Healing Privacy Wounds with SPLINT: A Psychological Framework to Preserve Human Well-Being during Informational Privacy Trade-Offs

Zina Efchary
Hughes Hall, University of Cambridge

This paper explores the critical role of informational privacy in promoting human well-being and flourishing, with particular attention to the challenges posed by Artificial Intelligence (AI) systems. As AI increasingly mediates digital interactions and processes large scales of personal data, controlling the flow of personal information becomes intractable. In response to these evolving challenges, this paper argues for an alternative approach to informational privacy that emphasises its psychological value to support autonomy and positive liberty. To operationalise these values, I adapt Self-Determination Theory (SDT) as a psychological framework, mapping the dimensions of autonomy, relatedness, and competence to the core benefits of informational privacy. Furthermore, by examining the threats posed by predictive AI algorithms to informational privacy in personalised targeting, I argue that conventional privacy measures, such as the notice and consent model, fail to address the psychological challenges to human well-being. In response, I propose a supplementary framework called SPLINT (Self-determined Privacy Loss in Informational Networks and Technologies) and provide concrete application examples of it. This model leverages the psychological insights of SDT to guide the design of mitigation strategies to preserve human well-being even if privacy trade-offs occur. By focusing on preserving the psychological values underpinning informational privacy, SPLINT aims to offer a proactive approach to safeguarding human well-being in AI-mediated digital environments. I conclude that SDT-based approaches like SPLINT provide a progressive, promising starting point to navigate privacy trade-offs, although their wider societal impact as measures and the benefits of informational privacy as a psychological phenomenon require further empirical investigation.

Keywords: Informational Privacy, AI Ethics, Self-Determination Theory (SDT), Digital Well-Being, Predictive AI Algorithms

Introduction

Informational privacy has valuable qualities in preserving personal autonomy and maintaining psychological well-being (Véliz, 2024). Yet, the rapid advancement of AI poses unprecedented challenges to this paradigm. AI systems, particularly those employing predictive algorithms in "personalised targeting", can undermine personal autonomy and interfere with personal development in ways that traditional digital technologies cannot. Thus, the question is how one can benefit from modern AI technologies and yet protect the values of privacy in the presence of trade-offs.

In this paper, I will argue that informational privacy is fundamental for human well-being and flourishing. Thus, it is worth protecting. This is done by focussing on operationalising the psychological values of privacy and using them as a guide to mitigate the threats posed to human well-being by predictive AI algorithms.

Moreover, this paper is divided into four main sections. In section 1, I will define key terms and assumptions to develop a comprehensive account of informational privacy, advocating its protection as essential to human flourishing and well-being. In section 2, I will apply a psychological model to this notion to unpack the psychological values of informational privacy. In section 3, I describe predictive AI algorithms' threats to the introduced values. By applying the developed psychological account as a guide, I introduce a model to mitigate these impacts, aiming to balance privacy trade-offs with human well-being. Finally, in section 4, I conclude that operationalising the values of informational privacy plays a significant role in its protection, pointing at future areas of research.

1. Philosophical Foundations of Privacy

In the following section, I will define some necessary terms and outline my underlying assumptions needed to develop a

comprehensive account of privacy for this paper. My main focus will be on the concept of informational privacy. While defining it, I will differentiate it from other forms of privacy, and clarify its relationship with other moral goods such as autonomy and liberty.

1.1. Defining Privacy

One key aspect towards defining privacy is the distinction between descriptive (what it is) and normative (what it ought to be) approaches. While descriptive accounts focus on privacy as a condition that can be obtained, normative accounts see it as a right, referring to moral obligations. In this paper, I will adopt a normative approach towards informational privacy, defining it as a right to control the flow of personal information.[1]

Informational privacy is distinguished from physical forms of privacy by focusing on the protection and management of data about oneself across domains of life (Koops *et al.*, 2017).[2] For example, while protecting bodily privacy means preventing unwanted physical contact, informational privacy in the AI era involves controlling not just how basic health data is shared, but how AI systems can combine and analyse multiple data streams to make intimate predictions about one's health status and future conditions.

An informative overview to illustrate this widespread nature of informational privacy is provided by Koops *et al.* (2017; See Figure 1).

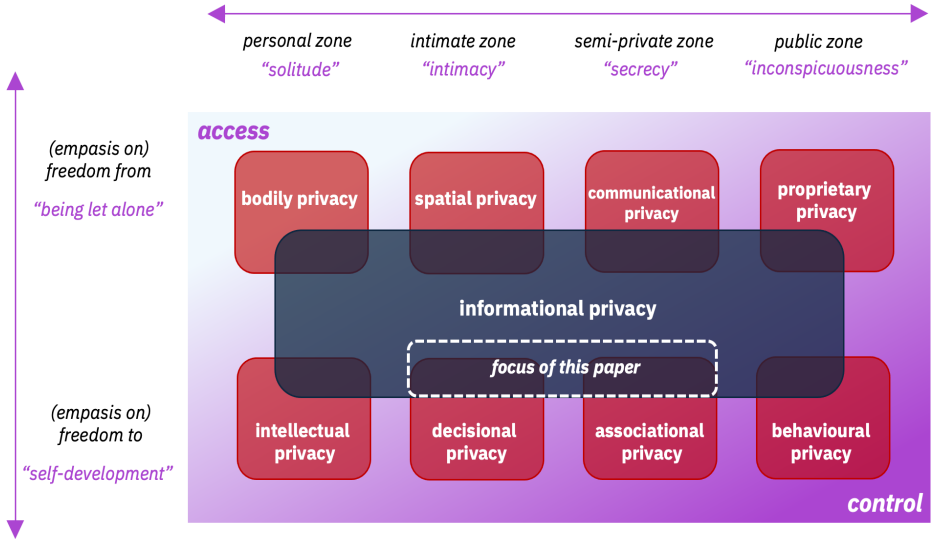

Figure 1: *Typology of Privacy. Adopted from Koops et al. 2017 (modified), illustrates privacy across life's spheres (horizontal) and the spectrum of positive-negative liberty (vertical), against an access-control gradient (shaded background). This is a spectrum between giving initial access to others and restricting the access after it has been given. This paper's primary focus is the informational privacy area (dotted) and its overlap with associational and decisional privacy.*

I adopt this overview, though not elaborating on all privacy types as this would go beyond the scope of this paper. However, there are two final points here that are needed to clarify my account of informational privacy as the focus of this paper:

Firstly, the notion of positive-negative liberty in Figure 1 is based on Berlin's account of liberty (Berlin, 1969), highlighting the balance between "freedom from" (negative liberty) and "freedom to" (positive liberty). In relation to privacy, negative liberty focuses on an individual's right to be free from interference and surveillance, emphasising protection and the right to privacy. Positive liberty, conversely, centres on the individual's ability to make choices and participate freely in society, linking closely to

[1] I adopt the "control over information" definition discussed by Moore (2008). However, I add the notion of the "flow" of personal information borrowed from Nissenbaum (2004) to emphasise that control should not be strictly limited to possession but also include the choice, concerning the extent and appropriateness of sharing information.

[2] These are types of privacy related to the direct objects, vulnerable to observation or intrusion. e.g. spatial privacy.

the control over personal information and engagement in personal relationships. In this paper, I will rather focus on the significance of informational privacy to positive liberty, specifically regarding self-determination and self-development, which I will also elaborate on in the next section.

Secondly, the typology aims to highlight key privacy concepts without being exhaustive or rigid in its classifications. It functions as an analytical framework for this paper, showing the connections between informational privacy and other privacy types, and their links to other moral goods like liberty. Specifically, it helps to define the scope of my argument and clarify its focus at the intersection of associational and decisional privacy. Associational privacy is defined as the right to choose one's social interactions, including friends, groups, and communities. Decisional privacy is concerned with intimate decisions regarding personal matters, emphasising sensitive decision-making over one's development and character. In these contexts, the notion of personal autonomy as another moral good becomes important for my framework.[3]

Having established informational privacy's definition and its relationship with other moral goods within my framework, I will now proceed to elaborate on its values.

1.2. The Normative Values of Informational Privacy

An important distinction relevant to our discussion is whether privacy holds intrinsic value (meaning it should be protected for its own sake) or instrumental value (meaning it should be protected for its relevance to other moral goods). In this paper, I will focus on autonomy and positive liberty as instrumental values of informational privacy. But let me be clear, I am not arguing that privacy is not intrinsically valuable nor am I implying that the values I focus on here are the only ones of significance.

A final assumption under which I will operate is that privacy is a cultural universal, meaning that its values benefit members across different cultures.[4]

Having set up my framework of informational privacy, I will now argue that it is worth protecting because of its normative values towards personal autonomy and positive liberty.

First, let us start with personal autonomy. This is especially important at the intersection of decisional privacy, the right to exercise one's mind and develop oneself in the way one wishes. The act of protecting informational privacy enables personal self-determination. This is a condition for self-governance. It is crucial for engaging in the kind of critical self-reflection that results in personal autonomy, allowing individuals to determine their own course in life based on their unique values and goals (Roessler, 2005).

Controlling the flow of personal information in this context means enabling individuals to proactively shape their environment and themselves as they see fit. For example, consider a young artist who utilises social media to showcase their work. They selectively share their creations, choosing which pieces are known and seen by others and which ones are not. This selective sharing, enabled through informational privacy, allows them to shape their artistic identity in the world on their own terms.

Conversely, the lack of control seems to make individuals vulnerable to external influence, reducing their personal autonomy. To be clear, I am not arguing that an individual is only autonomous if she is not influenced by her environment. In fact, a big part of personal development and making personal decisions involves social interactions – we may seek advice from our parents, and friends, or ask our doctor or lawyer for their expertise. However, personal autonomy is protected, when we are

[3] I define personal autonomy as the individual's capacity to "self-govern". This does not mean that autonomous beings are defined by independence or self-sufficiency, rather that they are capable of setting their own norms and laws.

[4] I acknowledge extreme outliers in cultural attitudes toward privacy, but given the widespread value placed on privacy globally (Moore, 2003), including in WEIRD societies, I assume a broad convergence on the value of privacy in the vast majority of cultures and countries.

the initiator, who decides to consciously share information about ourselves and ultimately given the room and space to make our mind to make autonomous decisions. The problem for personal autonomy arises when external forces use our personal information to influence our decisions, or even manipulate us.[5] An example of such practice was the Cambridge Analytica case, where millions of users' Facebook data was used to profile voters and directly target them with political advertising. This does not mean that any lack of control over information results in manipulation but even, the mere awareness that our actions could be monitored alters our perspective, slowly shaping our behaviours to align more with perceived expectations than our own desires.

Second, and relatedly, informational privacy plays a key role in building voluntary, chosen social relationships. Following our introduced privacy framework, this can be seen at the intersection of associational privacy and informational privacy. Associational privacy describes the individual's capacity to follow their social choices and define their social groups and relations, an act of positive liberty. With regards to the overlaying informational privacy, control over personal information means control over who to share personal information with. As argued by Fried (informational) privacy provides the "means for modulating degrees of friendship" (Fried, 1968). This seems to be the precondition to creating different circles of trust and building deeper social connections such as friendship and love.

For example, imagine a fictional society called "Everknown", in which everyone's personal information is known by everyone. It would be hard to imagine how your social relationship with your partner would be any different compared to a friend or someone you are not even related to. Or imagine the reverse case: Alex wants to keep every information about herself to herself and never opens up to anyone, this seems to make it hard for her to create deeper social relationships. It seems intuitive that we share personal information voluntarily with people we trust and this in turn allows us to be vulnerable, be understood and build more trust. This chosen vulnerability seems to not be fully possible without having control over personal information.

Some may object that while informational privacy affects friendship and trust levels, it is not the only or most vital factor, as relationships also depend on shared experiences, emotional compatibility, mutual respect, and invested time and energy. However, I contend that controlling personal information is a fundamental aspect that allows individuals to shape these relationships on their own terms. My argument does not negate the importance of other factors but rather positions informational privacy as an essential enabler of the other dimensions.

Having established the importance of informational privacy in relation to personal autonomy and positive liberty, some may further object that the concept of privacy is a second-order, reducible right. Reductionists like Thomson argue in this manner, stating that privacy rights are not distinct but rather "a cluster of rights" such as "the right over the person" (Thomson, 1975). Following this line of reasoning, some may object that instead of focusing on protecting privacy, we should focus on autonomy or liberty as more fundamental rights. Informational privacy is indeed related to other moral goods. However, this does not establish that privacy is any less fundamental than the rest. In fact, one can equally argue that privacy is more fundamental than the other rights. For instance, as argued, protecting informational privacy allows individuals to have the space to make their own decisions and self-govern, thus we could view informational privacy as a precondition to personal autonomy. Thus, for our purposes, reductionist objection does not undermine the value of informational privacy. It rather underlines that the protection of informational privacy is as important as protecting other moral goods, and since by protecting informational privacy, we also often protect personal autonomy, we have good reasons to value privacy highly.

To sum up: Informational privacy as control over the flow of personal information is crucial

[5] As manipulation, I define external influences "that (1) are hidden, (2) exploit cognitive, emotional, or other decision-making vulnerabilities, and (3) are targeted" (Susser, Roessler, and Nissenbaum 2019:27)

for shaping both personal autonomy and positive liberty. It enables individual self-determination and the formation of genuine, voluntary social connections. In the next section, I will provide a psychological basis for its values.

2. A Psychological Model as a New Lens for Informational Privacy

To say that informational privacy is crucial to personal autonomy and positive liberty does not fully capture how it enables human well-being and flourishing. To address this, I will now introduce a psychological model to enhance our understanding of the psychological values of informational privacy. This should not be viewed merely as a purely descriptive model aimed at underpinning the psychological values of informational privacy. As I will show in section 3, it will also serve as a useful guide for protecting human well-being in case of privacy trade-offs.

2.1. Self-Determination Theory (SDT)

One such psychological framework is the Self-Determination Theory (SDT), developed by Deci and Ryan (2017). SDT is an empirically well-supported framework, dedicated to understanding and promoting human well-being and flourishing. According to SDT, there are three basic psychological needs that are essential to a human's psychological well-being.[6] These are:

(1) *Autonomy* – defined as the need for self-regulating one's actions and experiences, characterised by voluntary and genuine alignment with one's interests and values.
(2) *Relatedness* – involves feeling socially connected, cared for, and encompassing both receiving support and contributing to others and social groups, crucial for experiencing belonging.
(3) *Competence* – understood as a feeling of mastery and proficiency in life's various contexts.

While informational privacy is not explicitly a psychological need in SDT, I argue that it positively impacts each of these dimensions.

2.2. Mapping Informational Privacy to SDT – The Psychological Values of Informational Privacy

Now I will unpack each of the three psychological needs and map them to the introduced conceptual values of informational privacy. As I will argue they align well, enabling a clear explanation of the psychological benefits of informational privacy through the lens of SDT.

Firstly, starting with autonomy, I argue that our philosophical notion of personal autonomy is consistent with the concept of autonomy as a psychological need outlined in SDT. A self-governed individual who acts in their own interests and values is essentially satisfying their psychological need for autonomy. Building on the argument presented in Section 2 regarding the critical role of informational privacy in personal autonomy, it follows that informational privacy supports this aspect of SDT. It is important to clarify that I am not suggesting that informational privacy is the sole contributor to psychological autonomy. Indeed, there may be additional social, cultural or psychological factors that play a significant role in shaping an individual's sense of psychological autonomy. For instance, Alice may have control over her information, not being targeted by political advertising from Cambridge Analytica, yet choose to vote for a political party against her values because of being peer-pressured by her colleagues at work. In contrast, even if she is psychologically autonomous, losing her informational privacy would put her at risk of also losing her psychological autonomy.

Some may object if she does not realise being manipulated by political advertising, she may still believe to be fully autonomous in her decision and thus, not lose her feeling of psychological autonomy. However, this cannot hold as the defined notion of psychological autonomy puts an emphasis on "genuine" alignment with one's values and interests (Ryan & Ryan, 2019). In contrast, manipulation defined as a hidden influence that exploits vulnerabilities, cannot coexist with a state of psychological autonomy. Thus, for our purposes, we can establish that ensuring

[6] Needs are understood as "nutrients that are essential for growth, integrity, and well-being". Thus, psychological needs are the kinds of needs vital for psychological development and wellness to be sustained (Ryan and Deci 2017:10).

informational privacy contributes positively to psychological autonomy.

Moreover, I argue that protecting informational privacy has a positive impact on an individual's feeling of relatedness within SDT. This is again based on the value of informational privacy to an individual's positive liberty in forming voluntary personal relationships. Recall once again our fictional example Everknown, where all personal information is known by everyone. Let us this time question whether the condition for relatedness in SDT could be met in Everknown. Again, it is hard to imagine different depths of social connections evolving; in other words, concepts such as trust, friendship, or love would have different dynamics and, consequently, perhaps different meanings. However, it does not automatically follow that relatedness would be impossible. In fact, some may argue that since everyone knows everything about everyone, it would be easier to find people with whom one feels related. Yet, relatedness in SDT is more than simple relations, it is about the kinds of relationships that allow an individual to experience a sense of belonging, to care, and to be cared for. And this perhaps requires deeper social connections. While a basic sense of belonging might be achieved in Everknown through various social constructs, such as those between work colleagues or neighbours, this alone does not satisfy the psychological need for relatedness. The control over one's personal information afforded by informational privacy allows individuals to voluntarily shape the deeper relationships required to meet their psychological need for relatedness.

Finally, I argue that ensuring informational privacy has a positive influence on the competence dimension in SDT. Although its connection to competence might seem less obvious than to other psychological needs, the link is nonetheless significant. Informational privacy grants individuals a safe space to try different identities and evolve personally, free of judgement and pressure[7]. Allowing this general form of self-development can be seen as beneficial to an individual's feeling of efficiency and thus, the development of any form of competence in various contexts in the long term. For instance, imagine Alex seeks to become a great writer but unfortunately for her, she lives in Evertown and everything she writes is immediately accessible to everyone. That may make her feel uncomfortable to make mistakes and consequently, not allow her true self to develop, learn and feel competent in her abilities.

Notably, this example touches upon personal autonomy. It is important to note that while the three psychological needs are separately formulated, they can impact each other. For instance, if one has a high sense of psychological autonomy and enjoys warm relatedness and support, it is more likely that they will also feel competent in what they are doing. Therefore, by supporting psychological autonomy and enabling meaningful connections, informational privacy indirectly but substantially can boost competence, affirming its critical role in personal and professional development.

As I will show in section 3, these psychological needs take on new significance in the age of AI, where algorithms can process and analyse personal information at unprecedented scales and depths. AI systems do not just collect data – they can identify patterns, make predictions, and influence behaviour perhaps in ways that traditional digital systems cannot.

In summary, I introduced SDT as a framework to streamline and operationalise the psychological values of informational privacy. This does not indicate that every psychologically self-determined person will also enjoy informational privacy nor vice versa. However, it provides a more tractable psychological link to the value of informational privacy for human well-being. Building on this link, and working backwards, I will use SDT later in the next section as a guide to operationalise counter-measures that support human well-being, even when trade-offs against informational privacy are made.

[7] This point becomes especially relevant when considering the societal pressures faced by minorities, as illustrated by Allen (1988).

3. Navigating AI's Threats to Informational Privacy through an SDT Framework

So far I have drawn the following picture: informational privacy is a valuable pre-condition to a human's sense of personal autonomy as well as positive liberty. The SDT gives a reasonable framework to unpack these values and see why they are essential for an individual's self-determination and thus, psychological well-being. Now, I will draw my attention specifically to how AI presents unique challenges to this framework in ways that go beyond traditional digital privacy concerns.

3.1. AI's Unique Threat to Informational Privacy

Modern AI systems, particularly machine learning (ML) algorithms, rely on mass data to realise predictive tasks in ways fundamentally different from traditional data processing. By focusing on predictive targeting algorithms as an example of such AI-systems, I will now argue that this reliance on data, together with AI's unique capabilities and the scale at which they are implemented, make the notion of "control over the flow of information" increasingly impossible and thus poses unprecedented threats to autonomy as the introduced value of privacy.

First, the use of personal information in AI-driven behavioural targeting algorithms and profiling presents challenges that go beyond traditional targeted advertising.

These AI systems operate by not only aggregating vast amounts of personal data from various sources but by identifying complex patterns and making sophisticated predictions about individual behaviour. The concern here is that AI-powered categorisation can limit personal choice and autonomy in ways traditional systems cannot. By defining and narrowing the options available to individuals based on past behaviour and inferred preferences, AI-driven targeting can restrict one's ability to explore and define their identity independently. While this might seem to be a minor problem in the context of product advertising, the predictive power of AI makes it particularly concerning in political campaigns and recommendation algorithms. The case of Cambridge Analytica mentioned in section 1 demonstrates how AI-powered targeting can manipulate behaviour at unprecedented scales. Advocates of such methods may object that the AI-driven suggestions are rather in the interest of the user because they are more likely to be aligned with their interests and hence improve their overall experience. However, the underlying issue with this argument is the assumption that relevance as determined by AI algorithms equates to genuine interest of the user. While this may be true in some cases, it is unlikely to be true for all cases. In fact, one may suggest that influencing a user to buy a product through an AI-optimised targeting might be simpler than finding the perfect product in line with their interest. A helpful question to clarify this point is, how much do the targeter's interests truly align with those of the targeted person (Vold and Whittlestone, 2020).

Second, the current measures designed to ensure user control over their information flow are particularly inadequate when applied to AI systems. The concept of notice and consent has been the primary model employed. Its central idea is that as long as the user is notified about the AI profiling and targeting transparently and consents to the practice, informational privacy is protected. However, the scale of data needed to train and maintain ML models makes full transparency either impossible or impractical. This creates what I call an *AI transparency paradox* building on Nissenbaum's original concept of "transparency paradox" (Nissenbaum, 2011). This paradox highlights the dilemma between overly detailed policies about AI operations that are too complex for users to practically engage with and simplified summaries that omit essential information about AI processing, rendering informed consent ineffective. Critical details lost in simplification include the specifics of how AI systems process and share data, their learning and adaptation over time, and the roles of various AI systems across business associates, which are essential for any truly informed decision. Consequently, the problem is that uninformed consent is often falsely interpreted as individuals exercising control over their information.

Having established the challenges posed by predictive ML algorithms to the foundational value of privacy, it does not follow that they are

intrinsically unbeneficial nor that they cannot contribute to human flourishing. In fact, there are many applications that bring social and individual goods in spite of making control over the flow of information difficult.[8]

Therefore, the question becomes what is a reasonable approach to navigate various trade-offs to the individual's informational privacy? What makes AI systems unique in this context is that the scale of data processing makes the concrete control of the flow of personal information not just difficult, but effectively unmeasurable and intractable. However, crucially, while direct information control may become intractable, the psychological benefits of privacy should remain tractable and protectable.

3.2. Trading-off Informational Privacy through the Lens of SDT

In the following section, I will operate under the assumption that in order to benefit from predictive AI algorithms at least some trade-offs to informational privacy will be unavoidable. Thus, the question I aim to answer is how we can make sure that individuals still benefit from the trade-offs even if they may not be fully controlling the flow of their personal information. To be clear, I will not argue whether such trade-offs are morally justifiable, nor what particular implementations are morally permissible. I will rather focus on what measures are needed to ensure the protection of human well-being and flourishing when informational privacy trade-offs occur, particularly in AI contexts where direct information control becomes intractable.

Focussing on our SDT approach and the defined psychological needs, autonomy, relatedness, and competence, I will now show that they can be used as a guide to allow for prioritisation of user empowerment in design and the mitigation of privacy harms after they occur. By using the psychological needs as a guide we can set boundaries and adequate design mechanisms to help users retain a sense of autonomy, relatedness and competence. The existence of such measures is even more important, the less direct control users have over their information.

The central idea of our SDT-based approach is to mitigate the negative impacts of privacy loss by introducing supplementary measures within the same context. These measures are guided by the same virtues and values that underpin informational privacy. The three dimensions provided by SDT serve as a guide to operationalise these measures. For example, does a particular privacy trade-off restrict an individual's sense of relatedness? Then there must be further measures in place to counter the impact and strengthen the individual's feeling of relatedness.

Putting this together, I call the resulting model "Self-determined Privacy Loss in Informational Networks and Technologies" or in short SPLINT. The analogy of a splint, defined as a medical device used to support and protect an injury to facilitate healing, applies in the same way that our psychological model aims at ensuring conditions through which loss of informational privacy can be mitigated after it has occurred. Additionally, in the same way that a splint as a medical device does not explain the cause of an injury or is not a replacement for physical health, our SPLINT model does not aim to explain or justify informational privacy trade-offs nor be a replacement for informational privacy. It only focuses on making sure that the core principles in informational privacy that safeguard human well-being are preserved and respected even if trade-offs happen.

Furthermore, the SPLINT framework's value becomes particularly apparent in contexts where direct information flow control becomes intractable, as is often the case with large-scale AI systems. By focusing on preserving the psychological benefits of privacy rather than attempting to maintain direct control over information flow, SPLINT offers a practical approach to privacy protection in increasingly complex technological environments. This makes it especially valuable for AI applications while remaining relevant to other digital contexts where similar challenges arise.

An application of the introduced SPLINT model on two specific predictive algorithm use cases is depicted in Figure 2.

[8] See Jumper, J., Evans, R., Pritzel, A. *et al.* (2021) for predicting protein-folding or Courtiol, P., Maussion, C., Moarii, M. *et al.* (2019) for cancer patient survival prediction.

AI Application

Psychological Value of Informational Privacy

SDT Dimension	Personalised Advertising	Content Recommendation Systems
Autonomy	Provide individuals with a full overview of their data used along with analytics tools to edit and delete them. Allow for **adjusting preferences** for product categories, brands, and the frequency of ads.	Enable users to explore and discover content based on their unique interests and past interactions, while also offering the **flexibility** to explore new domains or unexpected content, encouraging a sense of **personal agency**.
Relatedness	Use advertising to promote products or services that **encourage community building**, social interaction, or connect users with groups and activities that match their interests.	Help users manage their time on the platform to maintain a **healthy balance** between digital and real-life interactions.
Competence	Facilitate **emotional learning** and share behavioural insights with users to facilitate education and **self-awareness** of online behaviour and vulnerabilities, reducing misuse risks and also increasing personal autonomy.	Provide resources that explain the system and its use, help individuals to **recognise their own content consumption patterns** to reduce exploitation risks.

Figure 2: *Application of the SPLINT Framework across different predictive AI domains.*

3.3. Evaluation and Limits

The introduced approach to mitigate the harms associated with informational privacy loss has some limitations that are important to address.

Firstly, one may justifiably object that the proposed framework appears too individualistic, overlooking the social dimensions of privacy trade-offs which are essential for understanding their impact. This consideration is indeed vital for justifying trade-offs against privacy. However, this is not the aim of the SPLINT framework. It does not and should not serve as a framework for justifying trade-offs. Instead, its purpose is to help the mitigation of individual harms in informational privacy trade-offs.

Moreover, it is important to note that the SPLINT model is not an alternative to the notice-consent model but a supplement. Being transparent about the challenges of achieving full transparency, along with implementing measures across various dimensions, ensures psychological benefits. For instance, SPLINT approaches consent not merely as a sufficient condition for respecting autonomy over one's data but promotes a more nuanced and holistic treatment of autonomy within the context of informational privacy than what the notice-consent model alone may offer. By implementing supplementary measures, such as encouraging individuals to understand their own behavioural patterns, habits, and vulnerabilities within the systems they engage with, it ensures that a loss of informational privacy does not translate into a long-term loss of autonomy. It is an imperative, a call for action to mediate the effects of trading off informational privacy. It emphasises that further commitments must be made by the entity that compromises an individual's informational privacy.

Conclusion

In conclusion, informational privacy, understood as the control over the flow of personal information, is worth protecting because it enhances human well-being and flourishing. It serves as an enabler of personal autonomy and positive liberty, facilitating the formation of voluntary, meaningful social relationships. To support this argument, I introduced the psychological model of Self-Determination Theory (SDT) and mapped the values of informational privacy to its three dimensions—autonomy, relatedness, and competence—operationalising how informational privacy translates into human well-being. I then argued that predictive AI algorithms, such as those used in personalised advertising, pose a threat to the values introduced, and that the current measures of notice and consent fail due to the scale of processes and the difficulty of achieving full transparency. To mitigate privacy harms to an individual's well-being in cases of privacy trade-offs, I employed an SDT-based approach to

introduce a supplementary framework: the SPLINT model.

As Cohen notes, "privacy has an image problem" (Cohen, 2013). It is often labelled as an imperative of not doing. Not accessing. Not using. Protecting but not progressing. However, focusing on its values shows us, it is rather an enabler to become. To self-develop. To be autonomous. To be self-determined and to flourish and enjoy psychological well-being. A clear operationalisation of these values in regard to technology design and additional supplementary measures may give us a clear way to protect it progressively.

My main aim in this paper was to provide a preliminary model of this sort by focussing on privacy's psychological values towards human flourishing. While limited in its societal applicability, the introduced SPLINT framework calls for proactive encouragement of operationalised privacy values.

While there has been an extensive amount of sophisticated approaches to apply SDT to technology design, my account focused particularly on addressing the close relationship between informational privacy's values and self-determination as a psychological virtue in AI-mediated environments.[9] Future research could shed more light on the exact benefits of informational privacy as a psychological phenomenon, useful methods to quantify the extent and the appropriateness of supplementary measures, and ways to include wider societal impacts on individuals' well-being in relation to privacy.

References

Allen, Anita L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield Publishers.

Berlin, Isaiah. (1969). *Four essays on liberty*. Oxford University Press.

Calvo, Rafael A., Dorian Peters, Karina Vold, and Richard M. Ryan. (2020). "Supporting Human Autonomy in AI Systems: A Framework for Ethical Enquiry." Edited by Christopher Burr and Luciano Floridi. Ethics of Digital Well-Being: A Multidisciplinary Approach. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-50585-1_2.

Cohen, Julie E. (2013). WHAT PRIVACY IS FOR. *Harvard Law Review*, *126*(7), 1904–33.

Courtiol, P., Maussion, C., Moarii, M. *et al.* (2019). Deep learning-based classification of mesothelioma improves prediction of patient outcome, Nat Med *25*, 1519–1525.

Fried, Charles. (1968). Privacy. *The Yale Law Journal*, *77*(3), 475–93.

Jumper, J., Evans, R., Pritzel, A. *et al.* (2021). Highly accurate protein structure prediction with AlphaFold. *Nature*, *596*, 583–589.

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Tomislav Chokrevski, and Maša Gali. (2017). A Typology of Privacy, 38.

Moore, Adam. (2008). Defining Privacy. *Journal of Social Philosophy*, *39* (3), 411–28.

Moore, Adam D. (2003). Privacy: Its meaning and value. *American Philosophical Quarterly*, *40*(3), 215–27.

Nissenbaum, Helen. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 119.

Nissenbaum, Helen. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Peters, Dorian, Rafael A. Calvo, and Richard M. Ryan. (2018). Designing for Motivation, Engagement and Wellbeing in Digital Experience. *Frontiers in Psychology*, 9.

Roessler, Beate. (2005). *The Value of Privacy*. Polity Press.

Ryan, W. S., & Ryan, R. M. (2019). Toward a social psychology of authenticity. *Review of General Psychology*, *23*(1), 99-112.

[9] See for example Shevlin 2024; Calvo *et al.* 2020 and Peters, Calvo, and Ryan 2018.

Ryan, Richard M., and Edward L. Deci. (2017). *Self-Determination theory: Basic psychological needs in motivation, development, and wellness.* Guilford Press.

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. (2019). Online manipulation: Hidden influences in a digital world." *Georgetown Law Technology Review*, *4*, 1–45.

Thomson, Judith Jarvis. (1975). The Right to Privacy. *Philosophy and Public Affairs*, *4*(4), 295–314.

Véliz, Carissa, ed. (2024). *The Ethics of Privacy and Surveillance*, Oxford University Press.