Towards a Heuristic Model for Usable Privacy

Mohamad Gharib[1]

[1]University of Tartu, Tartu, Estonia

Abstract

In response to the excessive collection and misuse of Personal Information (PI), many privacy regulations that govern such collection and use have been enacted. Consequently, privacy compliance has become a main concern for any legal entity dealing with PI since failing to comply with these regulations results in huge fines. Nevertheless, these regulations required the aforementioned entities to provide privacy protection mechanisms (called privacy solutions) and inform data subjects (DSs) how their PI will be processed, leaving the burden of understanding relevant information and the use of protection mechanisms on the side of DSs. However, most DSs fail to properly use these mechanisms, and in turn, safeguard their PI. This problem could be solved if the solution is designed with respect to the DS's capability for making informed decisions. However, it is not always easy to design a system that fits the needs of DSs with different experiences. A potential solution is the use of privacy heuristics to assist DSs to make informed privacy decisions and act accordingly. This paper aims to tackle this issue by proposing a privacy heuristics model and a corresponding method, which can be used to design usable privacy solutions. We demonstrate the applicability and utility of the model and method with an illustrative example.

Keywords

Usable privacy, Privacy heuristic, Heuristic model, Privacy Engineering, Privacy-aware systems

1. Introduction

Information can be described as the new gold in the 21st century as it is fueling the success of many companies/enterprises [1]. This trend has led to the collection and processing of an enormous amount of information, especially, PI [2]. Such information can be used to improve and optimize companies' services, reduce costs, increase profits, identify and effectively target potential customers, etc. [1, 2]. In response to this trend, many privacy-relevant regulations/laws have been enacted (e.g., the General Data Protection Regulation (GDPR)) [3]. Consequently, privacy compliance has become a main concern for companies dealing with PI as failing to comply with these regulations results in huge fines [4].

These regulations rely heavily on the concept of informational self-determination [5]. Accordingly, companies are required to provide privacy protection mechanisms and inform data subjects (DSs) how their PI will be processed, leaving the burden of understanding relevant information and the use of protection mechanisms on the side of DSs. However, a considerable number of studies have demonstrated that most of these mechanisms fail to safeguard users because users do not understand how to use them properly [6].

Joint Proceedings of RCIS 2024 Workshops and Research Projects Track, May 14-17, 2024, Guimarães, Portugal

mohamad.gharib@ut.ee (M. Gharib)
0000-0003-2286-2819 (M. Gharib)

The Usable Security and Privacy (USP) research area aimed to solve this problem for the last few decades [6, 7]. Still, most existing USP solutions either are not designed for novice users or there is no proper management of conflicts between security/privacy, and usability, etc. [6]. This problem could be solved if the solution is designed with respect to the DS's capability for making informed decisions. However, it is not always easy to design a system that fits the needs of DSs with different experiences. Specifically, there will be always a gap between what is expected from some DSs and what they can actually do.

A potential solution is the use of heuristics that can be defined as mental shortcuts or rules of thumb, which can be employed to decrease the cognitive burden and speed up the process of decision-making [8, 9]. Specifically, privacy heuristics can be used to assist users in making informed decisions and acting accordingly. However, work on privacy heuristics is scarce due to their complex design as well as the belief that they do not guarantee optimal solutions [9]. Moreover, general usability heuristics (e.g., Nielsen heuristics [10]) do not directly apply to privacy. This paper aims to tackle this issue by proposing a privacy heuristics model and a corresponding method, which can be used to design usable privacy solutions.

The rest of the paper is organized as follows; Section 2 presents the baseline of this research. We propose our privacy heuristic model in Section 3, followed by the corresponding method to be used for designing usable privacy solutions in Section 4. We demonstrate the model and method applicability and utility by applying them to an illustrative example in Section 5. Finally, we conclude and discuss future work in Section 6.

2. Baseline

2.1. Heuristics: Origins and Evolution

The origin of the heuristics term goes back to Ancient Greek, which means "serving to find out or discover" [11, 8]. Heuristics are often characterized as 'mental shortcuts' or 'rules of thumb' [8, 9], which can be used to decrease the cognitive burden and reduce difficult decisions to solvable simple ones [9, 11]. Although the notion of heuristics has gained significant attention in a wide range of fields, including psychology, decision theory, and computer science [9, 11, 12], researchers still struggle to find an accurate agreed-upon definition of heuristics [9], i.e., the range of what has been called heuristics is very broad [9]. Some scholars have even debated that the heuristic concept has lost its meaning [12, 13], and its definition has changed almost to the point of inversion [12, 13]. Other researchers concluded that the heuristic concept is vague enough to describe anything that is why it is used to describe nearly everything [12].

Despite this, many definitions of heuristics have been introduced. For instance, heuristics has been defined as a simple procedure that facilitates finding adequate, though often imperfect, answers to difficult questions [14], as a strategy that ignores part of the information, to make decisions more quickly, and/or accurately than more complex methods [11], and as a simple but useful method for problem-solving, decision-making, and discovery [8]. Reviewing the previous (and other) definitions, it is easy to note that most of them are vague. For example, how simple a heuristic has to be, and how do we know if it is still useful? What an adequate means? Why it is often imperfect? Consequently, we need to answer all these questions to classify a thing as a heuristic.

On the other hand, heuristics used to be seen as a problem-solving method that *does not guarantee an optimal solution* [9]. Specifically, heuristics save efforts at the cost of accuracy (called *Accuracy-Effort Trade-Off*) [12]. In this view, heuristics are error-prone mental tools and poor substitutes for computations that are too demanding for ordinary minds to carry out [13]. However, a new view started to emerge in the early 90s, which suggests that heuristics, rather than leading to irrationality, enable rationality [13]. Moreover, recent studies have shown that heuristics can outperform more complex strategies (less-is-more effects) [11, 8]. In this work, we adopt this view, and we briefly discuss the dual heuristic-systematic model in the next subsection.

2.2. The Heuristic-Systematic Model

The heuristic-systematic model (shown in Fig. 1) is one of the most prominent dual-process models that aim to explain how individuals receive and process information for making a decision [11]. The model states that individuals can process information for making a decision in one of two modes: heuristically or systematically [15]. However, later studies have confirmed that individuals may use both modes simultaneously [16]. The *systematic processing mode* involves in-depth and comprehensive analysis and cognitive processing of decision-relevant information [15, 17]. On the contrary, *heuristic processing mode* refers to the use of simplifying decision rules or heuristics (judgmental rules) to quickly assess decision-relevant information [18, 17].

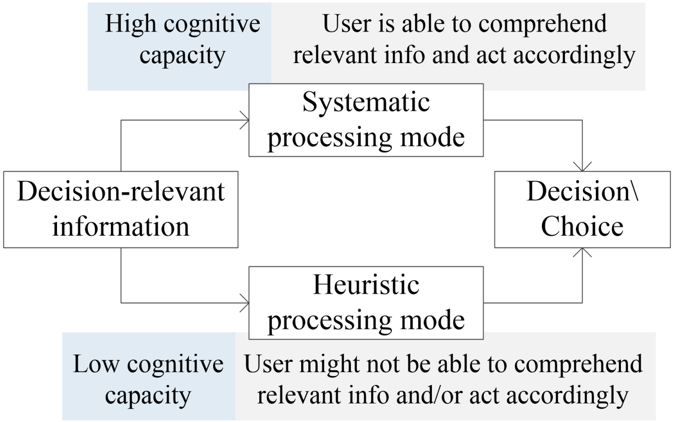
High cognitive capacity
User is able to comprehend relevant info and act accordingly
Systematic processing mode
Decision-relevant information
Decision\ Choice
Heuristic processing mode
Low cognitive capacity
User might not be able to comprehend relevant info and/or act accordingly

Figure 1: The Heuristic-Systematic model

According to Eagly and Chaiken [18] the processing mode is determined by the cognitive capacity of the individual. More specifically, when individuals have the required cognitive capacity they, most likely, will proceed using the systematic processing mode. Otherwise, they will rely on the heuristic processing mode. Moreover, choosing the processing mode is highly influenced by the consequences of the decisions [16]. In particular, individuals, most likely, will use the heuristic processing mode when they believe their decision will not have significant consequences on themselves. In contrast, they will use the systematic mode (if they can) for decisions that might have serious consequences.

3. A Heuristic Model for Usable Privacy

This section proposes the privacy heuristic model that has been constructed taking into consideration the dual heuristic-systematic model since a DS might use heuristic or systematic processing mode or both of them simultaneously. In other words, this model allows considering DSs with different capabilities for making informed decisions (e.g., expert and novice DSs).

The model (shown in Fig. 2) adopts the four key main concepts of the dual heuristic-systematic model, namely: decision-relevant information, heuristic processing mode, systematic processing mode, and decision/choice, which we call privacy decision. We also consider three key concepts, which are essential for the model, namely: DS, PI, and privacy requirements. The first represents the entity of concern that will make the decision, the second is the subject of the decision, and the last will be used to derive the criteria for an informed privacy decision, i.e., the decision should be compliant with the privacy requirements of the DS. We define the above concepts as follows:

A *DS* represents a natural person, who can be identified directly or indirectly by reference to an identifier [19]. *PI* represents any information that can be related, directly or indirectly, to an identified or identifiable natural person (DS), who has the right to control how such information can be used by others [19]. *Privacy requirement* represents the specifications that must be met to ensure the DS' needs concerning the collection, use, storage, and processing of her PI [19]. *Decision-relevant information (DRI)* refers to data, facts, or details necessary for making an informed decision. E.g., why the decision is required, what are its consequences, etc. *Systematic processing mode* refers to the systematic use of decision-relevant information [15, 17]. *Heuristic processing mode* refers to the use of simplifying decision rules or heuristics to assess decision-relevant information quickly [18, 17]. Finally, *a privacy decision* refers to the act of making a conscious determination regarding the extent to which a DS's PI is processed by others.

The processing mode, as previously discussed, is determined by the individual's cognitive capacity [18], which can be defined as the ability to acquire and utilize relevant knowledge. Accordingly, a DS should have the required knowledge for making an informed decision (Declarative knowledge (know-that)) and act accordingly (Procedural knowledge (know-how)). These two types of knowledge can be defined, as follows: *Declarative knowledge* is the knowing of *this* or*that*, i.e., knowing about things [20], and *Procedural knowledge* is the knowing of *how* to do things or the steps/strategies involved in how to do things [20].

A DS should have the previously mentioned types of knowledge to use the *systematic processing mode*, as well as specifying her privacy requirements. Otherwise, a DS will completely or practically rely on the *heuristic processing mode*, which is required to offer the DS the required knowledge through privacy heuristics for the previous activities. We define the concepts relevant to this type of processing, as follows: *Privacy Heuristic (PH)* is a type of heuristics that is specialized for privacy, which has an *Acceptance Criteria (AC)*. *AC* offers a checklist that can be used to assess the aforementioned PH. The main aim of a PH is to offer *procedural* and/or *declarative information* that contribute to the *procedural* and/or *declarative knowledge* respectively, which are required for making an informed privacy decision. Please note that it is arguable whether knowledge can be transferred, but knowledge can be interpreted as information as well as the rules over it to infer new information, which can be transferred [21].

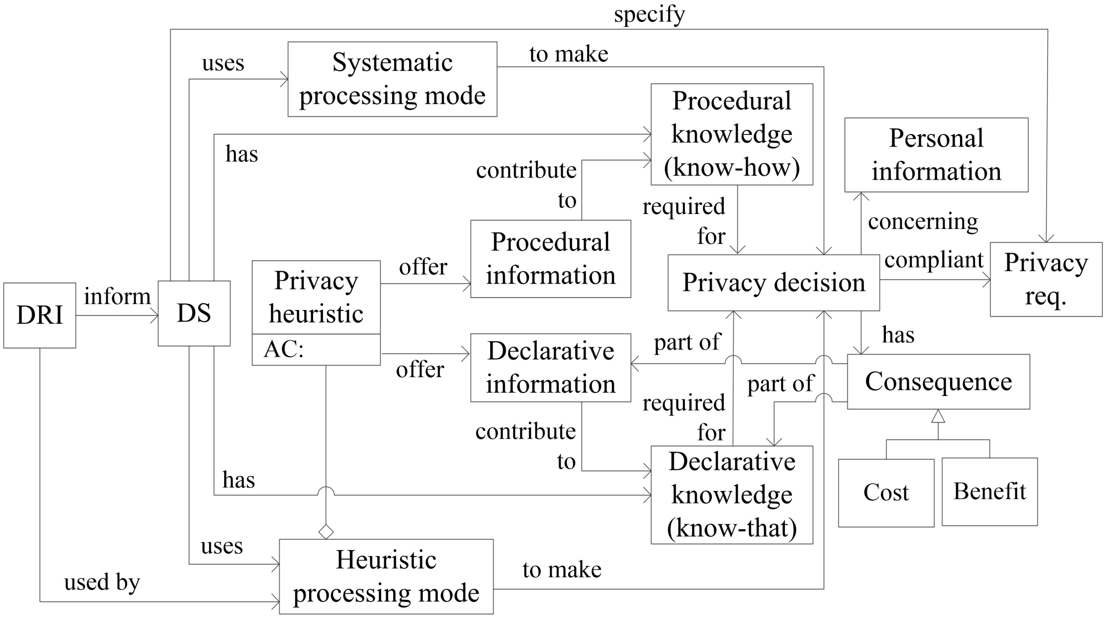

Figure 2: The Heuristic-Systematic metamodel

Therefore, we use *procedural* and *declarative information* concepts as means to contribute to the required *procedural* and *declarative knowledge*.

As already discussed, the consequences of the decisions might influence the selection of the processing mode [16], but such consequences also influence the privacy decision itself as indicated by numerous scholars (e.g., [22]). Specifically, privacy decisions are highly influenced by the consequences of such decisions in terms of their costs and benefits [22], i.e., a DS's privacy decisions are determined by a rational calculus of the benefits and costs. As the consequences are mainly related to the *"know that" knowledge*, it should be a part of the *declarative information*, and in turn, of the *declarative knowledge*. We define the relevant concepts, as follows: *consequence* refers to the effect, result, or outcome of a privacy act or a decision. A *cost* is the probability of having a negative outcome of a privacy decision that has an unfavorable effect on the DS. On the contrary, a *benefit* is the probability of having a positive outcome of a privacy decision that has a favorable effect on the DS.

4. A heuristics-based method for designing usable privacy solutions

After presenting our model and describing its key concepts, we present its corresponding method that has been designed to utilize the model and to guide the design of heuristics-based usable privacy solutions in this section. The process is shown in Fig. 3, and it is composed of four consecutive steps:

1. Identify relevant privacy requirements. Any privacy decision needs to be compliant

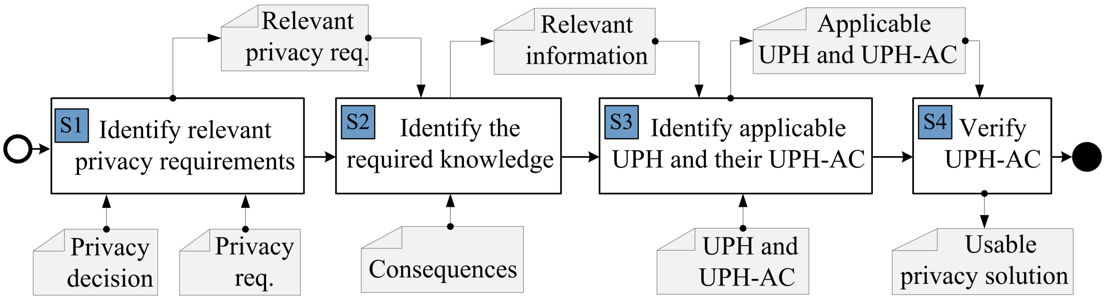
Relevant privacy req.
Relevant information
Applicable UPH and UPH-AC
S1 Identify relevant privacy requirements
S2 Identify the required knowledge
S3 Identify applicable UPH and their UPH-AC
S4 Verify UPH-AC
Privacy decision
Privacy req.
Consequences
UPH and UPH-AC
Usable privacy solution

Figure 3: A heuristics-based method for designing usable privacy solutions

with the DS' privacy requirements. Accordingly, this step takes the privacy decision and a set of privacy requirements as input aiming to identify a subset of these requirements relevant to the decision of concern. As for a comprehensive set of privacy requirements, we adopted eight privacy requirements presented in our previous work [19], namely: confidentiality, anonymity, unlinkability, unobservability, notice, minimization, transparency, and accountability.

2. Identify the required knowledge. This step takes the privacy requirements identified in the previous step as well as the consequences of the decision of concern as input. Then, based on them, specifies the knowledge required for making an informed privacy decision. After that, it derives the *procedural* and/or *declarative information* for the identified *procedural* and *declarative knowledge.*

3. Identify applicable usable privacy heuristics (UPH) and their corresponding Acceptance Criteria (UPH-AC). This step takes a set of UPH and their corresponding UPH-AC step as well as the *procedural* and *declarative information* identified in the previous as input. Then, identify UPH and UPH-AC applicable to such information. As mentioned earlier, work on privacy heuristics is scarce, thus, we used available usable security heuristics (e.g., [23, 24, 7]), which has been built based on usability heuristics (e.g., Nielsen's heuristics [10]) to develop our list of UPH and their UPH-AC that is shown in Table 1.

4. Verify UPH-AC. This step takes the applicable UPH and their corresponding UPH-AC identified in the previous step as input and verifies whether the AC for each UPH has been satisfied in the design of the usable security solution. If any of them is not satisfied, the solution needs to be modified accordingly. The step might be iterative until all AC of the applicable UPH are satisfied.

Table 1: UPH and their corresponding UPH-AC

UPH1.	**Visibility:** the system should keep DSs informed about their privacy choices.
UPH1AC.	Is there a feedback for every privacy-related action?
UPH2.	**Revocability:** the system should allow DSs to revoke any privacy actions.
UPH2AC.	Can DSs easily reverse their privacy actions?
UPH3.	**Clarity:** the system should inform DSs about the consequences of any privacy actions.

UPH3AC.	Does the system warn DSs if they are about to make a potentially privacy error?
UPH4.	**Expressiveness:** the system should guide DSs on privacy while still gives them freedom of expression.
UPH4AC.	Is there a clear understanding of the systems privacy options?
UPH5.	**Learnability:** the system should ensure that privacy actions are easy to learn and remember.
UPH5AC.	Are privacy operations easy to learn and use?
UPH6.	**Minimalist design:** the system should offer DSs relevant information relating to their privacy actions.
UPH6AC.	Is only the privacy information essential to decision-making displayed to the user?
UPH7.	**Errors:** the system should provide DSs with detailed privacy error messages that they can understand and act upon.
UPH7AC.	Do error messages suggest the cause of the privacy problem, and how it can be corrected?
UPH8.	**Satisfaction:** the system should ensure that DSs have a good experience when making a privacy decision and that they are in control.
UPH8AC.	Do privacy-related prompts imply that the user is in control?
UPH9.	**User suitability:** the system should provide options for DSs with diverse levels of skill and experience in security.
UPH9AC.	If the system supports both novice and expert DSs, are multiple levels of privacy error messages available?
UPH10.	**User assistance:** the system should make privacy help apparent to DSs.
UPH10AC.	Is there a visible privacy help?

5. Demonstrating the Applicability and Utility of the Model and Method

We illustrate the utility of the model and method by applying them to an illustrative scenario concerning the social network platform. Consider for example a scenario of a DSs, Sarah, who is using a social network platform to connect with friends, colleagues, etc., and share content (information, photos, etc.) interests, and activities with her contacts. Sarah wants to enjoy the platform while maintaining her privacy. Let's consider one privacy-related decision of Sarah: "posting content about an activity with her friends while she is supposed to be working remotely". Concerning this decision, in *Step 1* will need to identify relevant privacy requirements. Although several privacy requirements might be relevant, we will consider only one of them for simplicity, namely: *confidentiality*.

For *Step 2*, we need to identify the knowledge (procedural and/or declarative) required for making an informed privacy decision based on the identified privacy requirements (i.e., *confi-*

dentiality) and the decision-relevant consequences in terms of its *benefits* and *costs*. Concerning the *benefits*, many aspects might be relevant (e.g., self-satisfaction, feeling connected, gaining attention), and for the *costs*, they may range from losing the job, harming professional reputation, etc. In this context, it is easy to understand why DSs tend to share on social platforms, but we need to know when they should not or at least control who can see their post. Consequently, Sarah will require declarative knowledge that enables her to answer questions like *who can see the post? Who should not see the post? does the post contain information/PI that should not be there?* etc. She also will require procedural knowledge that enables her to use the posting mechanism in a privacy-aware manner, i.e., she should be able to know *who can see the post, how she can specify/modify who can see the post, how she can modify the post, or even delete it if required*, etc.

After identifying the required knowledge, we can specify information that can contribute to such knowledge. In short, such information should enable Sarah to answer the declarative knowledge-related questions mentioned above and enable her to use the posting mechanism in a privacy-aware manner. This information is used in *Step 3* to identify the UPHs and their corresponding UPH-AC. Specifically, these UPHs need to be provided by the platform to enhance the usable privacy of its users.

Reviewing the UPH listed in Table 1, we can identify that we need to consider the following UPHs for declarative information: *UPH1. Visibility*, the system should keep Sarah informed about her privacy choices, e.g., before posting, the system should provide a UPH that informs Sarah about who will see her post when shared, and whether this is an adequate group of contacts, as well as a UPH that scans the post and highlights PI. *UPH3. Clarity*, the system should inform Sarah about the consequences of posting, e.g., the system should provide a UPH that when detecting that the post is shared with an inadequate group of contacts, or contains PI that should not be shared, the UPH will highlight potential cost such as losing job or harming professional reputation, etc. *UPH9. User suitability*, the UPHs mentioned above should provide Sarah with more detailed information if the provided information is not sufficient for Sarah to make an informed decision.

We also need to consider the following UPHs for procedural information: *UPH2. Revocability*, the system should provide information about revoking any privacy action, e.g., the system should provide a UPH that informs Sarah how she can delete/modify her post when there is a need. *UPH5. Learnability*, the system should ensure that all privacy actions are easy to learn and remember. Finally, *UPH10. User Assistance*, the system should make privacy help apparent to Sarah, e.g., all implemented UPHs should be accompanied by a UPH that provides cues for Sarah about existing help to correctly finalize the action.

After the implementation of the solution, the UPH-ACs of all implemented UPHs are verified at *Step 4*, to ensure that each of the UPH has been satisfied in the design of the usable security solution. If any of them is not satisfied, the solution needs to be modified accordingly.

6. Conclusions and Future Work

In this paper, we aimed to tackle the problem of designing usable privacy solutions by proposing a privacy heuristics model and a corresponding method, which can be used to design such solutions. We have also demonstrated the applicability and utility of the model and method with an illustrative example.

For future work, we plan to investigate the effectiveness of adopting the dual heuristic-systematic model in practice with potential users that have different levels of experiences, and better understand the reasons for adopting the mode of processing. Moreover, we aim to provide guidelines for developing *responsible UPHs*, i.e., UPHs that do not result in bias. We also plan to use the model and method as a basis to develop a heuristics-based approach for designing usable privacy solutions. This will also require extending the UPH list as well as their corresponding UPH-ACs. The developed approach will be evaluated by privacy experts and validated by applying it to case studies from different domains.

Acknowledgment

This study 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).

References

[1] M. Gharib. Privacy and Informational Self-determination Through Informed Consent: The Way Forward. In *LNCS*, vol. 13106, pp. 171–184. Springer Science and Business Media Deutschland GmbH, 2022.

[2] D. Neally. Data Brokers and Privacy: An Analysis of the Industry and How It's Regulated. *Adelphia LJ*, 22:30, 2019.

[3] M. Gharib, J. Mylopoulos, and P. Giorgini. COPri - A Core Ontology for Privacy Requirements Engineering. In *Research Challenges in Information Science*, vol. 385, pp. 472–489. Springer, 2020.

[4] M. Gharib, P. Giorgini, and J. Mylopoulos. Towards an Ontology for Privacy Requirements via a Systematic Literature Review. In *LNCS*, vol. 10650, pp. 193–208. Springer Verlag, 2017.

[5] M. Gharib. Toward an architecture to improve privacy and informational self-determination through informed consent. *Information and Computer Security*, 30(4): pp.549–561, oct 2022.

[6] D. Jacobs and T. McDaniel. A Survey of User Experience in Usable Security and Privacy Research. In *LNCS*, vol. 13333, pp. 154–172. Springer Science and Business Media Deutschland GmbH, 2022.

[7] M. Gharib. US4USec: A User Story Model for Usable Security. In *Research Challenges in Information Science (RCIS)*, pp. 1–16. Springer, 2024.

[8] R. Hertwig and T. Pachur. Heuristics, History of. In *International Encyclopedia of the Social and Behavioral Sciences: Second Edition*, pp. 829–835, 2015.

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

[10] J. Nielsen. Nielson, J. 10 Usability Heuristics for User Interface. Tech. rep. 1995.

[11] G. Gigerenzer and W. Gaissmaier. Heuristic decision making. *Annual Review of Psychology*, 62:451–482, jan 2011.

[12] A. K. Shah and D. M. Oppenheimer. Heuristics Made Easy: An Effort-Reduction Framework. *Psychological Bulletin*, 134(2):207–222, 2008.

[13] D. G. Goldstein and G. Gigerenzer. Models of ecological rationality: The recognition heuristic. *Psychological Review*, 109(1):75–90, 2002.

[14] D. Kahneman. *Thinking, fast and slow*, vol. 31. 2011.

[15] S. Chaiken, A. Liberman, and A.H. H. Eagly. Heuristic and systematic information processing within and beyond the persuasion context. *Unintentent Thought*, 16:212–252, 1989.

[16] S. Chen and S. Chaiken. The heuristic-systematic model in its broader context. *Dualprocess theories in social psychology*, pp. 73–96, 1999.

[17] S. Chen, K. Duckworth, and S. Chaiken. Motivated Heuristic and Systematic Processing. *Psychological Inquiry*, 10(1):44–49, 1999.

[18] AH Eagly and S Chaiken. *The psychology of attitudes.* Harcourt brace Jovanovich college publishers, 1993.

[19] M. Gharib, P. Giorgini, and J. Mylopoulos. COPri v.2 — A core ontology for privacy requirements. *Data and Knowledge Engineering*, 133:101888, 2021.

[20] G. Schraw. Promoting general metacognitive awareness. In *Instructional Science*, vol. 26, pp. 113–125, 1998.

[21] D. Stenmark. Information vs. knowledge: The role of intranets in knowledge management. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pp. 928–937. IEEE, 2002.

[22] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[23] A. Yeratziotis, D. Pottas, and D. v. Greunen. A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm. *International Journal of Human-Computer Interaction*, 28(10):678–694, oct 2012.

[24] M. Mujinga, M. M. Eloff, and J. H. Kroeze. Towards a heuristic model for usable and secure online banking. In *Proceedings of the 24th Australasian Conference on Information Systems*, pages 1–12, 2013.