Towards an Approach for Designing Responsible Privacy Heuristics

Beatriz Pontes da Costa Reis[1], Mohamad Gharib[1]

[1]*University of Tartu, Tartu, Estonia*

Abstract

Privacy compliance is a major business and societal requirement, deeply embedded in organizational business processes, for legal entities handling Personal Information (PI). Regulations mandate these entities to implement privacy protection mechanisms (privacy solutions) within their business workflows and inform data subjects (DSs) about PI processing. However, DSs often struggle to understand relevant information and effectively use these mechanisms, leaving their privacy vulnerable. This disconnect underscores the social and human aspects, where organizational processes intersect with the cognitive and behavioral capacities of DSs. Consequently, ensuring compliance is not solely a technical or procedural task—it requires designing processes that support human understanding, decision-making, and trust. Privacy heuristics offer a potential solution by assisting users in making informed decisions. Yet, their design is complex, prone to bias, and, if done irresponsibly, may lead to unethical or manipulative outcomes. This paper addresses these challenges by developing an approach that offers design principles to guide the design and evaluation of Responsible Privacy Heuristics (RPHs) for usable privacy-aware systems or solutions. These principles aim to guide the creation of privacy-aware systems that empower users, respect autonomy, and enhance informed decision-making. By embedding these principles, organizations can better align privacy mechanisms with human needs. We demonstrate the applicability of our approach through a practical example.

Keywords

Usable privacy, Responsible privacy heuristic, Privacy Engineering, Privacy-aware systems

1. Introduction

In 2009, European Commissioner for Consumer Protection Meglena Kuneva stated that *"Personal data is the new oil of the Internet and the new currency of the digital world"* [1]. Spiekermann et al. [2] highlight the growing challenges of personal data (PD) (also called Personal Information (PI)) markets and privacy, emphasizing how PD has evolved into a valuable asset for both companies and consumers [3]. They also discuss its role in powering various services, including personalized advertising, recommendation systems, consumer risk analysis, and even as a product itself—particularly in user-generated content on social networks.

As personal data increasingly becomes a product and service, integrating privacy into digital system development has become essential [4]. Regulations such as the General Data Protection Regulation (GDPR) in the EU [5], Brazil's General Personal Data Protection Law (LGPD) [6], and Japan's Act on the Protection of Personal Information (APPI) [7], among others, impose

RCIS 2025 Workshops and Research Projects Track. 20 - 23 May, 2025. Seville, Spain

*Corresponding author.

beatriz.pontes.da.costa.reis@ut.ee (B. P. d. C. Reis); mohamad.gharib@ut.ee (M. Gharib)

0000-0003-2286-2819 (M. Gharib)

legal obligations to safeguard data subjects (DS) and their privacy. These laws aim to protect DS and prevent the mismanagement of their PI—including misuse, excessive processing, improper storage, and unauthorized third-party sharing [8].

Although legal entities handling PI are required to provide DSs with privacy protection mechanisms and disclose how their PI will be processed, the responsibility of understanding this information and effectively using these mechanisms still falls on DSs [9]. This poses a challenge, as users have varying levels of digital literacy and may struggle with the legal jargon found in privacy policies or cues.

This challenge reflects a broader issue concerning the need to consider social and human aspects when designing and managing processes involving PI. Business processes, traditionally, focus on efficiency and compliance, but when it comes to privacy, they must also account for the psychological and behavioral dimensions of user interaction. Users are not merely endpoints in a process; they are active participants with diverse expectations, preferences, and vulnerabilities. Failing to address these aspects can lead to disengagement, mistrust, or even harm.

A promising solution is the use of heuristics, more specifically, privacy heuristics that can help users make informed decisions and take appropriate actions [10]. However, designing privacy heuristics is complex and prone to bias [11]. More critically, if not designed responsibly, they may influence the DS judgments or decisions in a manner that is considered unethical, immoral, or socially irresponsible.

This paper aims to address and mitigate this burden by developing an approach that offers design principles to guide the design and evaluation of Responsible Privacy Heuristics (RPHs) for privacy-aware solutions. These principles aim to empower users, uphold their autonomy and self-determination, and facilitate informed decision-making.

The remainder of this paper is structured as follows: Section 2 outlines the research baseline, while Section 3 explores both unethical and ethical design patterns. Section 4 introduces our approach, detailing the methodology used in its development. Section 5 demonstrates its applicability, and Section 6 concludes the paper with a discussion on future work.

2. Baseline: Heuristics & Privacy Heuristics

Heuristics, often described as “rules of thumb” or “mental shortcuts”, aid faster decision-making [12, 11]. While broadly defined, they are commonly seen as problem-solving methods that do not guarantee optimal solutions [11]. They help with both ill-defined and well-defined problems by reducing cognitive effort [10]. Heuristics can be instinctive (automatic) or deliberate, with experience transforming one into the other over time [11].

Heuristics play a key role in online privacy, especially in PI disclosure, where they are termed Privacy Heuristics (PHs). Sundar et al. [13] classify PHs into three decision-making contexts: Personal (self-protection or self-reward in disclosure), Social (influence of group dynamics), and Technological (interface elements shaping behavior). Vincent et al. [14] propose six super-ordinate PH classes: Prominence (credibility and trust), Network (social influence), Reliability (trust in design and consistency), Accordance (alignment with beliefs), Narrative (impact of storytelling), and Modality (influence of new technologies).

In short, privacy heuristics simplify privacy decisions by enabling quick, efficient choices

while ignoring some information. They can be deliberate or automatic, influenced by the environment, experience, and cognitive biases. Table 1 compiles key heuristics from [13, 14, 15], which can influence privacy decisions.

Table 1
Heuristics that can influence privacy decisions

Affect Heuristic. People judge objects or events by associating them with positive or negative feelings.
Anchoring. Under uncertainty, people tend to be biased towards a reference point, or "anchor".
Choice Overload. Too many options make people feel overwhelmed and influence their judgment negatively.
Contrast effect. People's decision is influenced by comparing one instance with another, instead of relying on impartial standards.
Framing. People's choice frame is set up in a way to manipulate/control the user's decision.
Functional Fixedness. People tend to fixate on a specific use of an object
Instant gratification. People prioritize quick rewards at the expense of future gains.
Loss Aversion. People prefer avoiding losses rather than acquiring equivalent gains.
Optimism bias. People tend to underestimate the chances of experiencing negative events and overestimate positive ones.
Social Norms. People's behavior is influenced by social norms, that either play a part in guiding or constraining it.
Status Quo/Default Effect. People tend to favor options that maintain the current state over those that introduce change.
Authority. Recognized brand, institution or person that vouches for the security, influences disclosure.
Bandwagon. People are influenced by the decision of many or the majority to disclose information.
Reciprocity. People are more likely to share information with someone who has disclosed theirs to them.

3. Unethical & ethical design patterns

In this section, we explore unethical patterns followed by ethical, fair, and responsible ones as decision support mechanisms within the context of privacy.

Unethical patterns. Unethical or descriptive patterns, commonly referred to as "dark patterns", were first described by Brignull in 2010 [16] as '*'tricks used in websites and apps that make you do things you didn't intend to, such as buying or signing up for something*". These patterns are often coercive, manipulative, and exploitative, aiming to guide the user into decisions that primarily benefit the service provider, often at the expense of the user's best interest [17]. Deceptive patterns exploit user biases and heuristics to trigger automatic, fast, and intuitive decision-making. They frequently alter the choice architecture by hiding or obstructing privacy-preserving options, instead promoting those that encourage greater PI disclosure [18]. This manipulation prevents users from making informed, conscious choices, potentially leading to harmful decisions regarding their personal data.

Kitkowska [15] has identified unethical patterns in the existing literature, and organized them into taxonomies. Based on her work, Table 2 presents examples of privacy-deceptive patterns

(PDPs), the psychological effects (heuristics and biases) they may trigger, and their potential impact on user decisions. Please note that due to space limitations, the table is not meant to provide an exhaustive list of PDPs but to illustrate the concept and lay the groundwork for an ethical approach.

Table 2: Privacy Deceptive Patterns, triggered heuristics and effects on user based on [15]

PDP	Heuristic(s)	Effect on user
Privacy Zuckering: is the use of deceptive design or persuasive tactics to manipulate users into sharing more PI than they intend to.	Choice overload, Status quo, and Framing.	Users share more PI than they intended and might be unaware of how their PI is being processed.
Bad defaults: user account options are often preconfigured in a privacy-invasive manner (over-sharing) and sometimes with no alternative options available.	Default effect, Status quo, and Loss aversion	Same as Privacy Zuckering.
Comparison obfuscation: hinders users from easily comparing privacy policies, data collection practices, or security features across different services.	Anchoring and Optimism bias.	Users adopting privacy-invasive options.
Forced action: Users are forced to make choices immediately to use a service.	Instant gratification, Framing.	Users end up sharing more PI than they intended to keep using a service.
False necessity: Persuades users into privacy-invasive choices by claiming the data is essential for the service.	Framing, and Status quo.	Same as Forced action effects.
Just between you and us: Makes false promises of confidentiality to encourage users to disclose more information.	Optimism bias and Framing.	Users might share more than they usually would due to the false sense of confidentiality.
Trick questions: Deceive users into making privacy-invading choices with misleading or ambiguous wording.	Default effect, framing and anchoring.	Users will be confused and most likely misinterpret their choices.
Attention diversion: Distracts users from privacy-conscious choices by other aspects of the interface.	Anchoring and Framing	Hinders users from properly reflecting on their privacy-related choices.
Wrong signal: Uses distinguishable icons, symbols, or other elements in the UI to misguide users.	Anchoring, Framing, Affect	Certain UI elements create the illusion of privacy-conscious choices, misleading users into feeling secure.

PDP	Heuristic(s)	Effect on user
Confirmshaming: Steer users to make specific choices through guilt/shame. May use UI elements to induce a certain emotional state.	Affect, contrast and default effects, Framing	Users are manipulated to share more data through guilt or social pressure.
Last-minute consent: leverages time pressure and context to push users to consent to less optimal privacy options choices or make privacy decisions without the option to delay.	Loss aversion and Status quo	Users experience a reduced freedom of choice and might be coerced to comply with privacy-invasive choices to avoid losing progress.
Safety blackmail: Users are pressured into less optimal privacy options by implying that failing to do so could result in safety or security risks.	Functional fixedness and instant gratification.	Users end up sharing more PI than they intended to enable their accounts.

While deceptive patterns have been extensively researched and existing work offers valuable insights into what should be avoided, there is a notable gap in research focusing on what should be done [17]. This paper addresses that gap by proposing a systematic approach for developing RPHs (i.e., ethical decision-support mechanisms) within the privacy context.

Ethical patterns. Ethical, fair, or responsible patterns are decision support mechanisms designed to prioritize the user's interests, enabling them to make informed and unobstructed decisions [18], in contrast to dark patterns, which manipulate users. These patterns aim to

Table 3
A taxonomy of dark patterns with corresponding fair patterns that can influence privacy decisions

Dark pattern	Fair pattern
Harmful Default: default settings are against the user's interest.	**Protective Default:** defaults prioritize user privacy and well-being, aligning with positive societal outcomes.
Missing Information: Selective disclosure of information.	**Adequate Information:** Users receive clear, sufficient, and relevant information without unnecessary overload.
Maze: User path to information, preferences, or choices are made unnecessarily complex.	**Seamless Path:** User path to information, preferences or choices are as easy when they are in the user's interest than when they are in the service provider's interest.
Push & Pressure: Emotional, or time-based triggers pressure user decisions.	**Pressure:** No manipulative nudges unless they serve user or societal benefits.
Misleading or Obstructing Language: Language is confusing, manipulative, or impedes user understanding.	**Plain and Empowering Language:** Clear, accessible, and jargon-free wording helps users make informed decisions.
More than intended: Users are led through a series of steps that force them to do or give more than they originally intended.	**Free action:** Users are empowered to understand the consequences of their choices—especially regarding spending or data sharing—without unnecessary information overload.
Distorted UX: The UI is designed to mislead or trap users.	**Fair UX:** The UI ensures the clarity, shape, size, and prominence of buttons and icons.

empower users by presenting their choices transparently and clearly, facilitating well-informed decisions. To achieve this, ethical patterns must be succinct, transparent, accessible, and easy to understand. They serve as ethical counterparts to deceptive patterns. In this regard, Potel-Saville and Rocha [18] developed a taxonomy (presented in Table 3) that pairs dark patterns (DPs) with their corresponding fair patterns (FPs). The authors also note that some of these patterns align with specific GDPR Articles, providing designers with a framework that ensures both ethical design and regulatory compliance.

4. An Approach for Designing Responsible Privacy Heuristics

The research methodology has been developed following the Design Science Research (DSR) approach [19]. Specifically, our methodology aligns with DSR's key steps while further refining some into sub-steps, as illustrated in Figure 1, and described as follows:

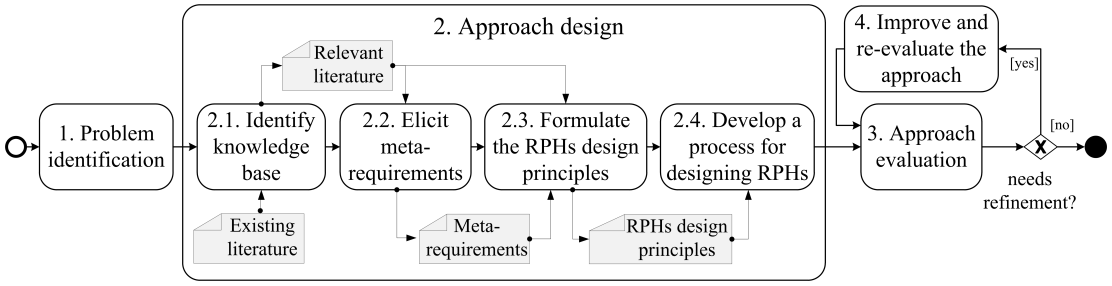


Figure 1: The process for constructing and evaluating the approach

1. **Problem identification:** as discussed earlier, there is a need for an approach to guide the design and evaluation of RPH for privacy-aware solutions.

2. **Approach design:** is composed of four sub-steps; *2.1. Identity knowledge base*, *2.2. Elicit Meta-requirements*, *2.3. Formulate the RPHs design principles*, and *2.4. Develop a methodological process for designing RPHs.* The first three sub-steps have been adopted following the method for developing design principles in [20], and the last step offers a systematic process for using the approach. We describe these steps in the following section.

3. **Approach evaluation:** aims at evaluating the approach based on how well it supports solutions in the problem space. In particular, we will demonstrate its applicability (e.g., usability and validity) for the design and evaluation of RPH for privacy-aware solutions and its effectiveness in identifying wrong/bad design practices in privacy heuristics.

4. **Improve and re-evaluate the approach:** this step mainly focuses on identifying limitations or areas of improvement and refining the approach accordingly.

In this paper, we cover the approach design and illustrate its applicability, leaving its evaluation for future work.

4.1. Approach design

4.1.1. Identity knowledge base.

The approach aims to guide the design and evaluation of RPH for privacy-aware solutions. At its core, the design principles that guide this process. Design principles are clear statements that are prescriptive in nature, with different levels of abstraction depending on the context [21]. According to Möller et al. [20], they are "fundamental propositions that aid designers in achieving successful transfer of requirements to design", and they should also encapsulate and communicate knowledge that can be reused in similar instances that are subject to similar conditions [20]. Having this in mind, we identified the literature related to ethical and unethical design patterns and principles that apply to privacy heuristics at this step. This enabled us to identify the most relevant design patterns related to this research, which has been presented earlier in the paper.

4.1.2. Elicit Meta-requirements.

Based on related literature, we define RPHs as user-empowering, transparent, accessible, and easy-to-understand decision support mechanisms that respect user autonomy and self-determination and enable informed privacy decisions. Additionally, they should be based on ethical principles such as: Respect, Beneficence (and Non-maleficence [22]), Justice, Integrity, and Social Responsibility [23]. Based on this definition and the ethical principles identified in [23], we elicited five Meta-Requirements (MR), which are listed in Table 4.

Table 4
Meta-requirements for RPHs

Meta Requirement (MR)	Source
MR1. Integrity: Information presented through RPHs must be accurate, truthful, consistent, and free from incomplete representations.	[23]
MR2. Non-manipulation: A RPH must not exploit cognitive biases or limitations to steer users toward privacy-invasive decisions.	[24]
MR3. Beneficence and non-maleficence: A RPH should maximize user benefits while minimizing privacy risks and potential harms, ensuring ethical and responsible guidance.	[23, 22]
MR4. Autonomy and control: A RPH should empower user's autonomy and freedom of choice by offering genuine, meaningful, and informed options without implicit coercion.	[22, 24]
MR5. Context-aware and accessible: A RPH should, when possible, adapt to different contexts by considering risk levels, situational factors, and user diversity	[13]
MR6. Regulatory compliant: A RPH should align with legal standards (e.g., GDPR).	[5]

4.1.3. Formulate the RPHs design principles

The formulation of RPH design principles was grounded in the relevant literature identified in the *Identify knowledge base* step. Specifically, we examined existing deceptive patterns and

related heuristics (see Table 2) and reviewed research on deceptive strategies (e.g., [16, 25, 26, 24]) to better understand how user behaviors are manipulated or exploited concerning their privacy choices. We paid particular attention to Ahuja and Kumar work [24], which identifies 25 dark strategies and seven broad ethical concerns—compulsion, inadequate information, biased evaluation, insufficient deliberation, lack of control, pressure to conform, and restricted options—arising from these deceptive patterns. Their study further anchors these concerns in four theoretical conceptualizations of autonomy: agency, freedom of choice, control, and independence. Building on these insights, we formulated the design principles aimed at mitigating deceptive and unethical strategies while ensuring compliance with the established meta-requirements. The resulting principles are presented in Table 5.

Table 5
Design principles for Responsible Privacy Heuristics

DP1.	**Neutral:** A RPH should present information about privacy choices in a neutral, balanced, and clear manner, avoiding framing that could lead to biased or skewed decisions.
DP2.	**Honesty and clarity:** A RPH should ensure that all information presented to users is truthful, clear, and easy to understand.
DP3.	**Navigable and actionable information:** A RPH should help users easily identify, understand, and act upon privacy-related information.
DP4.	**Unpacking complexity:** A RPH should empower users to reflect and comprehend privacy information that can affect their data disclosure.
DP5.	**Pressure-free:** A RPH should not impose time constraints, emotional manipulation, or other coercive tactics that pressure users into making privacy decisions. Instead, it should allow users to deliberate freely, ensuring informed and voluntary choices.
DP6.	**Benefit-Risk Balance:** A RPH should prioritize user benefits while proactively minimizing potential privacy risks.
DP7.	**Consequences awareness:** A RPH should not obscure the consequences of a privacy choice.
DP8.	**Empowering:** A RPH should support users to select privacy choices that align with their privacy requirements.
DP9.	**Context-aware:** A RPH should help users assess privacy decisions in context, considering factors such as data sensitivity, purpose of collection and use, recipient trustworthiness, and potential risks.
DP10.	**Situation-aware** A RPH should adapt to different situations to provide relevant, meaningful, and actionable guidance.
DP11.	**Accessible and inclusive:** A RPH should ensure that users—regardless of their abilities, or technical expertise—can understand and act upon privacy-related information.
DP12.	**Regulatory compliant:** A RPH must not encourage or lead to violating privacy legislation (e.g., purpose limitation, data minimization).

4.1.4. Develop a methodological process for designing RPHs

In this section, we outline the methodology to be followed for designing RPHs. The process, illustrated in Fig. 2, consists of three key steps:

1. **Identify core privacy heuristics for usability:** Takes the privacy solution (system) as input and derives Privacy Heuristics (PH) that enhance its usability. Gharib [10] formu-

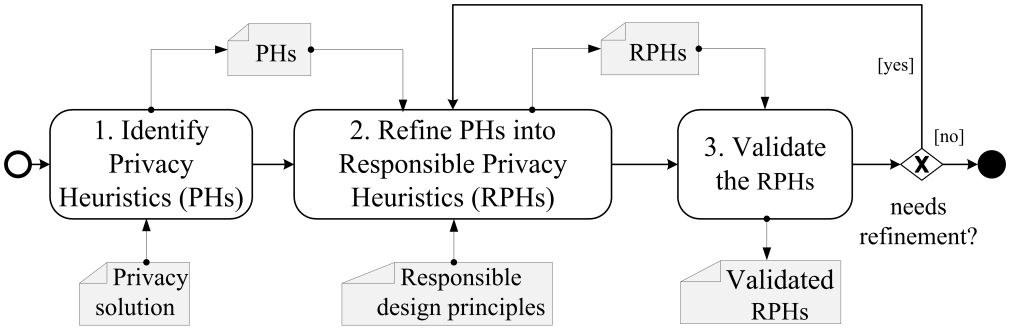


Figure 2: The methodological process to be followed during the overall RPHs design

lated ten Usable Privacy Heuristics (UPHs) that can be applied at this stage to guide the design process. The goal is to ensure that privacy-related interactions are intuitive, clear, and user-friendly, making it easier for users to understand and manage their privacy settings effectively.

2. **Refine PHs into RPHs:** Takes the identified PHs and the responsible design principles as input. The PHs are then refined using these principles to develop RPHs.

3. **Validate the RPHs:** Evaluates whether the RPHs achieve the purpose of their development, which can be conducted through one or a combination of commonly used methods, such as end-user testing, expert reviews, or other assessment techniques.

5. Illustrating the Applicability of the Approach

We demonstrate the applicability of the approach with an example from the online social network (OSN) domain. Privacy settings are arguably the primary mechanism through which a DS can exercise control over their PI in OSN, as such settings can be used to manage how their PI is shared and processed. To better understand the types of actions and information that OSN privacy settings typically provide, we reviewed the settings of a few widely used platforms, including Facebook and Instagram (via Meta's Privacy Center), LinkedIn, and Reddit. Given that these platforms serve varying purposes and user contexts, we synthesized their settings into five broad key categories. We then derived related core functionalities and organized them in Table 6.

Due to space limitations, we focus only on *Profile Visibility* - that is managed via a profile visibility interface - as our *solution* of concern (**Step 1**). The profile visibility interface (see Figure 3) allows the DS to manage the visibility of various profile elements, including personal details, activity such as posts, comments, and reactions on others' posts, and content which the DS has been tagged.

To enhance the usability, several UPHs can be applied such as a minimalist and consistent layout that offer the DS with relevant information related to their privacy actions following **UPH6. Minimalist design:** the system should offer DSs relevant information relating to their

Table 6
Key privacy settings and related functionalities

Key setting	Related settings functionality
Account & Security: controls over account details and account deletion	- Change password; - Enable/disable two-factor authentication; - Account deletion or temporary deactivation; - Manage devices and active sessions;
Profile Visibility: controls how DS profile and activity are presented to others	- Profile visibility control (i.e., who can see user's profile, and what profile details); - Activity visibility control (i.e., who can see user's posts, interactions, status and other related activities);
Interaction Preferences: controls how others can interact with DS's profile and activity	- Profile interaction control (i.e., who can tag the DS or comment on their posts, and who can message them); - Activity interaction control (i.e., who can interact with users' posts); - Blocking other profiles;
Ad preferences: ads customization and experience management	- Inform on who uses and what data they use on advertisement customization; - Ad customization information management (i.e., manage what information the advertiser can access and process for ads experience enhancement;
Permissions and Policies: control over data access and processing, and privacy policies	- Permissions controls (OSN and third parties) - Inform on which services has access and uses DS data, what data and how they process this data; - Enable DS to export their data; - Enable user access to privacy and cookie policy;

privacy actions. At the top of the interface (see Figure 3), the DS is met with a brief description of what these settings enable. They are also informed that tapping on the setting will lead them to more information about it, inspired by **UPH1. Visibility:** the system should keep DSs informed about their privacy choices. This approach guides the DS while allowing them to make changes freely, as instructed by **UPH4. Expressiveness:** the system should guide DSs on privacy while still giving them freedom of expression. Moving down, the privacy choices were organized into sections with relevant naming and phrased in a simple and precise manner (avoiding technical terms). This decision was made so the DS can easily understand what each setting can do, and caters to DSs with different levels of digital literacy as instructed by **UPH9. User suitability:** the system should provide options for DSs with diverse levels of skill and experience in security.

Moving to **Step 2** of the process, we refine the identified UPHs into RPH. In particular, we analyze the identified UPHs one-by-one and apply the design principles we see fit. In what follows, we first present the original UPH, then highlight its refinement with underlining as each principle is applied.

UPH1 – *Visibility – "A DS should be informed about their privacy choices."*

RPH1.1 - *DP10. Situation-aware - "A DS should be provided with meaningful and actionable guidance when informed about their privacy choices, allowing them to adapt to different situations.."*

RPH1.2 - *DP9. Context-aware - "A DS should be provided with meaningful contextually relevant*

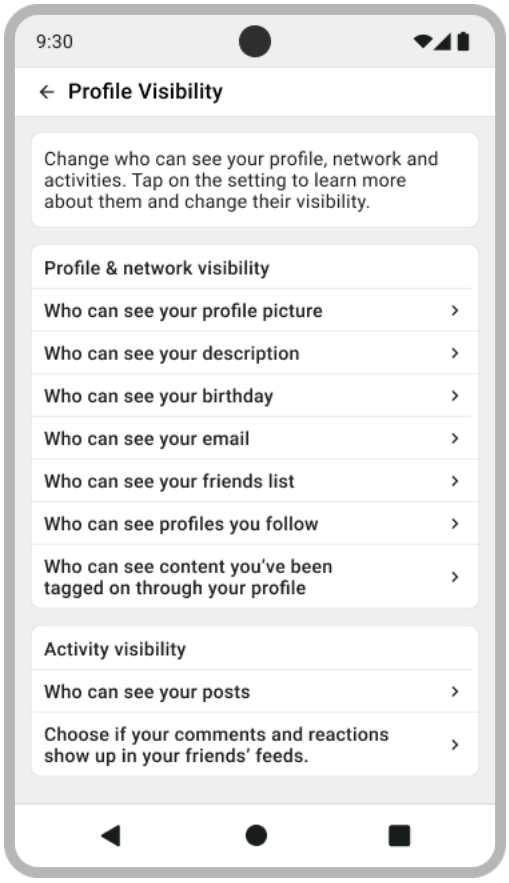


Figure 3: Profile visibility settings following UPHs.

and actionable guidance when informed about their privacy choices, allowing them to adapt to different situations and recognize potential privacy risks."

UPH4 – *Expressiveness – " A DS should be guided on privacy while still being able to have freedom of expression."*

RPH4.1 - *DP8. Empowering - "A DS should be supported with intuitive privacy mechanisms while still being able to have freedom of expression , enabling decisions that align with their beliefs."*

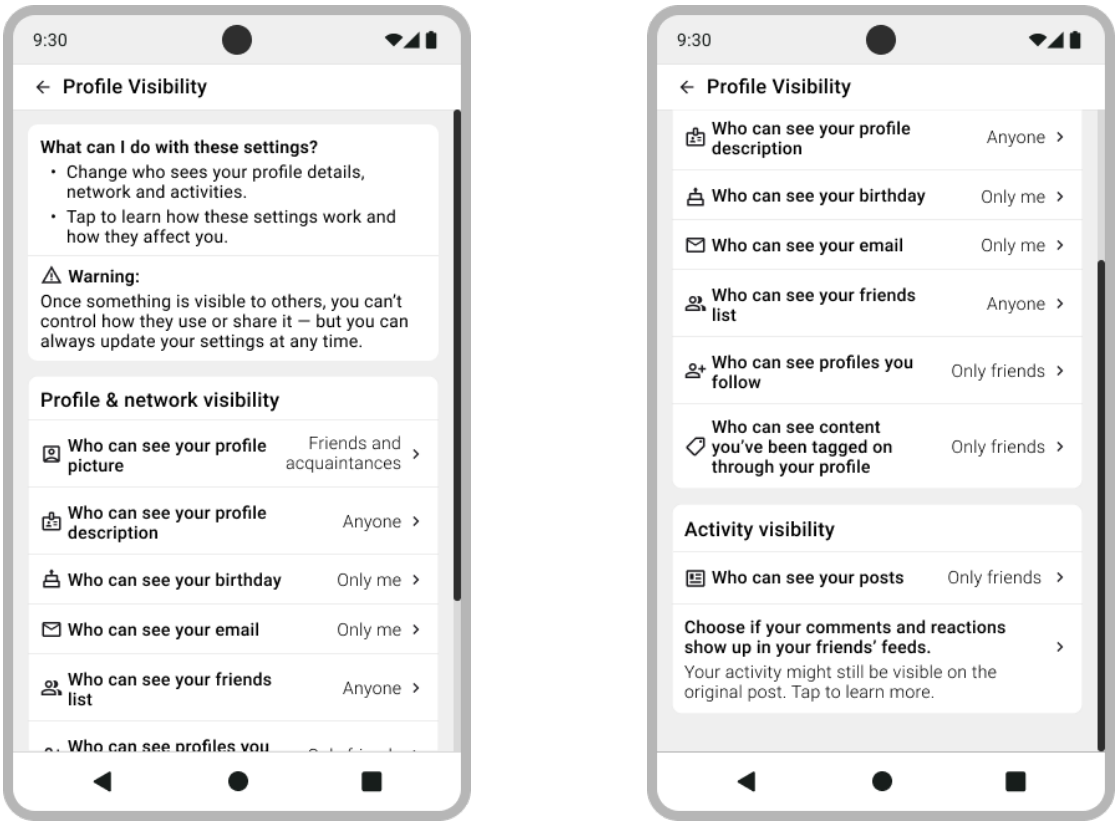
UPH5 – *Minimalist design – "A DS should be offered relevant information relating to their privacy actions."*

RPH5.1 – *DP3. Navigable and actionable privacy – "A DS should be offered relevant, easy to learn information relating to their privacy actions , making sure it is easily recognizable and usable."*

UPH9 – *User suitability – "DSs should be provided with options considering their diverse levels of skill and experience in security."*

RPH9.1 - *DP11. Accessible and inclusive - "DSs should be provided with inclusive options considering their diverse levels of skill and accessibility needs."*

Now that the UPHs have been refined into RPHs, we revisit the initial profile visibility interface accordingly. We follow the same structure as before, beginning with the *Profile Visibility* settings (Figure 4). In which the original setting description has been slightly rephrased into a question, followed by two concise bullet points and a warning. This format is intended to help the DS easily identify the privacy actions they can take (*RPH5.1*), make them aware of potential risks related to the visibility of their information, and make sure they know that they can change them whenever they want (*RPH1.1, RPH1.2, RPH4.1). This enables the DS to quickly understand their existing choices at a glance, without needing to click into each setting individually (RPH1.1, RHP9.1*).



(a) (b)

Figure 4: Profile visibility controls following RPH (a) part 1 and (b) Part 2

Finally, **Step 3** validates the effectiveness of the produced RPHs. The most effective approach for our example combines expert evaluation and A/B testing with potential end-users. First, experts assess the RPHs. Then, two versions of the privacy settings interface are tested: a baseline version using PHs and an improved version using RPHs. Participants are assigned to one interface, and their interactions and decisions are compared to evaluate the impact of RPHs.

6. Conclusions and Future Work

We aimed to tackle the problem of designing Responsible Privacy Heuristics (RPHs) by proposing an approach that offers design principles to guide the design and evaluation of RPHs for usable privacy-aware solutions. Recognizing privacy compliance as a human-centered challenge, our approach aims to empower users, enhance informed decision-making, and foster trust. We detailed the methodology used for the approach development and illustrated its applicability with an example.

For future work, we will assess the completeness of the proposed principles, define acceptance criteria for their application, and validate the approach through expert evaluations. We also plan to apply it in real-world case studies to refine and strengthen its practical relevance.

Acknowledgment

This work was supported by the Estonian Research Council grant "Developing human-centric digital solutions" (TEM-TA120), and was performed within the framework of COST Action CA22104 (Behavioral Next Generation in Wireless Networks for Cyber Security), supported by COST (European Cooperation in Science and Technology; www.cost.eu).

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Meglena Kuneva. Roundtable on online data collection, targeting and profiling, 2009.

[2] Sarah Spiekermann, Alessandro Acquisti, Rainer Böhme, and Kai Lung Hui. The challenges of personal data markets and privacy. *Electronic Markets*, 25(2):161–167, jun 2015.

[3] Mohamad Gharib. Privacy and Informational Self-determination Through Informed Consent: The Way Forward. In *Lecture Notes in Computer Science*, volume 13106 LNCS, pages 171–184. Springer Science and Business Media Deutschland GmbH, 2022.

[4] Argyri Pattakou, Aikaterini Georgia Mavroeidi, Christos Kalloniatis, Vasiliki Diamantopoulou, and Stefanos Gritzalis. Towards the design of usable privacy by design methodologies. In *Proceedings International Workshop on Evolving Security and Privacy Requirements Engineering, ESPRE*, pages 1–8, 2018.

[5] European Parliament. 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 Da. *Official Journal of the European Communities*, 59:1–88, 2016.

[6] Nadine D'Oliveira and Francisco José Aragão Pedroza Cunha. Brazilian General Data Protection Law (LGPD): the relationship between information policy and information regime. *Revista Digital de Biblioteconomia e Ciencia da Informacao*, 22, 2024.

[7] Hitomi Iwase. Overview of the act on the protection of personal information. *European Data Protection Law Review*, 5(1):92–98, 2019.

[8] Mohamad Gharib, Paolo Giorgini, and John Mylopoulos. COPri v.2 — A core ontology for privacy requirements. *Data and Knowledge Engineering*, 133:101888, may 2021.

[9] Danielle Jacobs and Troy McDaniel. A Survey of User Experience in Usable Security and Privacy Research. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 13333 LNCS, pages 154–172. Springer Science and Business Media Deutschland GmbH, 2022.

[10] Mohamad Gharib. Towards a Heuristic Model for Usable Privacy. In *Joint Proceedings of RCIS (Research Challenges in Information Science) Workshops and Research Projects Track*, pages 1–10. CEUR-WS.org, 2024.

[11] Mohamad Hjeij and Arnis Vilks. A brief history of heuristics: how did research on heuristics evolve? *Humanities and Social Sciences Communications*, 10(1), 2023.

[12] Ralph Hertwig and Thorsten Pachur. Heuristics, History of. In *International Encyclopedia of the Social and Behavioral Sciences: Second Edition*, pages 829–835, 2015.

[13] S. Shyam Sundar, Jinyoung Kim, Mary Beth Rosson, and Maria D. Molina. Online Privacy Heuristics that Predict Information Disclosure. In *Conference on Human Factors in Computing Systems - Proceedings*, pages 1–12. Association for Computing Machinery, apr 2020.

[14] Vincent Marmion, Felicity Bishop, David E. Millard, and Sarah V. Stevenage. The cognitive heuristics behind disclosure, decisions. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 10539 LNCS, pages 591–607. Springer Verlag, 2017.

[15] Agnieszka Kitkowska. The Hows and Whys of Dark Patterns: Categorizations and Privacy. *Human Factors in Privacy Research*, pages 173–198, 2023.

[16] Arunesh Mathur and Jonathan Mayer. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In *Conference on Human Factors in Computing Systems - Proceedings*, pages 1–18. Association for Computing Machinery, may 2021.

[17] Evan Caragay, Katherine Xiong, Jonathan Zong, and Daniel Jackson. Beyond Dark Paterns: A Concept-Based Framework for Ethical Sofware Design. In *Conference on Human Factors in Computing Systems - Proceedings*, page 16. ACM, may 2024.

[18] Marie Potel-Saville and Mathilde Da Rocha. From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 13888 LNCS, pages 145–165. Springer Science and Business Media Deutschland GmbH, 2024.

[19] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Quarterly: Management Information Systems*, 28(1):75–105, 2004.

[20] Frederik Möller, Tobias Moritz Guggenberger, and Boris Otto. Towards a Method for Design Principle Development in Information Systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 12388 LNCS, pages 208–220. Springer Science and Business Media Deutschland GmbH, 2020.

[21] Stefan Cronholm and Hannes Göbel. Guidelines supporting the formulation of design principles. In *ACIS 2018 - 29th Australasian Conference on Information Systems*, volume 1, 2018.

[22] Lorraine Kisselburgh and Jonathan Beever. The ethics of privacy in research and design: Principles, practices, and potential. In *Modern Socio-Technical Perspectives on Privacy*, pages 395–426, 2022.

[23] Karen Renaud and Lynsay A. Shepherd. How to make privacy policies both GDPR-compliant and usable. In *International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA*, pages 1–8, 2018.

[24] Sanju Ahuja and Jyoti Kumar. Conceptualizations of user autonomy within the normative evaluation of dark patterns. *Ethics and Information Technology*, 24(4):52, dec 2022.

[25] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4):237–254, 2016.

[26] Johanna Gunawan, Cristiana Santos, and Irene Kamara. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. In *Proceedings of the 2022 Symposium on Computer Science and Law*, pages 181–194. Association for Computing Machinery, Inc, nov 2022.