more than a narrow focus on *data protection*. The concept of "digital protection" is proposed, encompassing data protection but extending beyond it to safeguard the full spectrum of digital rights. This approach recognizes the multifaceted nature of the challenges posed by digital technologies and the need for comprehensive solutions that protect all aspects of digital rights.

This issue is particularly pressing as humanity stands on the cusp of technological advancements that will profoundly shape its future. If a shift in perspective toward a more inclusive understanding of digital protection is not widely adopted by academia, policymakers, and practitioners, there is a risk of developing infrastructures, ecosystems, and practices with

long-lasting impacts that may be detrimental and challenging to reverse. To effectively actualize *human-compatible* approaches in digital protection, it is imperative to engage comprehensively with the *cognitive*, *contextual*, and *collective* aspects. This article underscores the critical need for a holistic approach that encompasses all facets of digital rights. Such an approach ensures that human considerations are at the forefront in the rapidly evolving digital landscape. The discourse insists on the integration of these aspects in both the development and implementation of digital technologies, advocating for a paradigm that prioritizes *human-compatible* considerations in this dynamic field.

4 Humans [plural] in the loop: systemic changes needed

The discourse in preceding sections first established a *human-compatible* perspective on digital privacy and consenting. This framework emphasizes the *collective* dimension, tandem with *cognitive* and *contextual* dimensions, of data protection and consenting, highlighting a significant lacuna in current practices, in which *individual users* are often isolated in managing their privacy, lacking ongoing *collective support*. Acknowledging the imperative of incorporating humans in the decision-making loops, the narrative underscores a pivotal critique: current approaches, while purporting to include "humans in the loop," often adopt an excessively *individual-centric* stance. This myopic view overlooks the intrinsic nature of humans as *collective cognitive entities*, along with their specific needs, limitations, and capabilities. Such approaches, under the guise of *human-centricity*, inadvertently contribute to the very issues they aim to ameliorate. Thus, the article advocates for a paradigm shift toward practices that foster *collective*, *cognitive*, and *contextual supports* for individuals. This is particularly pertinent for vulnerable social groups such as children, the elderly, people with disabilities, and those with linguistic barriers, such as immigrants. For these groups, providing *collective support* is not merely beneficial but an ethical and legal imperative to uphold their digital rights, especially in the context of burgeoning AI advancements, personalization, and the proliferation of digital technologies in various life domains, including IoT and mixed reality.

Moving beyond mere advocacy for *human compatible digital protection and controlling practices* with a focus on *collective* dimensions, this section embarks on a critical analysis of current *data protection and consenting practices*. The inquiry delves into how *cognitive*, *collective*, and *contextual supports* can be extended to users, and identifies the systemic shifts necessary for this transformation.This analysis narrows its focus from the broader concept of "digital protection" to specifically examine *current* data protection and consenting practices, which are the primary areas of emphasis within digital protection at present.

In the ensuing analysis, it becomes apparent that the current paradigm governing data protection and consenting processes is predominantly skewed toward *data controllers*. These entities exercise exclusive control over data, procedures, and user interfaces, effectively marginalizing users from any meaningful involvement. This systemic imbalance deprives users of control and fails to furnish them with copies of information they receive/disclose or decisions they make. Such a framework egregiously undermines the ability of individuals to retract consent, as tracking and recalling their consent becomes a herculean task.

A fundamental deficiency in the existing setup is the absence of widely adopted *Internet protocols* (Degeling and Human, 2023) that facilitate bidirectional communication of data, information, requests, and decisions between users and various stakeholders. This gap denies users equitable control and impedes the integration of data and user interfaces with supportive software and mechanisms on the user's side.

The proposition here is the development and implementation of Advanced Digital Protection Controls (such as Human, 2022a). These would comprise communication protocols and socio-cognitive-techno-legal mechanisms that enable the exchange of data, information, requests, and decisions between *individuals* and a spectrum of other parties, ranging from *data controllers* to trusted auxiliary entities. Furthermore, the proposed controls would encompass *cognitive*, *collective*, and *contextual support mechanisms*, which are vital for restructuring the current power dynamics on the Internet. This paradigm shift is necessary to counter the *individual-centric* and problematic approaches to data protection and consenting that currently prevail. In essence, the establishment of such mechanisms is pivotal not only for realizing "human-compatible data protection" practices but also for safeguarding and actualizing other digital rights, extending beyond the realms of *privacy and consenting* to realize "human-compatible digital protection".

4.1 Who is controlling the *data* concerning privacy and consenting?

Various legal frameworks, such as the General Data Protection Regulation (GDPR) of the European Union, mandate that *data controllers* must provide *data subjects* with essential information regarding privacy and consenting. These frameworks necessitate securing consent or privacy-related decisions through legitimate and ethical means. Typically, this is achieved through mechanisms like "cookie banners" (Degeling et al., 2018). However, studies indicate that these mechanisms often lack transparency, comprehensibility, and ethical standards (Utz et al., 2019; Human and Cech, 2021; Santos et al., 2019), leading to the control over *data concerning users' privacy and consenting* remaining exclusively with the *data controllers*. This lack of reciprocity places *data subjects* in a disadvantaged position, without any *records* of their decisions or the information provided to them (Jesus, 2020). The imbalance in data governance impacts *data subjects*' autonomy in digital environments, as they lack control over their *personal data protection and consenting records*. This undermines trust in digital services and exacerbates the power imbalance between *data controllers* and *subjects*.

Advanced Digital Protection Control mechanisms (such as Human, 2022a) could enhance transparency and user empowerment by providing a more nuanced approach to managing *consent and privacy data*. Features enabling users to access a comprehensive history of their consent

decisions and data usage could significantly mitigate current challenges in digital governance, offering greater visibility and control over their data related to their privacy and consenting.

4.2 Who is controlling the *procedures* concerning data protection and consenting?

Currently, *data controllers* have complete authority over procedures in data protection and consenting, including the timing and nature of *privacy/consent-obtaining "pop-ups"*. This control enables them to tailor these procedures to their advantage, often making consenting via a *consent banner* the simplest option, while revoking consent remains complex and obscure. Advanced Digital Protection Control mechanisms can empower *data subjects* with autonomy over *data protection and consenting procedures*, enabling them to initiate or modify these processes. Such autonomy allows *data subjects* to independently start communication processes with *data controllers* or selectively respond to requests, fostering a more equitable balance between *data subjects* and *data controllers*.

There is a need to reevaluate and redesign the procedural aspects of data protection and consenting mechanisms, emphasizing *human-compatible* procedures. By enabling *cognitive*, *contextual*, and *collective* supports, Advanced Digital Protection Control mechanisms could simplify and enhance data protection and consenting procedures, thereby reducing cognitive burden, empowering individuals, and improving the overall user experience.

4.3 Who is controlling the *user interfaces and designs* concerning data protection and consenting?

Data controllers currently dictate every aspect of user interfaces in privacy and consenting mechanisms, leading to the deployment of manipulative tactics, known as *dark patterns*, within *consent banners* (Nouwens et al., 2020). Advanced Digital Protection Control mechanisms could transfer control of these interfaces to users (i.e., on the user-side, e.g., on the browsers or operating systems) and their trusted intermediaries, thereby diminishing the prevalence of *dark patterns* in digital privacy and consenting mechanisms.

The various forms of *dark patterns* significantly impact user experience and decision-making. Their design can lead to decision fatigue, reduced autonomy, and compromised privacy. Advanced Digital Protection Control mechanisms are instrumental in encouraging the development of standardized, user-friendly interfaces that prioritize clear communication and ease of use. Furthermore, involving independent bodies in the design and review of these interfaces ensures alignment with ethical standards and best practices in user experience design.

4.4 The imperative for advanced digital protection, consenting and controlling communication mechanisms

Given the concerns highlighted previously, it becomes evident that in the current paradigm, almost all elements including design, processes, data, and interfaces are not only governed by *data controllers* but are also implemented on *their* platforms. For instance, a "cookie banner" displayed on a *data controller*'s website encapsulates all interactions within its domain. When a user engages with such an interface, say, by providing consent, there is a notable absence of any receipt, confirmation, or data correlating to the information presented to them and the decisions they make. This deficiency hinders the development of *cognitive*, *collective*, or *contextual support mechanisms* for the user. A pivotal component of such mechanisms is the communication means that facilitate the exchange of information, data, requests, and decisions *concerning digital protection, consenting, and controlling* (Degeling and Human, 2023). The implementation of these mechanisms can usher in standardized user interfaces, integrated within operating systems, browsers, and applications, potentially replacing the traditional cookie banners and placing control back in the hands of users. Furthermore, many decision-making processes could be automated, granting users the ability to store, update, and revoke their previous decisions as needed. Depending on the context, various aspects of the digital protection mechanism can be tailored.

Crucially, such communication mechanisms can enable the provision of *collective support*. Trusted experts, organizations, friends, and family members can assist users in safeguarding their digital rights. This is particularly pertinent for children and members of other vulnerable groups who require continual support and can now be effectively empowered and supported by their guardians. The technical intricacies of such mechanisms, including the Advanced Data Protection Control (ADPC), have been expounded upon in other works (see, e.g., Human, 2022a).

By enhancing the autonomy and control of users over their digital interactions and personal data, these advanced mechanisms not only address the current inadequacies but also lay the groundwork for more equitable digital environments. This is a step toward democratizing digital protection, ensuring that every individual, irrespective of their technical acumen or societal status, can exercise meaningful control over their digital lives. The implications of such a shift are profound, extending beyond mere compliance with legal frameworks to fostering a culture of respect and responsibility toward humans' digital rights in the digital realm.

5 The advanced data protection control

In the preceding section, we elucidated that the absence of prevalent, *bidirectional*, and *human-compatible* communication mechanisms concerning *digital protection*–particularly in relation to privacy and consenting data, meta-data, information, requests, preferences, and decisions–coupled with factors such as the business models or conflicts of interest of *data controllers* and

browser companies, has led to a dominant paradigm of online privacy and consenting. Within this paradigm, the fundamental components, including *data*, *procedures*, and *user interfaces*, are predominantly designed, developed, maintained, and controlled by the *data controllers*. This imbalance of power can have significant societal repercussions (Human et al., 2019). The Advanced Data Protection Control (ADPC) seeks to address this core issue by implementing the missing communication mechanism. The technical specification of the ADPC is available at https://www.dataprotectioncontrol.org.

ADPC should not be seen merely as an isolated technical solution, but as a socio-cognitive-techno-legal solution embedded within the complex ecosystem of digital protection. As with any socio-cognitive-techno-legal solution, the ADPC necessitates support from diverse interdisciplinary perspectives to be adopted, achieve its transformational goals, and undergo continuous improvement. Consequently, it is imperative that the foundations of the ADPC be articulated in a comprehensible manner to non-technical experts to foster the development of future multidisciplinary solutions through collaboration across various fields. To this end, the following section is structured around key potential interdisciplinary questions regarding the ADPC, aimed at informing the non-technical audience of this article about the ADPC.

5.1 What is the ADPC?

The Advanced Data Protection Control (ADPC) is a technical specification, complemented by its associated socio-cognitive-techno-legal solutions, designed for communicating data protection and consenting data, meta-data, information, requests, preferences, and decisions. For example, the ADPC specification details automated methods enabling *data subjects* (such as website visitors) to: 1) grant or deny consent for specific purposes delineated by the *data controller*, 2) withdraw previously given consent, and 3) object to processing for direct marketing purposes based on the *data controller*'s claimed *legitimate interest*. This empowers users to manage data protection decisions through their web browser (or other means such as operating system interfaces or mobile apps) and potentially customize how requests are presented and managed (e.g., via a browser extension to import or specify lists of trusted websites). This system is analogous to how websites request permission to access a webcam or microphone through a browser: the browser tracks the user's decisions on a site-by-site basis, ensures the user maintains genuine autonomy in their choices (e.g., without *dark patterns*), and empowers the user to *control* their decisions.

5.2 How does ADPC work?

The ADPC specification delineates a mechanism for articulating user decisions regarding personal data processing in compliance with European Union data protection regulations and similar regulations outside the EU. This mechanism functions by exchanging HTTP headers between the user agent and the web server, or through an equivalent JavaScript interface (or Bluetooth in the case of ADPC-IoT). Future expansions may incorporate additional protocols and technologies for transmitting *ADPC signals*.

This mechanism allows users to grant or refuse consent, withdraw consent, and object to processing, among other actions. It offers an alternative to existing non-automated consent management methods (e.g., *cookie banners*) and aims to reduce the effort required from all parties involved in managing and protecting users' privacy, while also ensuring compliance with regulations and ethical expectations.

5.3 What are the legal foundations of the ADPC?

In addition to the Charter of Fundamental Rights of the European Union, as cited in the ADPC specification (Human et al., 2021), various legal frameworks, such as the EU's General Data Protection Regulation (GDPR) and the ePrivacy Directive, define the rights and obligations surrounding personal data processing in the European Union[3]. The GDPR stipulates that personal data processing is only lawful if it has an appropriate legal basis, one being that "the data subject has given consent to the processing of his or her personal data for one or more specific purposes" (Article 6(1)(a) GDPR). Similarly, the ePrivacy Directive [Article 5(3)] requires user consent for storing or retrieving any data from terminal equipment beyond what is strictly necessary. Furthermore, when a *data controller* relies on claimed *legitimate interest* for direct marketing, the user has an unequivocal right to *object* under Article 21(2) GDPR.

Currently, website publishers often seek to process visitors' personal data for purposes beyond what is necessary to serve the website and beyond what can be justified by legitimate interest. They frequently ask for visitor consent via intrusive and repetitive interfaces embedded in web pages (e.g., "cookie banners") rather than through browsers or automated channels. However, users can choose how to communicate their GDPR rights to *data controllers*—via email, letter, or website button clicks. Additionally, technical means are permissible: Article 21(5) GDPR explicitly states that "the data subject may exercise his or her right to object by automated means using technical specifications." Recital 32 of the GDPR clarifies that requesting and giving consent can take many forms, including "ticking a box when visiting an internet website, [or] choosing technical settings for information society services," provided it is informed and unambiguous. Recital 66 of Directive 2009/136/EC, which updates the 2002 ePrivacy Directive, likewise states that "the user's consent to processing may be expressed by using the appropriate settings of a browser or other application." Despite various legal provisions suggesting its validity, standardized methods for communicating GDPR rights have thus far been lacking.

3 The ADPC can also be used to manage privacy and consenting under non-European legal frameworks.

5.4 What makes the ADPC "*Advanced*"?

There have been previous attempts to implement automatic privacy controls, such as the "Do Not Track"[4] (DNT) and its recent adaptation, the "Global Privacy Control"[5] (GPC) (Zimmeck and Alicki, 2020). The ADPC distinguishes itself by better integrating with the requirements of GDPR, and other international laws:

- The ADPC is domain-specific, enabling users to tailor their interactions with different websites and *data controllers*.
- The ADPC accommodates opt-in (consenting) and opt-out (objection, withdrawing consent, updating decisions) signals, whereas other signals (e.g., DNT or GPC) were based on an opt-out framework.
- The ADPC permits domains to define consent requests or use formulations standardized by industry groups (such as the IAB's TCF specification), making it open and interoperable with other systems.
- The ADPC supports general signals (e.g., "reject all", "withdraw all", "object to all", "do not track", "do not sell"), specific signals (e.g., consent to a specific request), and combinations of general and specific signals (e.g., "reject all, but consent to requests 'x' and 'y").
- The ADPC allows browsers, plugins, or operating systems to provide users with settings and logic for managing requests. This includes white- and blacklisting, industry-wide purposes, or logic such as showing a request only when visiting a page regularly.
- The ADPC reduces the *legal fingerprinting* surface by not sending any signal if a domain does not support the ADPC (thereby publicly committing not to use the signal further) and sending different signals to different domains.
- The ADPC can be used in different environments such as the web, IoT, augmented reality, and potentially any other environment that data exchange is occurring.
- The ADPC enables decentralized or centralized data protection and consenting management.
- The ADPC enables providing *collective support* to users (a short reflection on this can be found below).

5.5 Does the ADPC provide its own vocabulary?

The ADPC is not constrained to any specific vocabulary (ontology). It can be utilized with various vocabularies depending on the sector, use case, and legal requirements. Nevertheless, the ADPC can be complemented with standardized vocabularies, e.g., Pandit et al. (2019).

4 https://www.w3.org/TR/tracking-dnt/

5 https://globalprivacycontrol.github.io/gpc-spec/

5.6 Who can initiate the procedure?

As previously discussed, the *power* to initiate the communication of privacy and consenting data and decisions is a critical factor shaping the dynamics of online personal data processing. *Privacy signals* like the DNT or the GPC enable users to send a single binary message to *data controllers* regardless of their consent-obtaining mechanisms. In contrast, current consent-obtaining mechanisms, such as *cookie banners*, give *data controllers* full control over initiating the procedures. The ADPC, however, provides a bidirectional mechanism allowing either party to start the communication. For instance, a data subject can send a withdrawal request without waiting for the *data controller*'s query, or a *data controller* can send a set of requests to a data subject to initiate the procedure—both are possible.

5.7 Who determines the user interface design?

A significant advantage of the ADPC is that it transfers the representation and decision-making mechanisms to the *user-side*. Depending on the implementation, the user, browser companies, operating system developers, app or plugin developers, or trusted actors can decide on (or design) the representation and decision-making mechanisms. Consequently, ADPC-based user interfaces, if designed in a Human-compatible, Accountable, Lawful, and Ethical (HALE, Human, 2022b) manner, can mitigate (or eliminate) the use of problematic nudging mechanisms (e.g., *dark patterns*) in privacy-related solutions by shifting control from *data controllers* to *data subjects* (or their trusted parties).

5.8 Is the ADPC limited to the web?

Currently, the ADPC supports HTTP and JavaScript, making it applicable in browsers and potentially in web apps, mobile apps, and other solutions (from smart TVs to various IoT devices) based on these technologies. However, the ADPC aims to support other technologies in the future. For instance, the Sustainable Computing Lab (https://www.sustainablecomputing.eu) is leading projects to extend the ADPC to *IoT* and *Mixed Reality* devices and environments using *Bluetooth* and other protocols.

5.9 What distinguishes the ADPC from GPC or DNT?

Do Not Track (DNT) and Global Privacy Control (GPC) are binary HTTP header *signals* developed based on an approach to online privacy aligned with California's legal framework, such as the California Consumer Privacy Act (CCPA). The ADPC, conversely, is a *bidirectional advanced communication mechanism* capable of conveying various types of information and decisions related to privacy and consenting. While the

ADPC can generate binary signals similar to DNT or GPC, it is not confined to this function. Although designed with European laws in mind, the ADPC is adaptable to any legal framework.

5.10 How can the ADPC contribute toward human-compatible data protection?

Empowering users by bringing *privacy and consenting data* to the *user-side* and involving them in controlling the procedures and designs of personal data processing is crucial. However, users, as *human beings*, possess limited cognitive capacities, knowledge, expertise, time, and motivation to manage their privacy independently. They require *empowerment* (Human et al., 2020) through socio-cognitive-techno-legal means, such as Personal Data Protection and Consenting Assistant Systems (PDPCAS) (Human et al., 2022), which provide *cognitive*, *collective*, and *contextual* supports (Kirchner et al., 2019; Human and Kazzazi, 2021). These systems can offer users automation tools, management tools, memorization tools, and trust assessment tools, among others. Additionally, users can be supported through *whitelists* or *blacklists*, aiding them (or their *agents, i.e., their PDPCASs*) in interacting with online services or making privacy-related decisions more easily. The development of PDPCASs or other supporting tools is nearly impossible without the ADPC (or similar mechanisms) since such systems require access to *privacy and consenting data* (i.e., *data concerning privacy and consenting*) and must be involved in the *procedures* to function.

5.11 What about the *collective* dimensions?

Digital protection is a complex and demanding task that necessitates support for almost everyone. Specific groups, such as children, the elderly, individuals from underprivileged social backgrounds, and people with disabilities, require even more assistance. Yet, in the current *digital world*, nearly everyone, regardless of their age or need, is left to manage their own online digital protection independently. The ADPC enables bringing "humans (plural) in the loop." For instance, ADPC-Kids, while interacting with children to keep them informed in an age-appropriate manner, can forward privacy-related requests sent by *data controllers* to the children's guardians (e.g., parents) for decision-making. This mechanism can also provide any user with institutional support from NGOs or other experts, either on demand or globally. This marks a significant step toward realizing "humans in the loop" in a way that is *human-compatible*. Instead of leaving "individual humans confused and unsupported in the loop", the ADPC facilitates "real" support from both *automated systems* and *humans and organizations*.

5.12 What are the benefits for data controllers?

Several benefits accrue to *data controllers* supporting the ADPC. First, it demonstrates respect for users' privacy and agency, potentially enhancing trustworthiness and serving as a value proposition (Simkevitz, 2009). Second, developing and maintaining *consent banners* can be costly and challenging; the ADPC can alleviate this burden. Third, the current *consent banners* are disruptive and diminish user experience. The ADPC can help companies eliminate them, thereby improving user satisfaction and revenue (Salutari et al., 2020).

5.13 What if the ADPC is misused?

Security and privacy considerations have been integral to the ADPC's development. For example, the ADPC's domain-specific nature significantly reduces the risk of problematic *fingerprinting*. However, like any technology, the ADPC can be misused. Developers are expected to implement further privacy and security measures depending on the specific application. A useful analogy is the *email protocols* (e.g., Simple Mail Transfer Protocol, SMTP): while SMTP includes privacy and security measures, it does not prevent spam. Complementary solutions providing *anti-spam techniques* are necessary. Similarly, the ADPC should be accompanied by privacy and security measures and complementary solutions tailored to the application area, use case, and underlying technological systems.

5.14 From data protection to digital protection with the ADPC

As discussed previously, *digital protection* extends beyond merely *data protection*, *privacy*, and *consenting*. However, personal data protection and consenting play a fundamental role in the broader concept of digital protection. While the ADPC was primarily focused on *data protection and consenting*, its communication mechanism and associated socio-cognitive-techno-legal solutions can be leveraged to communicate other types of information, requests, data, and decisions pertinent to *digital protection*. For instance, the ADPC can be employed to inform users about the reasons behind specific decisions made by online algorithms, thereby enhancing the *transparency* and *accountability* of digital services. Such information can be seamlessly stored on the client-side, enabling users to maintain a record of their online activities. This record serves as proof of their digital interactions, empowering them to protect their digital rights, particularly with the *cognitive*, *collective*, and *contextual supports* enabled by the ADPC. As more digital rights, beyond data protection, are integrated into the ADPC, it would necessitate rebranding from *Advanced 'Data' Protection Control* to *Advanced 'Digital' Protection Control*.

6 Discussions

6.1 Rethinking policy and legal frameworks

In the realm of digital protection, the existing legal frameworks fall short in comprehensively addressing its multifaceted nature. Current legislation largely focuses on privacy, often termed 'data protection' in the European legal context, and the right to consenting, or places particular emphasis on safeguarding vulnerable social groups such as children. However, despite the historical precedence of these considerations, most frameworks tend to adopt an *individual-centric* lens when examining the interplay between human agency and digital technologies. This perspective, while ostensibly promoting human autonomy, often neglects inherent human limitations such as restricted capacities, expertise, motivation, and resources. A quintessential example of this is the prevalent practice of "cookie banners" in privacy management. Although claimed to be designed to empower users through control over their personal data, they fail to truly enable individuals due to their disregard for human cognitive constraints. It is imperative to recognize that an overly *individual-centric* approach to human interaction with digital technologies, even if it is framed as "humans in the loop", can exacerbate rather than alleviate the issue.

In the previous sections, we posited that *digital protection* and its subsets, including *data protection* and *the right to consenting*, should be conceptualized as *sociocognitive* actions encompassing *cognitive*, *contextual*, and *collective* dimensions. Focusing primarily on the *collective* dimension, given the scope of this article, it becomes evident that current legal systems often overlook the necessity for *collective support* in safeguarding and actualizing individual rights within an increasingly digital society. This oversight prompts a need for novel regulatory approaches or reinterpretations of existing laws to facilitate *collective management and practice of digital protection*. This necessitates a thorough and critical assessment of legal frameworks, questioning, for instance, the feasibility and legality of delegating personal privacy or data processing management to specialized third parties, or seeking assistance in these domains.

The universal relevance of this issue is underscored by the overwhelming majority of individuals lacking the cognitive capacity, expertise, or motivation to manage their digital protection independently, given the complexity and breadth of the subject. This challenge is further exacerbated when considering specific demographics such as children, the elderly, or individuals with physical disabilities. The solution does not lie in the elimination of individual rights to autonomy, control, and consultation, but in augmenting these with *collective support mechanisms*. Furthermore, the *automation* of certain tasks related to *digital protection*, along with providing *other cognitive supports*, must be carefully balanced with *collective* efforts and humans (plural) involvement, particularly from experts and end-users, to ensure effective and equitable digital safeguards.

6.2 Harmonizing automation and humans involvement in digital protection and control

The failure of existing legal frameworks, such as the General Data Protection Regulation (GDPR), which primarily adopt an *individual-centric* approach, underscores the need for a more holistic method. These regulations, despite their comprehensive nature, often fall short in protecting human digital rights. The *individual-centric* approach fails to address the *collective* and *interconnected* nature of *digital environments*, leading to gaps in protection and control. This inadequacy highlights the necessity of a paradigm shift toward more inclusive and interactive models of *digital protection*.

In the preceding sections of this article, we have elucidated the necessity of furnishing users with comprehensive supports pertaining to their digital protection, consenting and controlling. This tripartite framework of support–*cognitive*, *collective*, and *contextual*–emerges as critical in navigating the complexities of the digital realm. *Cognitive support* aids users in understanding and managing their digital interactions, while *collective support* leverages community knowledge and guardian/expert guidance. *Contextual support*, on the other hand, aligns user experiences with their specific digital environments and personal preferences. The integration of these supports is paramount in fostering a secure and informed digital user experience.

To actualize this framework, the implementation of Advanced Digital Protection Control mechanisms within *internet infrastructure* is imperative. These mechanisms should facilitate the communication of data relevant to digital protection, thereby enabling the provision of the aforementioned supports. The augmentation of *internet infrastructure* with these controls is a significant step toward enhancing user autonomy and security in digital spaces. By providing users with more granular control over their digital interactions, these mechanisms can empower them to make informed decisions about their online presence and activities.

A substantial portion of *cognitive* and *contextual supports* can be effectively delivered through enhanced user interfaces on the user side. User interfaces that are intuitive and human-compatible can significantly diminish the cognitive load on users, aiding them in comprehending and managing their digital interactions with greater ease. Additionally, mechanisms such as whitelisting and blacklisting offer users straightforward tools for managing their digital exposure. However, the most impactful *cognitive* and *contextual supports* are likely to be derived from automation. Various models, including rule-based, preference-based, artificial intelligence-based, and predictive-based systems, can be employed to tailor digital experiences to individual user needs and preferences. These automated systems can proactively adjust user settings and alerts based on learned patterns and user-specified preferences, thereby enhancing the relevance and efficacy of digital protections.

In addition to these automated systems, the *collective support* from experts and trusted parties, such as guardians, parents, friends, family members, NGOs, and organizations, plays a vital role. The implementation of Advanced Digital Protection Control

mechanisms can facilitate this *collective support*. Importantly, these mechanisms also enable auditing and monitoring of automated systems, ensuring their reliability and compliance with ethical standards. This *collective involvement* not only provides a layer of oversight but also fosters a community-oriented approach to digital protection.

Achieving harmony between *individual agency*, *collective support*, and *automated systems* is crucial for the accountability, lawfulness, and ethicality of future digital protection practices. This triad ensures that digital protection mechanisms are not only technologically advanced but also *human-compatible*, addressing the diverse needs and rights of users. The harmonization of these elements leads to more resilient and responsive digital environments, where technological advancements are balanced with human insight and oversight. It fosters a *collaborative environment* where both users and experts contribute to the evolution of digital protection strategies, ensuring that these strategies are grounded in real-world contexts and human experiences. This balanced approach is instrumental in creating a digital landscape that is secure, reliable, trustworthy, human-compatible and adaptable to the evolving nature of digital threats and opportunities.

6.3 Data subject empowerment as a path to data controller empowerment

As discussed previously, the novel data protection and consenting mechanisms presented in this article, which provide *cognitive*, *collective*, and *contextual support* for end-users, can significantly enhance user empowerment by involving them (or their representatives) in the control procedures, design processes, and data management practices of online personal data processing. Additionally, it is crucial to recognize that, alongside empowering *data subjects* who face challenges in managing online privacy, *data controllers* also struggle with adhering to diverse legal frameworks and developing various privacy management mechanisms (see, e.g., Mikkelsen et al., 2019; Tsaneva et al., 2019), and they too need empowerment. For instance, developing consent-obtaining mechanisms, such as *cookie banners*, poses significant challenges, particularly for smaller enterprises. The approaches discussed in this article can introduce innovative methods for communicating privacy and obtaining consent from *data subjects*, potentially alleviating the burden of designing and maintaining current mechanisms like *cookie banners*. The *collective* approach can facilitate collaboration between user representatives (such as privacy-expert NGOs) and *data controllers*, leading to more streamlined decision-making processes for *data controllers*. Furthermore, the current practices can be highly disruptive to users. Given that *user experience* is a critical factor for online service providers, substituting these banners with more advanced mechanisms enabled by novel communication methods could provide substantial benefits for companies (Salutari et al., 2020). Ultimately, these improvements can also empower *data controllers*, as better privacy and data protection practices benefit *all stakeholders*, not just the *data subjects*.

6.4 The paradox of trust in *collective* digital protection

As previously discussed, a fundamental assumption underlying the advocacy of *collective* practices in digital protection is that not everyone possesses the knowledge, time, expertise, or motivation to protect their own digital rights. This need for support is especially crucial for children or individuals with specific needs or disabilities. Our proposal suggests that various types of *cognitive supports*, such as whitelisting, blacklisting, rule-based approaches, AI-based assistants, and support from other humans (e.g., family members, experts) or organizations (e.g., digital protection advocacy NGOs, companies offering digital protection services), can assist users in managing their digital protection.

We acknowledge the sensitivity of digital protection and the significant trust users must place in their supporting individuals or organizations. This aspect of trust, however, may attract potential criticism regarding our proposal. Concerns may arise about the potential misuse of this trust or the possibility of unsatisfactory outcomes due to mistakes in *collective digital protection*. These concerns are valid, and the issue of *accountability* is paramount and must be carefully addressed and designed.

However, we contend that the potential challenges of a practice should not warrant its complete disregard. Society comprises numerous specialized tasks performed by experts, and in all these tasks, the question "what if something goes wrong?" can always be posed. Despite this, we continue to "outsource" tasks to relevant experts without questioning the fundamental nature of *collective performance* in society. Typically, we design procedures to ensure that only qualified individuals (e.g., those with specific licenses or education) are permitted to perform certain tasks for others and establish legal frameworks that protect individuals' rights in cases of misuse or misconduct. We perceive the design of such procedures to ensure *transparency* and *accountability* in *collective digital protection* as a crucial next step in this research.

6.5 Standardization, adoption, complexity, and continuous co-creation for/of sustainability

The *digital protection, consenting and controlling communication mechanisms* discussed in this article represent a crucial, yet missing, component of the current *internet infrastructure*. However, they are merely a part of larger, intricate socio-cognitive-techno-legal ecosystems that need to be realized to embody and implement a value-driven, lawful, ethical, and human-compatible practice of digital protection. The standardization of mechanisms such as the ADPC can serve as an essential starting point for the adoption of such measures. As previously mentioned, this process must be supported by policies and regulations, given that many companies perceive a conflict of interest between more *human-compatible* digital protection practices and their business goals.

It is also imperative to engage in educating citizens about digital protection as an inviolable fundamental right and to instruct companies that ethical and human-compatible digital protection

practices are not contrary to business interests but can, in fact, foster innovation and trust. Achieving a genuine shift in digital protection practices necessitates various bottom-up and top-down activities and initiatives alongside technical advancements. Digital protection is inherently complex, involving numerous actors, layers, disciplines, and dimensions.

Continuous efforts must be made to sustain digital protection practices as new technologies emerge, each bringing its unique challenges and considerations. Complexity should never serve as an excuse for the lack of effort in improving and sustaining digital protection practices. This principle applies to numerous facets of modern society. For example, governing, enhancing the living conditions in large cities, and maintaining their sustainability are complex tasks, yet numerous successful stories from around the globe demonstrate constant improvement.

Recognizing digital protection as a fundamental dimension of our society, crucial for democracy and social sustainability, should motivate us to invest more resources into reconstructing the foundations of digital protection. This reconstruction should encompass not just technical perspectives but also policy, legal, economic, and societal dimensions.

6.6 Conclusion

The central thesis of this article posits that integrating or maintaining *humans involvement* in digital environments is vital for safeguarding human rights and ensuring pluralism, inclusion, and human agency in the creation, evaluation, and upkeep of digital technologies. However, this approach, if not founded on a comprehensive and multifaceted understanding of human nature, risks becoming counterproductive. We examined the paradigm of *digital protection* to demonstrate how an overly *individual-centric* approach to human interactions with digital technologies–designed ostensibly to enhance user control–may paradoxically lead to a loss of control. This is because individuals, lacking support, struggle to comprehend and manage the complexities of the surrounding digital environments. The study highlighted the current systemic limitations of the Internet, which impede the shift toward providing *collective user support*. We explored the concept of Advanced Digital Protection Control, advocating that such innovative communication mechanisms could be pivotal in offering *cognitive*, *contextual*, and *collective support* to users. This could fundamentally transform how digital rights are perceived and exercised. Additionally, the paper underscores the necessity for novel approaches in policy-making and law-making, as well as technical advancements, to implement mechanisms like the ADPC (Human, 2022a) effectively. In the era of widespread [generative] AI usage and ambient digital technologies, it is imperative to urgently and proactively implement, adopt, or enforce mechanisms that provide *cognitive*, *contextual*, and *collective support* to *every individual*. This is essential for preserving our individual and societal sustainability and realizing the true potential of "humans (plural) in the loop".

Author contributions

SH: Conceptualization, Funding acquisition, Investigation, Methodology, Resources, Supervision, Visualization, Writing – original draft, Writing – review & editing.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. This research was partially funded by netidee, the funding program of the INTERNET FOUNDATION AUSTRIA, under the project numbers 6944, 6442, 5937, and 4625. The support of netidee has been instrumental in enabling this work, and we gratefully acknowledge their contribution.

Acknowledgments

We acknowledge the support received from our colleagues at noyb and the Vienna University of Economics and Business, as well as all other collaborators involved in the development of the ADPC and its surrounding concepts and mechanisms. Their insights and assistance have been invaluable to this project. AI tools were utilized for enhancements in linguistic proficiency.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Augoustinos, M., Walker, I., and Donaghue, N. (2014). *Social Cognition: An Integrated Introduction*. Thousand Oaks, CA: Sage.

Brown, D. H., and Pecora, N. (2014). Online data privacy as a children's media right: toward global policy principles. *J. Child. Media* 8, 201–207. doi: 10.1080/17482798.2014.893756

Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., and Yu, I. (2021). "Achieving privacy: costs of compliance and enforcement of data protection regulation," in *Policy Research Working Paper, 9594. World Bank's World Development Report 2021 Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. 2021. Georgetown Law Faculty Publications and Other Works. 2374.* doi: 10.2139/ssrn.3827228

Choi, H., Park, J., and Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Comput. Human Behav.* 81, 42–51. doi: 10.1016/j.chb.2017.12.001

Council of Europe (1950). *European convention on human rights. Council of Europe Treaty Series No. 5. As amended by Protocols Nos. 11 and 14*. Strasbourg: Council of Europe.

Das, S., Kramer, A. D., Dabbish, L. A., and Hong, J. I. (2015). "The role of social influence in security feature adoption," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, NY: ACM), 1416–1426.

de Kerckhove, D. (2021). The personal digital twin, ethical considerations. *Philosoph. Trans. Royal Soc. A* 379:20200367. doi: 10.1098/rsta.2020.0367

Degeling, M., and Human, S. (2023). Internet privacy protocols. *Zeitschrift für Medienwissenschaft* 15, 55–70. doi: 10.14361/zfmw-2023-150107

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., and Holz, T. (2018). We value your privacy... now take some cookies: measuring the gdpr's impact on web privacy. *arXiv* [preprint] arXiv:1808.05096. doi: 10.14722/ndss.2019.23378

Desai, D. (2022). "Hyper-personalization: an ai-enabled personalization for customer-centric marketing," in *Adoption and Implementation of AI in Customer Relationship Management* (Hershey, Pennsylvania: IGI Global), 40–53.

Emami Naeini, P., Degeling, M., Bauer, L., Chow, R., Cranor, L. F., Haghighat, M. R., et al. (2018). The influence of friends and experts on privacy decision making in iot scenarios. *Proc. ACM on Human-Comp. Interact.* 2, 1–26. doi: 10.1145/3274317

European Parliament and Council of the European Union (1995). "European data protection directive," in *Directive 95/46/EC* (Brussels: European Union).

European Parliament and Council of the European Union (2016). "General data protection regulation," in *Regulation (EU) 2016/679* (Brussels: European Union).

European Parliament and Council of the European Union and Commission of the European Communities (2000). "Charter of fundamental rights of the European Union," in *2000/C 364/01* (Brussels: European Union).

Frith, C. D. (2008). Social cognition. *Philosoph. Trans. Royal Soc. B: Biol. Sci.* 363, 2033–2039. doi: 10.1098/rstb.2008.0005

German Federal Government (1977). "Federal data protection act," in *Federal Law Gazette I* (Berlin: German Federal Government), 201.

Granovetter, M. (2018). "Economic action and social structure: the problem of embeddedness," in *The Sociology of Economic Life* (London: Routledge), 22–45.

Gray, C. M., Santos, C., Bielova, N., Toth, M., and Clifford, D. (2021). "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY: Association for Computing Machinery), 1–18.

Hassanzadeh, Z., Biddle, R., and Marsen, S. (2021). User perception of data breaches. *IEEE Trans. Prof. Commun.* 64, 374–389. doi: 10.1109/TPC.2021.3110545

Hessian Parliament (1970). "Hessian data protection act," in *The First Data Protection Law Enacted at a Regional Level in Germany, Pioneering the Legal Framework for Data Privacy*. Wiesbaden: Hessische Staatskanzlei.

Human, S. (2022a). "Advanced data protection control (ADPC): an interdisciplinary overview," in *Sustainable Computing Paper Series*. Vienna: Vienna University of Economics and Business.

Human, S. (2022b). "THE HALE WHALE: a framework for the co-creation of sustainable, human-centric, accountable, lawful, and ethical digital sociotechnical systems," in *Sustainable Computing Paper Series*. Vienna: Vienna University of Economics and Business.

Human, S., Alt, R., Habibnia, H., and Neumann, G. (2022). "Human-centric personal data protection and consenting assistant systems: towards a sustainable digital economy," in *Proceedings of the 55th Hawaii International Conference on System Sciences* (Hawaii: University of Hawaii), 4727–4736.

Human, S., and Cech, F. (2021). "A human-centric perspective on digital consenting: the case of GAFAM," in *Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies*, eds. A. Zimmermann, R. J. Howlett and L. C. Jain (Singapore: Springer), 139–159.

Human, S., Gsenger, R., and Neumann, G. (2020). "End-user empowerment: an interdisciplinary perspective," in *Proceedings of the 53rd Hawaii International Conference on System Sciences* (Hawaii: Hawaii International Conference), 4102–4111.

Human, S., and Kazzazi, M. (2021). "Contextuality and intersectionality of e-consent: A human-centric reflection on digital consenting in the emerging genetic data markets," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&adpPW)*, 307–311.

Human, S., Neumann, G., and Peschl, M. F. (2019). [how] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies? *Intellectica* 70, 165–180. doi: 10.3406/intel.2019.1897

Human, S., Schrems, M., Toner, A., Gerben, and Wagner, B. (2021). "Advanced data protection control (ADPC)," in *Sustainable Computing Reports and Specifications 2021/01* (Vienna: University of Economics and Business).

Human, S., and Wagner, B. (2018). "Is informed consent enough? Considering predictive approaches to privacy," in *CHI2018 Workshop on Exploring Individual Differences in Privacy, Montréal, Canada*.

Human, S., and Watkins, R. (2023). Needs and artificial intelligence. *AI and Ethics* 3, 811–826. doi: 10.1007/s43681-022-00206-z

Jesus, V. (2020). Towards an accountable web of personal information: the web-of-receipts. *IEEE Access* 8, 25383–25394. doi: 10.1109/ACCESS.2020.2970270

Kirchner, N., Human, S., and Neumann, G. (2019). "Context-sensitivity of informed consent: The emergence of genetic data markets," in *Workshop on Engineering Accountable Information Systems* (Amman: European Conference on Information Systems-ECIS).

Lehtiniemi, T., and Kortesniemi, Y. (2017). Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data Soc.* 4:2053951717721935. doi: 10.1177/2053951717721935

Maaß, W. (2011). "The elderly and the internet: how senior citizens deal with online privacy," in *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Cham: Springer), 235–249.

Marwick, A. E., and Boyd, D. (2018). Privacy at the margins| understanding privacy at the margins–introduction. *Int. J. Commun.* 12, 1157–1165.

Mikkelsen, D., Soller, H., Strandell-Jansson, M., and Wahlers, M. (2019). *GDPR Compliance Since May 2018: a Continuing Challenge*. New York: McKinsey & Company, 22.

Morel, V., Santos, C., Lintao, Y., and Human, S. (2022). "Your consent is worth 75 euros a year-measurement and lawfulness of cookie paywalls," in *Proceedings of the 21st Workshop on Privacy in the Electronic Society* (New York, NY: Association for Computing Machinery (ACM)), 213–218.

Newen, A., De Bruin, L., and Gallagher, S. (2018). *The Oxford Handbook of 4E Cognition*. Oxford: Oxford University Press.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., and Kagal, L. (2020). "Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (New York, NY: Association for Computing Machinery (ACM)), 1–13.

Obar, J. A., and Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Inform. Commun. Soc.* 23, 128–147. doi: 10.1080/1369118X.2018.1486870

Organisation for Economic Co-operation and Development (1980). *Oecd Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD.

Pandit, H. J., Polleres, A., Bos, B., Brennan, R., Bruegger, B., Ekaputra, F. J., et al. (2019). "Creating a vocabulary for data privacy," in *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"* (Cham: Springer), 714–730.

Salutari, F., Da Hora, D., Varvello, M., Teixeira, R., Christophides, V., and Rossi, D. (2020). "Implications of the multi-modality of user perceived page load time," in *2020 Mediterranean Communication and Computer Networking Conference (MedComNet)* (Arona: IEEE), 1–8.

Santos, C., Bielova, N., and Matte, C. (2019). Are cookie banners indeed compliant with the law? Deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners. *arXiv* [preprint] arXiv:1912.07144.

Schröer, S. L., Apruzzese, G., Human, S., Laskov, P., Anderson, H. S., Bernroider, E. W., et al. (2024). *SoK: On the Offensive Potential of AI*.

Simkevitz, H. (2009). "Why privacy matters in health care delivery: a value proposition," in *2009 World Congress on Privacy, Security, Trust and the Management of e-Business* (St. John's, NL: IEEE), 193–201.

Solove, D. J. (2021). The myth of the privacy paradox. *George Wash. Law Rev.* 89:1. doi: 10.2139/ssrn.3536265

Taddei, S., and Contena, B. (2013). Privacy, trust and control: which relationships with online self-disclosure? *Comput. Human Behav.* 29, 821–826. doi: 10.1016/j.chb.2012.11.022

Tao, J., and Shuijing, H. (2016). "The elderly and the big data how older adults deal with digital privacy," in *2016 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)* (Changsha: IEEE), 285–288.

Tsaneva, M. (2019). "Challenges of GDPR compliance in consumer financing companies," in *Conferences of the department Informatics* (Varna: Publishing house Science and Economics Varna), 103–115.

United Kingdom Government (1999). "Telecommunications (data protection and privacy) regulations," in *Statutory Instruments 1999 No. 2093* (London: United Kingdom Government).

United States Congress (1998). "Children's online privacy protection act," in *Public Law No. 105-277, 112 Stat. 2681–728* (Washington, DC: United States Congress).

Utz, C., Degeling, M., Fahl, S., Schaub, F., and Holz, T. (2019). "(un) informed consent: studying GDPR consent notices in the field," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY: Association for Computing Machinery (ACM)), 973–990.

Varela, F. J., Thompson, E., and Rosch, E. (2017). *The Embodied Mind, Revised Edition: Cognitive Science and Human Experience*. Cambridge, MA: MIT Press.

Watkins, R., and Human, S. (2023). Needs-aware artificial intelligence: AI that serves [human] needs'. *AI and Ethics* 3, 49–52. doi: 10.1007/s43681-022-00181-5

Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. (2018). User perceptions of smart home iot privacy. *Proc. ACM n Human-Comp. Interact.* 2, 1–20. doi: 10.1145/3274469

Zhu, Q., Sun, R., and Yuan, Y. (2023). Impact of the normativeness and intelligibility of privacy interpretation information on the willingness to accept targeted advertising–a cognitive load perspective. *Curr. Psychol.* 2023, 1–15. doi: 10.1007/s12144-023-04325-6

Zimmeck, S., and Alicki, K. (2020). "Standardizing and implementing do not sell," in *Proceedings of the 19th Workshop on Privacy in the Electronic Society* (New York, NY: Association for Computing Machinery (ACM)), 15–20.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *J. Informat. Technol.* 30, 75–89. doi: 10.1057/jit.2015.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

Zuboff, S. (2023). "The age of surveillance capitalism," in *Social Theory Re-Wired* (London: Routledge), 203–213.