Journal of Ethics and Emerging Technologies

IEET

Research Article

Design for Embedding the Value of Privacy in Personal Information Management Systems

Haleh Asgarinia [1*]

[1] Ph.D. Candidate, e-mail: h.asgarinia@utwente.nl

[*] Correspondence: Ph.D. Candidate; Faculty of Behavioral, Management, and Social Sciences; Department of Philosophy; University of Twente; Netherlands

Abstract: Personal Information Management Systems (PIMS) aim to facilitate the sharing of personal information and protect privacy. Efforts to enhance privacy management, aligned with established privacy policies, have led to guidelines for integrating transparent notices and meaningful choices within these systems. Although discussions have revolved around the design of privacy-friendly systems that comply with legal requirements, there has been relatively limited philosophical discourse on incorporating the value of privacy into these systems. Exploring the connection between privacy and personal autonomy illuminates the instrumental value of privacy and highlights the importance of intentionally embedding the value of privacy into these systems. To translate the value of privacy into concrete design requirements, this study constructs a values hierarchy consisting of values, norms, and design requirements. After analyzing the relationships between privacy and autonomy and identifying norms, the design requirements translated from the norms associated with the components of personal autonomy are specified at the lowest layer. These requirements include a design to prevent unauthorized access and dark patterns and to provide effective and efficient notices and choices. The findings contribute to expanding the requirements for designing the aspect of privacy as a legal requirement to incorporate the value of privacy into systems.

Citation: Asgarinia, Haleh. 2023. Design for Embedding the Value of Privacy in Personal Information Management Systems. *Journal of Ethics and Emerging Technologies* 33: 1. https://doi.org/10.55613/xdrbyv83

Received: 29/11/2023
Accepted: 19/01/2024
Published: 20/01/2024

Publisher's Note: IEET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Keywords: personal autonomy; personal information management systems; value of privacy; values hierarchy

1. Introduction

To enable and ensure individuals control the sharing of their personal information, technologies can be used to mediate the relationship between them and developers or deployers who aim to collect the shared information, with PIMS being a notable example (Asgarinia et al. 2023). The term 'PIMS' broadly represents a category of technology that enables individuals to decide what information about them is collected, when it is collected, how it is collected, and with whom it is shared. Personal data stores, personal data vaults, personal information management services, and personal data spaces all fall under the umbrella term of PIMS (Janssen and Singh 2022). More recently, improved versions of PIMS, such as self-sovereign identity models, have been developed to enable individuals to mediate, monitor, and exert control over the access, usage, and sharing of their personal data (Asgarinia et al. 2023).

The PIMS approach promotes privacy self-management (Janssen and Singh 2022). The objective is to make the processing of personal data transparent and to enable individuals (i.e., data subjects) to make decisions about their data. Two pivotal elements of privacy self-management are providing individuals with information about the data

collected about them and how they are used (notice), as well as affording them the authority to decide whether they accept such data collection and usage (choice). This approach is commonly referred to as 'notice and choice' (Barocas and Nissenbaum 2009; Solove 2013).

There have been proposals to enhance the transparency of privacy notices, both in terms of content and the design of user interfaces. Transparency regarding content is commonly understood as a form of meaningful notice about the collection and usage of data (Barocas and Nissenbaum 2009). Measures to enhance the transparency of privacy policy[1] notices include presenting information about data usage in an understandable way. Furthermore, beyond content and readability, to enhance the transparency of privacy notices regarding the design of user interfaces, measures have been introduced by Waldman (2018) to emphasize the design and aesthetics of content. These measures include elements such as font, size, color backgrounds, and the use of charts or icons within notices, all aimed at effectively conveying information to individuals (Waldman 2018).[2]

Despite discussions regarding preserving privacy by implementing proper notice and choice, especially concerning privacy policies (Grannis 2015; Waldman 2016), there has been limited discourse on embedding the value of privacy into PIMS. Conducting philosophical investigations to integrate privacy into PIMS reveals the shortcomings of approaches that predominantly rely on notice and choice and suggests a more comprehensive approach for embedding privacy into the system. This paper aims to address these shortcomings by proposing design requirements to incorporate the value of privacy into PIMS thoroughly. In this way, PIMS contributes to the value of privacy, which designers and developers intentionally embed in the technology.

The purpose of this paper is to incorporate the value of privacy into PIMS; to do so, I draw a value hierarchy to translate the value of privacy into design requirements. As van de Poel (2013) explains, a values hierarchy consists of three layers of values, norms, and design requirements, in which higher-level elements are translated into lower-level ones. In this way, moving from the top layer to the bottom, abstract values are translated into tangible design requirements. In the values hierarchy this paper proposes, the instrumental value of privacy is described in connection with a person's autonomy. From this perspective, specific design requirements are derived by translating norms that are aimed at promoting autonomy.

2. Approach: Conceptualizing a Values Hierarchy for Privacy

Value Sensitive Design (VSD) is one of the most comprehensive, impactful embedded-value approaches (Friedman and Borning 2008). The goal of VSD is to consider and incorporate moral values comprehensively throughout the design process. The approach provides guidelines for designing and developing technological products that promote the values desired by the various stakeholders whom these technologies may impact (Brey 2010; van de Poel 2009).

[1] In general, privacy policies concern personal data collection, storage, and use, often aligning with the General Data Protection Regulation. This regulation, which is the European Union's landmark data protection legislation, establishes principles relating to the processing of personal data. These principles specify that personal data shall be minimized to what is necessary in relation to the purposes for which they are processed (data minimization), collected for specified and legitimate purposes (purpose limitation), and stored only as long as necessary for the purpose for which they are processed (storage limitation; EU Parliament 2016, Article 5).

[2] Utilizing tutorials and providing notices regarding privacy policies can contribute to making individuals more aware of the importance and sensitivity of privacy-related concerns (I thank an anonymous reviewer for mentioning this point).

An essential stage in VSD is translating values into tangible design requirements. To do so, van de Poel (2013) has introduced the notion of the value hierarchy, according to which values and design requirements have a hierarchical structure. The top layer of a values hierarchy consists of values; the intermediate layer consists of norms; and the most concrete layer involves design requirements. As van de Poel suggests, by moving from the upper to lower layers in a hierarchy, we can effectively translate abstract values into concrete design requirements.

Following van de Poel (2009, 2013), to construct a values hierarchy, leading to the intentional design of PIMS for the value of privacy, the following steps are essential: first, conceptualize how the value of privacy is understood or conceptualize the understanding of the value of privacy; second, translate the value of privacy into general and specific norms; and third, formulate design requirements through the translation of norms.

Regarding conceptualizing the value of privacy dedicated to the first layer of a values hierarchy, this paper discusses the value of privacy in connection with a person's autonomy, in which privacy is considered valuable for the sake of autonomy. The instrumental value of privacy depends on autonomy; the value of privacy is realized in metaphorical or symbolic spaces in which a person can develop and exercise their autonomy, enabling them to live their lives autonomously (Rössler 2005).

Concerning the second layer of a hierarchy dedicated to norms, in addition to the norm of reflection, I specify the norms associated with each component of the concept of personal autonomy. These components include authentication and identification, the genesis of desires, and goals and projects. The norms pertaining to the first component include exercising control over personal information to establish and maintain various social relationships; being aware of the types of relationships they are involved in, which helps them decide which part of their information to share; and considering social circumstances that provide a basis for recognition (see Section 4.1). The norms associated with the second component involve enabling a person to exercise control over their personal information to become less susceptible to manipulation and prevent manipulation to enable them to share their personal information as intended (see Section 4.2). Regarding the norms linked to the third component, they encompass the ability to contemplate and evaluate different alternatives for sharing information, ultimately choosing the one that aligns with one's objectives (see Section 4.3).

Concerning the third layer of a hierarchy centered on design requirements, I suggest the following design requirements regarding the value of privacy in PIMS: design for reflection through using friction, which obstructs a person in the completion of tasks typically performed without conscious thought, to stimulate imagination (translated for the norm of reflection; see Section 5); design to restrict unauthorized access by implementing encryption, considering the execution of contracts, and ultimately, employing blockchain technology to fulfil contract needs and apply encryption (translated from the first component of the concept of personal autonomy; see Section 5.1); design for effective notices, and design against dark patterns to prevent certain cognitive biases occurring (translated from the second component of the concept of autonomy; see Section 5.2); and design for effective and efficient notice and choice (translated from the third component of the concept of personal autonomy; see Section 5.3). As the proposed design requirements suggest, embedding the value of privacy into PIMS involves more than just designing for notice and choice, as privacy policies emphasize. Additional requirements must be articulated and considered in the design of PIMS.

The findings of this paper highlight that, although PIMS is primarily designed to protect privacy using the notice and choice approach that privacy policies regulate—design for meaningful notice and transparent choice—this approach must be completed by incorporating other elements, such as inclusiveness for diverse audiences (see Section 5.3). Furthermore, this paper emphasizes that the current privacy design in PIMS does not fully promote the realization of the instrumental value of privacy, as it mainly addresses one component related to this value (i.e., goals and projects; see Section 5.3). However,

other components, such as authenticity and identification, and the genesis of desires (see Sections 5.1 and 5.2), also require consideration in the design of PIMS. Therefore, the approach governed by privacy policies must be completed and also expanded to thoroughly incorporate the instrumental value of privacy. The main aim of this paper is to conduct philosophical investigations that articulate design requirements for embedding the value of privacy into PIMS.

In the following sections, three parts are presented, each dedicated to a layer in a values hierarchy, namely values, norms, and design requirements. These layers are described in Sections 3 to 5, respectively. In addition to the guidelines and strategies developed to facilitate the design of privacy-friendly systems to ensure compliance with legal requirements and privacy policies, the proposed design requirements ensure that PIMS is built to realize the value of privacy.

3. The Layer of Values: Privacy and Autonomy

Following van de Poel's (2009, 2013) approach, the top layer of a hierarchy includes values. Since this paper proposes a hierarchy for privacy, the top layer focuses on privacy. Therefore, to construct a hierarchy that facilitates proposing design requirements to incorporate the value of privacy into PIMS, the first step is to understand the value of privacy.

A few debates in the literature on privacy focus on the idea that privacy is intrinsically valuable. However, it has commonly been assumed by privacy scholars that privacy is valuable for the sake of something else, deriving its worth from other sets of moral values, principles, or commitments. Although the instrumental value of privacy has been discussed from different perspectives, from its relationship to social cohesion (Solove 2008) to political values, such as power (Véliz 2021) and democracy (Henschke 2021), I focus on the value of privacy in relation to personal autonomy, as PIMS is developed with the primary aim of promoting one's autonomy.

In the scholarly literature, different theories have been developed to explain the value of privacy in relation to autonomy, e.g., Goffman (1959), Riesman (1952), and Rössler (2005). Goffman (1959) argues that privacy should be understood as a form of autonomy. According to Riesman (1952), the value of privacy stems from its protection of individuals' autonomy, as privacy preserves a space around individuals, within which they can direct their lives and behavior irrespective of social pressures. Rössler (2005) highlights that, in liberal societies, privacy is functionally valuable for the sake of a person's autonomy, of living autonomously. In short, we value privacy because we want to be autonomous, and without privacy, autonomy cannot work.

3.1. Privacy and Autonomy

Regarding the above discussions about the instrumental value of privacy, privacy is deemed valuable for the sake of autonomy. The conception I adopt in this paper is based on Rössler's (2005) account of autonomy. Rössler argues autonomy is not connected to the strong criterion of rationality, unlike moral autonomy, and she considers social conditions' role in forming autonomy, such as relational autonomy. First, Rössler delineates between moral autonomy and personal autonomy, with a particular emphasis on the latter in terms of the functional value of privacy in furthering it. Each facet of autonomy necessitates a nuanced consideration of the underlying principles or conditions. Although Rössler does not explain the similarities and differences between moral and personal autonomy, I begin by briefly discussing moral autonomy and how it is often used following Kant. Second, Rössler identifies three sufficient and necessary components of personal autonomy and conceptualizes personal autonomy in a way that depends on and is bound up with an intersubjective network. Therefore, before exploring the components of autonomy in Rössler's view, I discuss relational autonomy as the

concept of personal autonomy with reference to intersubjective relations. Hence, in what follows, I provide an analysis of moral autonomy and discuss relational autonomy to facilitate an understanding of personal autonomy.

3.1.1. Moral Autonomy

As Korsgaard (2009) highlights, according to Kant, being autonomous means being governed by the principles of one's own causality–one's own maxims. The categorical imperative is a rule for constructing maxims (Korsgaard 2009, 81). In *Groundwork*, the first formulation of the categorical imperative (i.e., formula of universality) is that you should act only according to that maxim, through which you can, at the same time, will that it can become a universal law (4:421). According to Kant, acting autonomously entails ensuring the maxim guiding one's action is one you could will to be a universal law. Autonomy identifies with the universalizability of one's own maxims. Hence, to be autonomous means to act in conformity with the principle of *practical reason* (the categorical imperative; Korsgaard 2009, 71–80).

According to Korsgaard (2009), the reasons embodied in universal maxims must be understood as public or shareable: reasons with normative force for all rational beings. Instead of merely thinking that, if I have a reason to do action-A in circumstances-C, then I must be able to grant that you also would have a reason to do the same (which relates to the universalizability requirement regarding the private conception of reasons), the public conception of reason indicates that universalizability commits me to the view that, if I have a reason to do action-A in circumstances-C, I must be able to will that you should do the same, because your reasons are normative for me. It is only regarding the public conception of reasons that a universalizability requirement leads us into moral territory—conformity with Kant's law of humanity; by adopting other's reasons as our own, with normative force for us, we treat them as an end in themselves (Korsgaard 2009, 191–92).

Two features characterize Kant's conception of moral autonomy, as adopted by Korsgaard (2009): first, rationality, which involves acting in a way that conforms with the principle of practical reason (i.e., the categorical imperative), understood as public and sharable reason; and second, focusing on the form of the maxim that must serve as a law without investigating the subjective source and the content of the maxims.

3.1.2. Relational Autonomy

Relational autonomy does not refer to a single account but to accounts shared under the assumption that 'persons are socially embedded and that agents' identities are formed within the context of social relationships' (Mackenzie and Stoljar 2000, 4). Thus, the focus of relational approaches is to emphasize certain social circumstances allowing a person to develop their autonomy (Oshana 1998), interpersonal and social factors as conceptually necessary for autonomy (Christman 2004), and social conditions necessary for the constitution of affective attitudes towards oneself (Mackenzie 2008).

Marina Oshana defends and develops an influential account of social autonomy, emphasizing that autonomy should be conceived as a 'socio-relational' phenomenon (Oshana 1998, 94). In her account, it is social conditions that enable a person to self-determinate that mark autonomy; autonomy is obtained only when the social conditions surrounding an individual meet certain standards. In cases in which basic opportunities for self-determination are denied due to strict obedience or subservience, such as in cases of voluntary slavery, the subservient woman, the conscientious objector, or the monk, then even if a person meets the condition of authenticity and chooses to enter or continue in certain conditions, the surrounding social conditions in which they reside do not allow them to be autonomous. According to Oshana (1998), a person who resides under oppressive social conditions cannot be autonomous.

Christman (2004) critiques Oshana's view, arguing that, insofar as a person authentically embraces even an oppressive social status or subservient roles, they can still

be considered autonomous. In Christman's account, for a person to be autonomous, they must adequately reflect on their social conditions, including conditions of strict obedience. Rather than defending autonomy in idealized situations, breaking away from social norms that have influence over them, and pursuing their goals differently from those norms, as defended by Oshana's account of autonomy, Christman states a person who can reflect adequately—in the sense that they can imagine choosing otherwise to value that alternative position—is autonomous. A slave, according to Christman, can consider themselves autonomous when they can see themselves doing otherwise, under at least some imaginable conditions, without needing to reject those conditions (Christman 2004).

In contrast to Oshana (1998), Christman (2004) contends his view is consistent with the idea that selves are constituted by the social and interpersonal dynamics that surround them. In Christman's view, insofar as the self is socially constituted, it is counterintuitive to claim that such a self is only autonomous when they can break away from those very social conditions that constitute its being. As long as a person maintains the ability to reflect adequately on those conditions and embraces them, Christman argues we should continue to label them as autonomous (Christman 2004).

Mackenzie (2008) critiques Christman's (2004) view by arguing that oppressive social conditions might undermine autonomy. According to Mackenzie, a person's practical identity may be shaped by false norms, beliefs, and distorted values arising from oppressive social conditions. This situation can lead to cultivating destructive affective attitudes towards oneself, such as a lack of self-respect or mistrusting one's own judgement.

Mackenzie (2008) advances a concept of relational autonomy that can be characterized as weak compared with Oshana's strong account, which defends a strong account of relational autonomy in the sense that abusive or oppressive social relationships necessarily undermine autonomy. However, Mackenzie (2008) argues that such conditions impair autonomy only when they fail to provide individuals with the recognitive basis necessary to maintain certain attitudes towards themselves.

Mackenzie (2008) developed a recognition-based account of relational autonomy. According to her, an autonomous person must be able to reflect on certain attitudes towards themselves, attitudes constituted by society and in intersubjective relationships. Drawing on the insights of Benson (1994) and McLeod (2002), Mackenzie highlights particular attitudes towards oneself as attitudes of self-respect, self-trust, and self-esteem. These affective attitudes are constituted by society and in intersubjective relationships. Thus, practical identity is first-person identity aligned with Henschke's (2017) idea of self-regarding identity, which is constituted thoroughly in intersubjective relationships and depends upon the mutual recognition in socio-relational situations.

Relational theorists have rejected the individualistic conception of autonomy that typically tends to understand practical identity as being formed by one's own desires, values, and commitments independently of social influence. Instead, these theorists have argued that practical identity is shaped by the social and interpersonal aspects of one's life. Oshana (1998) advocates a strong condition for autonomy, arguing that, to exercise autonomy properly, a person must reject abusive and oppressive social relations that contribute to the formation of their practical identity. Christman (2004) defends the autonomy of those who, for religious or ideological reasons, authentically embrace subservient relationships. Mackenzie (2008) defends weak relational autonomy, in contrast to Oshana, arguing that, to exercise autonomy, the social environment should facilitate intersubjective recognition, which constitutes an affective attitude towards oneself.

I adopt Mackenzie's (2008) account of autonomy because I believe that those social relationships that do not provide a person with the recognitive basis necessary to sustain their affective attitudes towards themselves are inimical to autonomy, rather than advocating the strong idea that oppressive social conditions undermine autonomy or even

the idea that a person is autonomous insofar as they adequately reflect on social conditions and embrace them.

3.1.3. Personal Autonomy

Instead of discussing moral autonomy, Rössler (2005) focuses on personal autonomy, referring to it as general personal self-determination concerning how a person wants to lead their life. A person must be able to ask themself practical questions about how they want to live, what sort of person they want to understand themself as, and what kind of life is good for them. Additionally, a person must be able to make decisions from this perspective and live in accordance with such decisions. Instead of reflecting on the reasons for actions, a person must reflect on their own life. To ask oneself practical questions and to live accordingly is to be autonomous.

Three features characterize Rössler's (2005) theory. First, unlike moral autonomy, personal autonomy is not exclusively bound to a strong notion of rationality. A person is autonomous in the sense of having their own good reasons if they can understand themselves as the author of an action. However, this point need not simultaneously mean that other people accept these reasons, nor does it imply that reasons must be public or shareable. A person's choice or action incorporates personal feelings, obligations, memories, and biographical influences that may not appear equally sensible or convincing to everyone.

Second, regarding personal conditions, Rössler's (2005) conception of autonomy involves the genesis of desires, goals, and projects (see Section 3.2). As Williams (1976) highlighted, Kantian moral philosophy focuses on principles that apply universally, regardless of personal desires or the particular circumstances in which a person is situated. However, it is important to recognize that different people have different sets of desires, concerns, or projects for living their lives. It is not through having one's project affirmed by anyone that the person will have earned their place in the world; rather, a person will have made a distinctive contribution to the world if their distinctive project is realized (Williams 1976). William's objection to Kantian moral autonomy does not encompass personal autonomy, as the personal autonomy presented by Rössler (2005) incorporates personal elements within itself.

Third, Rössler (2005) also emphasizes that intersubjectivity is generally intrinsic to the process of autonomy in various respects, concerning both the genesis of autonomy and the question of what aims and projects a person wants and is able to pursue. In this regard, Rössler extends the concept of personal autonomy to include relational autonomy.

3.2. Three Components of Persoanl Autonomy

Rössler's (2005) analysis focuses on the necessary and sufficient components for the concept of autonomy. Rössler posits that an autonomous person is one who asks oneself the practical question, which involves considering how one is to behave in certain situations given certain desires, one's own history, and one's convictions. This approach means asking oneself which desires or convictions one wants to identify with, how to assess specific desires or preferences in their genesis, and which fundamental life projects are involved in the evaluation and appraisal of this identification. The concept of personal autonomy comprises three components: authenticity and identification, the history and genesis of desires, and goals and projects. I adopt these three necessary and sufficient components of the concept of autonomy proposed by Rössler (2005) as a basis for analyzing autonomy, and I refine them by considering relational autonomy.

Using van de Poel's (2009, 2013) methodology, the analysis reveals the link between autonomy and privacy is in the top layer of a values hierarchy. The connection between these values becomes more detailed by analyzing the components of autonomy, a task

undertaken in the following section. Section 4 discusses how privacy connects to autonomy by identifying privacy norms that should be met to promote autonomy.

3.2.1. Authenticity and Identification

The first component of the concept of autonomy is authenticity and identification. The authenticity condition specifies that, for a person to be autonomous, their beliefs, desires, value commitments, decisions, or actions must be authentically theirs, in the sense that they can identify with their desires, goals, and values as their own (Henschke 2017; Rössler 2005; Williams 1976).

A person is autonomous if their desires and subsequent actions are their own, meaning they are authentically theirs and do not feel alienated from them (Mackenzie 2008). To achieve this, a person must reflect on their desires, motivations, and values. Hence, a person must be able to, and in a position to, reflect on certain desires and, based on such reflections, accept, reject, or modify them. Therefore, the act of identification must be understood as evaluative (Rössler 2005). There are different ways to establish the connection between autonomy and an agent's identity or evaluative first-person perspective, for example, the reflective endorsement of one's desires and values (Korsgaard 1996) and identification with one's will (Frankfurt 1971).

The process of establishing authenticity and identification is not entirely free from social influences; it occurs within intersubjective relations. Nevertheless, this does not mean the social conception of self and the personal conception of autonomy are contradictory. Autonomy requires the internal integration of one's self, and since the self is constituted by social factors, a person acquires autonomy by reflecting on aspects of their character defined in the external relations they have with others (Christman 2004).

Following the recognition-based relational view of Mackenzie (2008), an agent's autonomy depends on intersubjective relationships that provide a basis for one's recognition. A person is autonomous if they can, and are in a position to, reflect on a practical identity or self-conception underpinned by certain affective attitudes constituted by society and developed in intersubjective relationships (Mackenzie 2008).

3.2.2. The Genesis of Desires

Authentic identification with a desire does not necessarily guarantee a person is genuinely autonomous, as the desire might be a product of manipulation. A person is autonomous regarding beliefs, desires, value commitments, or decisions only if, were they to reflect on the historical process of their formation, they would learn they are not products of manipulation. Considering this point, the historical component becomes integral to the conception of autonomy. Hence, both authenticity and identification and the genesis of desires are sufficient and necessary components of autonomy (Rössler 2005).

Reflecting on the genesis of desires helps a person avoid self-deception and manipulation, enabling them to develop a non-manipulative relationship with themselves (Rössler 2005). Moreover, concerning the intersubjective and social conditions under which autonomy is learned or acquired, reflecting on the formation of certain attitudes towards oneself is required to prevent a person becoming involved in oppressive and abusive interpersonal relationships. Although it might be demanding to be free from manipulative external circumstances in the strong sense defended by Oshana (1998), it is necessary in a weaker sense. A person must live in social conditions that do not deny them a form of recognition, as defended by Mackenzie (2008). Hence, reflection is necessary to prevent a person from engaging in social relationships that do not grant them appropriate recognition.

3.2.3. Goals and Projects

In addition to authenticity and identification and the genesis of desires, the third component of the conception of autonomy concerns a person's goals and projects. To be autonomous, a person must have the ability and be in a position to form goals and design projects and to pursue these in practice (Rössler 2005).

Rössler's (2005) argument does not explicitly refer to the diachronic dimensions of autonomy; however, it involves conceiving of autonomy in reference to personal history and the genesis of desires, which has retrospective elements. The argument is also related to making plans about the component of goals and projects, which have prospective elements. Considering both retrospective and prospective elements endorse that autonomy (specifically the self-governing dimension of it) is a diachronic, temporally extended process. This claim is defended by Bratman (2007), Christman (2009), and Mackenzie (2023).

As Mackenzie (2023) states, one way of conceptualizing the diachronic dimension of autonomy is Bratman's (2007) planning account. In that account, the temporally extended structure of autonomy is defined by a person perceiving their agency as extending both backward into the past and forward into the future. Considering the past through memories and envisioning the future through intentions and plans, a person establishes connections that bind their present to both their past and future. Mackenzie emphasizes that, according to the planning account, a person establishes these connections and organizes their activities over time by forming intentions, planning the means to realize those intentions, and enacting prior intentions (Bratman 2007; Mackenzie 2023). Autonomy is shaped over time by a person's intentions and plans orientating their reflections. To be autonomous is to form intentions, make plans, and direct one's life in accordance with those plans.

The temporally extended dimension of autonomy is shaped in relation to contingencies, social relations, and the social environment (Mackenzie 2023). The contributory role of social conditions in this component of autonomy can be explained in two ways. First, the goals, projects, and ways of life available to a person are determined by specific cultural assumptions and social contexts. An autonomous person can reflect on how they are situated in cultural, social, and intimate contexts and incorporate this reflection into forming part of their goals and projects (Rössler 2005). Second, involvement with particular other people might be one of the kinds of projects that figure in a person's life. An autonomous person can develop and sustain relationships with others with whom certain affective attitudes are formed.

The functional value of privacy is realized when a person can live their life autonomously. The conception of autonomy is explained precisely by analyzing the three necessary and sufficient components. Thus, the value of privacy is understood as a means to protect and promote the three components of autonomy, which is the aim of the top layer of a values hierarchy—to explore relationships between values. The intermediate layer explores the relationships between privacy and autonomy by identifying norms that promote autonomy.

4. The Layer of Norms: Norms for Promoting Personal Autonomy

Following van de Poel (2009, 2013), the intermediate layer of a hierarchy comprises norms translated from the upper layer of values. Based on the previous section, the functional value of privacy depends on autonomy. In this section, I go beyond the commonly recognized norm of reflection within the three components of autonomy—reflection on self-conception, reflection on the genesis of desires, and reflection on goals and projects. I specifically identify additional norms that must be met for an individual to be autonomous, focusing on autonomy's components to realize the functional value of privacy. By delineating these norms, I explore the connection between privacy and each component of autonomy in detail.

4.1. Authenticity and Identification

According to Mackenzie's (2008) view, a person must perceive themselves as the legitimate source of authority over their decisions and actions. This normative authority is grounded in one's attitudes towards themselves, which are intertwined with interpersonal relationships and the social structures of mutual recognition (Mackenzie 2008). Consequently, promoting autonomy involves fostering the interpersonal and social conditions necessary for its development and exercise. Furthermore, to foster autonomy, social circumstances should provide a basis for recognition that enables a person to realize their autonomy.

To promote autonomy, regarding relational autonomy, which emphasizes that autonomy is developed and sustained intersubjectively, a person must be able to situate themselves in a network of intersubjective relationships governed by various social norms, in which they see themselves in different roles, such as a friend, colleague, and wife. Moreover, as Mackenzie (2008) argues, for a person to be recognized within their social network, a series of interconnected obligations on the part of the social network must be fulfilled. These obligations include treating a person as someone with a conception of themselves and for whom certain things matter, as well as understanding the subjective perspective regarding one's situation.

To explore the relationships between privacy and autonomy, moving away from conceiving autonomy as detachment from social life to viewing it as socially embedded helps to explain privacy discourses. Scholars in privacy studies who recognize relational or social autonomy have argued that not only does privacy protect autonomy by preserving engagement in social interactions, but it also facilitates the social relationships required for a person to be able to exercise their autonomy (Rössler and Mokrosinska 2013).

In philosophical literature, privacy is commonly defined as control over access to oneself or one's information (Rössler 2005; Westin 1967). A person who has control over their information can determine what they disclose to others and what they conceal from them. Given that relationships between people can be differentiated according to the degree of personal information they share, the ability of individuals to disclose and conceal information to and from others enables them to form various social relationships. Hence, privacy regulates and facilitates the enactment of social relationships (Rössler 2005; Rössler and Mokrosinska 2013).

In accordance with Rachels's (1975) perspective, Rössler and Mokrosinska (2013) highlight that informational management within relationships comprises two aspects: a subjective aspect, linked to an individual's ability to control information, and an intersubjective aspect imposed by the type of relationship. Intersubjectively shared standards grounded in the purpose of social relationships determine the relevance of information to those relationships. What others, such as students or bankers, know about me is largely determined by the specific kind of relationship I am engaged in and the roles assumed within that relationship. Therefore, privacy involves an individual's control over access to their information by others, with the degree of control the individual possesses depending on the character of the social roles they perform and the nature of the social relations in which they participate (Rössler and Mokrosinska 2013).

Privacy is understood as a means of promoting a person's autonomy by fostering various social relationships and cultivating the social conditions required for the development and exercise of autonomy. Therefore, norms aimed at promoting autonomy, considering the first component of autonomy (i.e., authenticity and identification), involve, first, that individuals should have control over others accessing their information to maintain different social relationships. This control enables individuals to decide whether to disclose some information to certain people or conceal it from others. Second, individuals should be aware of the type of relationships they will be involved in to decide which information to share. Third, as mentioned earlier in this section about the

intersubjective aspect of privacy, social circumstances should provide a basis for one's recognition by others in intersubjective relationships.

4.2. The Genesis of Desires

The historical component of the conception of autonomy is necessary to prevent a person from falling into self-deception and manipulation, enabling them to escape the external circumstances that underpin destructive attitudes towards themselves. Unlike Oshana (1998), who maintains the strong view that a person must be free from manipulative external circumstances to be autonomous, and unlike Christman (2004), who argues that, in certain circumstances, we may accept a desire or approve certain ways of acting or behaving even once we understand they resulted from manipulation, Mackenzie's (2008) view posits that those social circumstances that erode one's normative authority over their decisions and actions compromise autonomy.

Manipulation involving personal information might occur in two cases. First, manipulation arises when personal information about an individual is used in a way that prompts that person to take a particular action. The case I am discussing is similar to those instances in which a company, having accumulated significant private data on a person, uses this information to manipulate them, for instance, through targeted advertising. Although manipulation can also occur in cases in which a person is forced to do things they might not otherwise do, such as in blackmail cases, these cases differ from the ones to which I refer. The manipulation I discuss here occurs because of the detailed information others have obtained about a person, not because of disinformation.

Second, manipulation might arise from software and user interface designs that afford certain actions, particularly the act of sharing personal information. These designs can manipulate a person by triggering cognitive biases, leading them to divulge more information than they intend to. One strategy to manipulate a person in this way is to present the information—about what happens to shared data and who accesses them—in such a way, both in terms of content and design, that it prompts them to share personal information they would not otherwise disclose.

As highlighted by Nissenbaum (2010), the relationship between privacy and autonomy is not restricted to one's ability to reflect on principles of actions and having the freedom to act according to them. The relationship also involves one's ability to carry out those actions without being manipulated by others or circumstances, which can influence the shaping of one's choices and actions (Nissenbaum 2010). In the first case, the manipulation that deprives one's autonomy occurs due to the absence (or invasion) of one's privacy. In this regard, privacy is required to mitigate the problem of manipulation. A person can only exercise control over their personal information when they know what is being done with their information, meaning they will be less susceptible to such manipulation.

In the second case, the person is exposed to information that triggers a specific cognitive bias, known as the metacognitive decision-making process (see Section 5.2), manipulating them into sharing their personal information (Waldman 2020). To prevent manipulation that erodes one's autonomy, measures should be taken to prevent system designers or developers from providing information that triggers cognitive biases. The content of the information presented in privacy notices and how it is presented are important (see Sections 1 and 5.3) for preventing manipulation and, ultimately, protecting one's autonomy.

Based on the two cases discussed above, two norms related to the historical component of autonomy regarding the mitigation or prevention of manipulation are derived. First, a person should be able to exercise control over their information to become less susceptible to manipulation. Second, the action of sharing personal information should be guided by one's intention or authentic desires rather than being caused by (external) factors triggering certain cognitive bias; the action of sharing should be formed

by this reflective process rather than being a mere reaction to the conditions prompting a person to share their information. Thus, privacy notices (see Sections 1 and 5.3) should prevent a person from being trapped by cognitive bias, thereby avoiding the unintended divulgence of their information.

4.3. Goals and Projects

The third component of the conception of autonomy, according to Rössler (2005), emphasizes that, to be autonomous, a person must be able to form goals and design projects by considering the social context in which they are situated and including the development of relationships with others. Furthermore, being autonomous is not solely about the ability to form intellectual plans; rather, an autonomous person can pursue their goals and projects in practice as well.

Regarding Bratman's (2007) planning account, autonomy is developed over time through a temporally extended process that involves the formation of intentions, the planning of means to realize those intentions, and the enactment of prior intentions that guide deliberation. To guide deliberation effectively, intentions and plans must meet certain norms, specifically means-end coherence. Means–end coherence helps guide deliberation by concentrating one's planning activities. For example, if a person aims to achieve an end, such as improving their fitness, this requires them to figure out the best means of doing so, meaning it is necessary to develop plans and subplans (Mackenzie 2023).

Regarding the sharing of personal information using PIMS, if a person intends to share such information as part of a plan, perhaps to enhance their health, they should assess whether PIMS is an effective means for achieving that end. PIMS, which enables a person to share their information, is an effective means to realize their end if the purpose for which the information is collected using the system aligns with the person's intended purpose. For a person to decide whether PIMS coheres with their goals, privacy notices embedded in the system should clearly state the purpose for which information is collected; for example, the collected information is fed as input into a machine learning model developed to detect a disease, helping individuals to decide about whether to use PIMS as a means to realize their goals (see Section 5.3).

Moreover, individuals should be able to assess and consider different alternatives for sharing information and choose the one that aligns with their objectives. Based on these alternatives, individuals can make meaningful decisions about sharing their information for specific purposes. Thus, privacy choices (see Sections 1 and 5.3) should enable a person to pursue their own choices.

5. The Layer of Design Requirements: Design for the Value of Privacy

Having outlined the norms in the second layer, the final step is to translate these norms into design requirements, comprising the lowest layer of the hierarchy. As I mentioned in Section 4, reflection is a common norm among the three components of autonomy, encompassing reflection on self-conception, reflection on the genesis of desire, and reflection on goals and projects. Therefore, a deliberate approach to designing for reflection is required to align with these overarching norms. Terpstra et al. (2019) suggest that *designing for reflection* can enable individuals to reflect.

As highlighted by Terpstra et al. (2019), reflection can be triggered by the introduction of friction. These scholars emphasize that deliberately incorporating friction into a design enables individuals to escape the habits of thought and behavior to reflect critically on their actions and decisions. Friction is commonly understood as anything that obstructs a user in the completion of the tasks they typically perform without conscious thought, thereby instigating reflective thinking. Designers can embed friction into their

designs by pre-emptively discerning a user's habitual behavior and devising strategies counter to it (Terpstra et al. 2019). Mackenzie (2000) highlights that representational or imagistic thinking is integral to the process of self-reflection and deliberation. Representational imagining can open up a space within which a person can step away from their habitual modes of understanding themselves and their relationships with others. Within this mental space, a person can explore different possibilities for themselves. At its core, the ability to imagine ourselves in different ways plays an important role in practical reflection and deliberation about the self (Mackenzie 2000).

Regarding the above discussions, friction can be used to trigger imagination, enabling a person to reflect on their desires, actions, decisions, and what matters to them. Thus, friction, understood as affording reflection and imagination, is a way of promoting autonomy. For instance, friction can be achieved by asking specific questions that prompt individuals to imagine themselves in certain situations in the present or even the future, while sharing their information with others. The inclusion of specific questions is a high-level requirement for incorporating friction (to trigger imagistic thinking) into design. The specific content of such questions, the ways they are presented, and the provision of explanations to users regarding why such questions are asked necessitate empirical investigation.

In addition to designing for reflection to meet the common norm in the three components of personal autonomy, the norms identified in Section 4 need to be translated into design requirements, which is the focus of the remaining sections.

5.1. Authenticity and Identification

The norms related to promoting autonomy concerning its first component (i.e., authenticity and identification) are that individuals should have control over access to their information by others; they should be aware of the types of relationships they are involved in to share their information accordingly; and the social network people participate should treat them as people for whom certain things matter, for example, which pieces of their personal information are shared with whom for which purpose. In this section, these norms are translated into design requirements.

Privacy regarding control over access to their information by others protects against unwanted or unauthorized access to information (Rössler 2005). Given that unauthorized access to one's information leads to a loss of control and infringement of one's privacy, the sufficient condition—though not necessarily a necessary one—for losing control is unauthorized access.[3] A measure to ensure a person maintains control over their information involves restricting unauthorized access to that information. Encryption is a valuable measure for protecting the sharing of information from unauthorized access. Employing encryption to protect privacy was proposed by Miller and Bossomaier (2021). Encryption works by converting data into a code that can be deciphered only by individuals who possess the correct decryption key. When data are encrypted, even if they are intercepted by a third party, that party should not be able to understand or make use of them without the decryption key (Coron 2006).

To fulfil the next two norms, which share the intersubjective element, I suggest using contracts, which identify the purpose of sharing information and the person or parties with whom that information will be shared, as well as providing instructions for caring for the data (Christidis and Devetsikiotis 2016). The purpose of contracts in contexts in which information is shared is to record how parties care about shared personal data and to serve as a reference to guide parties' activities. The contract emphasizes factors such as

[3] I thank an anonymous reviewer for highlighting the point that one of the most effective measures to prevent unauthorized access is multi-factor authentication. In this approach, a user is required to provide multiple forms of identification before being granted access (Ometov et al. 2018) to PIMS.

how caring about shared data matters for the person who shared them and how receivers care for something senders (or data subjects) care about. These aspects allow for a distributed consensus on a transaction and the sharing of data, ultimately facilitating mutual recognition.

PIMS should implement measures to restrict unauthorized access by third parties seeking to process user data. This system ensures that, even if an unauthorized third party gains access to encrypted data, they cannot decipher them without the proper cryptography key. Moreover, PIMS should execute contracts (or smart contracts). One way of meeting the needs of contracts and utilizing encrypted data is through the use of blockchain. Blockchain is a technology using cryptographic hash functions to store and distribute sensitive data (Hölbl et al. 2018; Khezr et al. 2019), and it has a feature that can execute smart contracts (Christidis & Devetsikiotis, 2016); therefore, PIMS should employ blockchain to fulfil the aforementioned norms.

5.2. The Genesis of Desires

The two norms described in Section 4.2 are associated with the historical component of the conception of autonomy. First, a person should be able to exercise control over their personal information to be less susceptible to manipulation. This norm necessitates that a person should know what is being done with their personal information. Second, the act of sharing information should be guided by one's intentions or authentic desires rather than being caused by or reacting to external factors. One way to realize this norm is to design privacy notices to prevent certain cognitive biases. These biases might otherwise manipulate individuals into unintentionally sharing their personal information. The design requirements derived from the control norm—which necessitates awareness of the purpose for which data are collected—are detailed in Section 5.3. This section outlines the design requirements associated with the second norm.

Platforms usually employ design tactics to manipulate users into disclosing more information than they initially plan to share, sustaining an information-driven business model. This manipulation frequently arises from implementing what are commonly referred to as 'dark patterns' in platform design. Designers employ such patterns to coerce and deceive users into disclosure and to trigger cognitive biases that prompt users to divulge information they might otherwise withhold (Waldman 2020).

Using dark patterns can trigger a cognitive bias known as the metacognitive decision-making process (Waldman, 2020). This bias hinders individuals' abilities to make choices that align with their preferences. When individuals encounter challenging decisions, some interpret the complexity as an indication of its importance, motivating them to engage in thoughtful deliberation when making choices. However, when individuals view difficulty as a signal that the task is impossible, they tend to be more likely to give up on their choices. This second approach indicates that, when individuals face challenges in making choices about sharing their personal information due to complex notices, as many often do, they become more inclined to avoid limiting the disclosure of their information (Waldman 2020). Designing to promote the metacognitive decision-making process can lead to the manipulation of users, prompting them to share more information than they desire or intend to.

To design PIMS to counter dark patterns, designers should present information using a plain and transparent design and language, encouraging users to make decisions by reading notices. To achieve this aim, designers must provide meaningful notices that are concise and easily understood by the majority of individuals, not just legal experts. Transparent design methods, such as using tables with appropriate fonts and colors (as explained in Section 1), can aid in this effort. Moreover, designers need to encourage users to manage their privacy by providing feedback that clearly illustrates how user choices impact the real world. As privacy choices are a process, the system must offer clear and

timely feedback that reflects the most recent user actions, indicating that privacy settings have been modified in accordance with their latest choices (Feng, Yao, and Sadeh 2021).

5.3. Goals and Projects

At this stage, the specific norms concerning goals and projects should be translated into design requirements. These norms encompass two key aspects: first, individuals should be made aware of why their personal information is collected and shared with others; and second, individuals should be able to assess and consider different alternatives for sharing information, and based on this assessment, they should choose and pursue their goals. The effective (in the sense of the information provided to individuals about the data collected about them and their usage) design of the notice fulfils the first norm, and the efficient (in the sense of enabling individuals to manage their own privacy preferences and interests) design of the choice aids in realizing the second norm.

The effective design of notices discourages users from habitually accepting the notices without considering their content, helping users pay attention to data practices. The content, presentation, inclusiveness for different audiences, and integration of notices into PIMS are all crucial factors for achieving effective notices. Regarding content, well-designed notices should notify individuals about the data practices of PIMS. This aspect includes specifying what data are being collected about individuals, for which purposes, with whom they are shared, why, and how long they are stored (Schaub et al. 2018). Furthermore, information should be presented in a manner that effectively and transparently communicates these data-collection and data-sharing purposes to individuals, helping them to decide about sharing their information. When the purpose is clearly stated in the notice, users are aware that, by sharing their information, they can achieve their desired outcome. Notices should also inform users about the options available to control or prevent certain data-sharing practices.

For the effective design of notices, the audience and how the notices are presented should be considered. Regarding the audience, effective notices need to consider a wide range. Notices are typically conveyed through text, images, or icons, and it is important to incorporate auditory methods to inform the visually impaired community. Notices are often presented separately and detached from the individual's interaction with the system, such as being placed at the bottom of a page. However, to maximize the effectiveness of a design, notices should be seamlessly integrated into PIMS, so individuals do not need to seek them out but encounter and engage with them as part of their interaction with the system and read them (Schaub, Balebako, and Cranor 2017).

In addition to the design of notices, the design of choices should be structured to provide individuals with control over certain aspects of data practices and accommodate diverse user preferences. Rather than presenting a binary choice design that restricts individuals' abilities to express their preferences, designers should employ multiple choices. For example, mobile platforms, such as Android and iOS, offer users various ways to decide how they want to allow apps to access the location data collected by their devices, including 'always', 'while using the app', 'never', and, more recently, iOS has introduced 'just once' (Feng, Yao, and Sadeh 2021). If the different options are clearly explained, they do not create a cognitive load for people to follow and understand what each option means, meaning it is less confusing for people to decide.

6. Summary

A summary of Sections 3–5, each dedicated to a different layer of a values hierarchy, is illustrated in Figure 1. The values are in dark grey in the top layer, and the connection between the instrumental value of privacy and the three components of autonomy is depicted in this layer. The middle layer is dedicated to the norms associated with each component of autonomy, displayed in light grey. Since reflection is a common norm, it appears in each component. The bottom layer is dedicated to the design requirements (in

white) derived from the translation of the norms. Although some design requirements are linked immediately to the upper level—for example, imagination can be triggered by friction—in some cases, there is no immediate link; for instance, the inclusiveness of the audience is connected to the effective notices placed two levels above it.

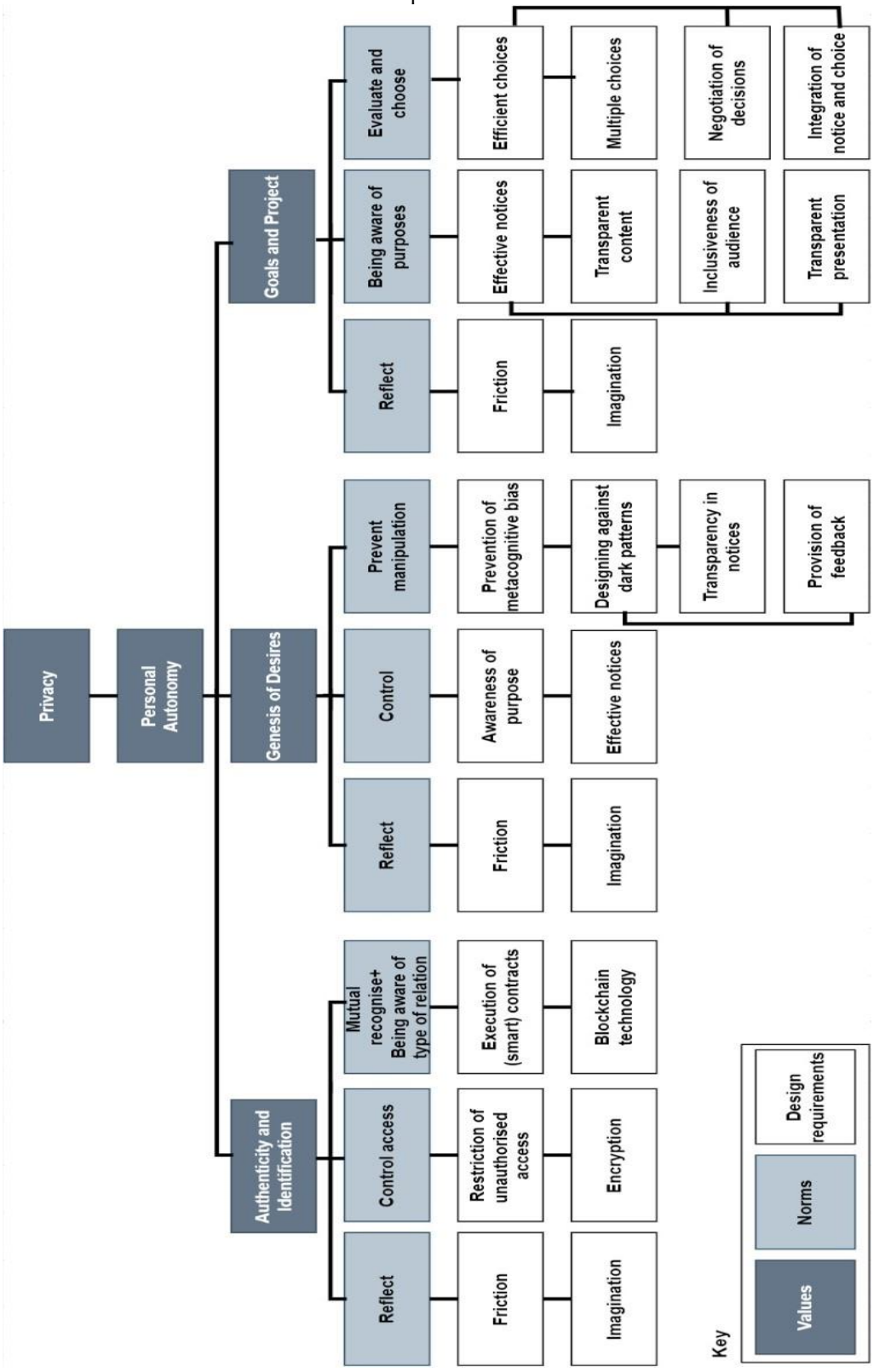

Figure 1. Possible Values Hierarchy for Privacy

7. Conclusion

This research proposed design requirements for embedding the value of privacy into PIMS. To achieve this goal, a three-layered values hierarchy was constructed. The first layer, dedicated to values, elucidated the connection between privacy and personal autonomy; privacy is functionally valuable for the sake of autonomy. In accordance with the three components of autonomy, namely authentication and identification, the genesis of desires, and goals and projects, the functional value of privacy was discussed. The second layer, dedicated to norms, identified commons and specific norms concerning the components of autonomy, considering that the value of privacy is realized when a person's autonomy is protected or promoted. In the third layer, design requirements were derived by translating the identified norms. Regarding the common norm, the design for reflection should be incorporated into PIMS. Concerning the specific norms, designing to prevent unauthorized access, to counter dark patterns, and to provide effective and efficient notices and choices related to the three components of personal autonomy, respectively, should be considered in the design of PIMS. The findings from this study contribute to the literature on privacy by design, emphasizing the incorporation of value into the design of PIMS and elevating it beyond mere legal compliance and privacy policy adherence throughout the system-development lifecycle.

Author Contributions: Haleh Asgarinia is the single contributor of this paper.

Funding: "This research was funded by PROTECT- Protecting Personal Data Amidst Big Data Innovation' project, funded by the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No. 813497."

Institutional Review Board Statement: "Not applicable."

Informed Consent Statement: "Not applicable."
Data Availability Statement: "Not applicable."

Acknowledgments: I wish to extend my special thanks to Dr. Adam Henschke for the helpful advice and comments that improved the quality of my paper and for the insightful discussion that contributed to the development of the ideas presented in this paper.

Conflicts of Interest: "The author declare no conflict of interest."

References

1. Asgarinia, H., Chomczyk Penedo, A., Esteves, B., & Lewis, D. (2023). "Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies. *Information*, *14(7)*(351). https://doi.org/10.3390/info14070351
2. Barocas, S., & Nissenbaum, H. (2009). *On Notice: The Trouble with Notice and Consent* (SSRN Scholarly Paper 2567409). https://papers.ssrn.com/abstract=2567409
3. Benson, P. (1994). Free Agency and Self-Worth. *The Journal of Philosophy*, *91*(12), 650–668. https://doi.org/10.2307/2940760
4. Bratman, M. E. (2007). *Structures of Agency: Essays*. Oxford University Press.
5. Brey, P. (2010). Values in technology and disclosive computer ethics. In L. Floridi (Ed.), *The Cambridge Handbook of Information and Computer Ethics* (pp. 41–58). Cambridge University Press.
6. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
7. Christman, J. (2004). Relational Autonomy, Liberal Individualism, and the Social Constitution of Selves. *Philosophical Studies*, *117*(1), 143–164.
8. Christman, J. (2009). The historical conception of autonomy. In *The Politics of Persons: Individual Autonomy and Socio-historical Selves* (pp. 133–163). Cambridge University Press.
9. Coron, J.-S. (2006). What is cryptography? *IEEE Security & Privacy*, *4*(1), 70–73. https://doi.org/10.1109/MSP.2006.29
10. EU Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and

repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) Doc Type: R Usr_lan: En. OJ L. Vol. 119. http://data. europa.eu/eli/reg/2016/679/oj/eng.
11. Feng, Y., Yao, Y., & Sadeh, N. (2021). A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–16.
12. Frankfurt, H. G. (1971). Freedom of the Will and the Concept of a Person. *The Journal of Philosophy*, *68*(1), 5–20.
13. Friedman, B., Jr, P. H. K., & Borning, A. (2008). Value Sensitive Design and Information Systems. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 69–101). John Wiley & Sons, Inc.
14. Goffman, E. (1959). *The presentation of self in everyday life*. Doubleday.
15. Grannis, A. (2015). You Didn't Even Notice: Elements of Effective Online Privacy Policies. *Fordham Urban Law Journal*, *42*(5), 1109–1170.
16. Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge University Press.
17. Henschke, A. (2021). From need to share to need to care: Information aggregation and the need to care about how surveillance technologies are used for counter-terrorism. In S. Miller, A. Henschke, & J. F. Feltes, *Counter-Terrorism* (pp. 156–168). Edward Elgar Publishing.
18. Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry*, *10*(10), Article 10.
19. Janssen, H., & Singh, J. (2022). Personal Information Management Systems. *Internet Policy Review*, *11*(2), 1–6.
20. Kant, I. (1993). *Grounding for the metaphysics of morals ; with, On a supposed right to lie because of philanthropic concerns* (J. W. (James W. Ellington, Trans.). Indianapolis : Hackett Pub. Co. http://archive.org/details/groundingformet000kant
21. Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences*, *9*(9), Article 9.
22. Korsgaard, C. M. (1996). *The Sources of Normativity* (O. O'Neill, Ed.). Cambridge University Press.
23. Korsgaard, C. M. (2009). *Self-Constitution: Agency, Identity, and Integrity*. Oxford University Press.
24. Mackenzie, C. (2000). Imagining Oneself Otherwise. In C. Mackenzie & N. Stoljar (Eds.), *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self*. Oup Usa.
25. Mackenzie, C. (2008). Relational Autonomy, Normative Authority and Perfectionism. *Journal of Social Philosophy*, *39*(4), 512–533.
26. Mackenzie, C. (2023). Autonomous agency, we-agency, and social oppression. *The Southern Journal of Philosophy*, *61*(2), 373–389.
27. Mackenzie, C., & Stoljar, N. (2000). Introduction. In C. Mackenzie & N. Stoljar (Eds.), *Relational Autonomy Feminist Perspectives on Autonomy, Agency, and the Social Self*. Oxford University Press.
28. McLeod, C. (2002). *Self-Trust and Reproductive Autonomy*. MIT Press. https://mitpress.mit.edu/9780262537230/self-trust-and-reproductive-autonomy/
29. Miller, S., & Bossomaier, T. (2021). Privacy, Encryption and Counter-Terrorism. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism* (pp. 139–154). Springer International Publishing.
30. Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.
31. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), Article 1. https://doi.org/10.3390/cryptography2010001
32. Oshana, M. A. L. (1998). Personal Autonomy and Society. *Journal of Social Philosophy*, *29*(1), 81–102.
33. Rachels, J. (1975). Why Privacy is Important. *Philosophy and Public Affairs*, *4*(4), 323–333.
34. Riesman, D. (1952). *Faces in the Crowd: Individual Studies in Character and Politics*. Yale University Press.
35. Rössler, B. (2005). *The Value of Privacy | Wiley*. Polity.
36. Rössler, B., & Mokrosinska, D. (2013). Privacy and social interaction. *Philosophy & Social Criticism*, *39*(8), 771–791.
37. Schaub, F., Balebako, R., & Cranor, L. F. (2017). Designing Effective Privacy Notices and Controls. *IEEE Internet Computing*, *21*(3), 70–77.
38. Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2018). A Design Space for Effective Privacy Notices*. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (1st ed., pp. 365–393). Cambridge University Press.
39. Solove, D. J. (2008). *Understanding Privacy* (SSRN Scholarly Paper ID 1127888). Social Science Research Network. https://papers.ssrn.com/abstract=1127888
40. Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126:1880*, 1880–1903.
41. Terpstra, A., Schouten, A. P., Rooij, A. de, & Leenes, R. E. (2019). Improving privacy choice through design: How designing for reflection could support privacy self-management. *First Monday*. https://doi.org/10.5210/fm.v24i7.9358
42. van de Poel, I. (2009). Values in Engineering Design. In *Philosophy of Technology and Engineering Sciences* (pp. 973–1006). Elsevier.
43. van de Poel, I. (2013). Translating Values into Design Requirements. In D. P. Michelfelder, N. McCarthy, & D. E. Goldberg (Eds.), *Philosophy and Engineering: Reflections on Practice, Principles and Process* (Vol. 15, pp. 253–266). Springer Netherlands.
44. Véliz, C. (2021). *Privacy is Power: Why and How You Should Take Back Control of Your Data*. Bantam Press.
45. Waldman, A. E. (2016). Privacy, Notice, and Design. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2780305
46. Waldman, A. E. (2018). Privacy, Notice, and Design. *STANFORD TECHNOLOGY LAW REVIEW*, *21:129*. https://digitalcommons.nyls.edu/fac_articles_chapters/1330
47. Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox.' *Current Opinion in Psychology*, *31*, 105–109.

48. Westin, A. F. (1967). Privacy And Freedom. *Washington and Lee Law Review*, *25*(1), 166–170.
49. Williams, B. (1976). Persons, Character, and Morality. In J. Rachels (Ed.), *Moral Luck: Philosophical Papers 1973?1980*. Cambridge University Press.