How to Protect My Privacy? - Classifying End-User Information Privacy Protection Behaviors

Frank Ebbers

▶ **To cite this version:**

Frank Ebbers. How to Protect My Privacy? - Classifying End-User Information Privacy Protection Behaviors. 14th IFIP International Summer School on Privacy and Identity Management (Privacy and Identity), Aug 2019, Windisch, Switzerland. pp.327-342, 10.1007/978-3-030-42504-3_21 . hal-03378956

HAL Id: hal-03378956

https://inria.hal.science/hal-03378956v1

Submitted on 14 Oct 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

How to Protect my Privacy? - Classifying End-User Information Privacy Protection Behaviors

Frank Ebbers[1]

[1] Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Str. 48, 76139 Karlsruhe, Germany
frank.ebbers@isi.fraunhofer.de

Abstract. The Internet and smart devices pose many risks at users' information privacy. Individuals are aware of that and try to counter tracking activities by applying different privacy protection behaviors. These are manifold and differ in scope, goal and degree of technology utilization. Although there is a lot of literature which investigates protection strategies, it is lacking holistic user-centric classifications.
We review literature and identify 141 privacy protection behaviors end-users show. We map these results to 38 distinct categories and apply hybrid cart sorting to create a taxonomy, which we call the "End-User Information Privacy Protection Behavior Model" (EIPPBM).

Keywords: Privacy Protection · Protection Behavior · Protection Activities · Privacy Responses · Taxonomy · Classification · Model · User-Centric

1 Introduction

The Internet and smart devices have become omnipresent. Besides all their advantages, it also poses various information privacy risks. Devices and services in the Internet collect, send and receive personal data of its users. For example data from smartphone sensors, e.g. gyroscopes, can reveal the gender of the user [1]. And even a smart light bulb can reveal a user's location [2]. Different parties collect these personal information, because they are valuable for them [3, 4], for example to offer personalized advertisement or to improve their products and services [5, 6]. However, these parties can misuse personal data for unforeseen and even illegal scenarios [3, 7].

Users in Germany are aware that they are tracked [8]. Although "[i]nvasion of privacy are increasingly regarded as acceptable" [9], recent studies show that users feel that governments and companies do not enough to protect personal data [10, 11]. With the rise of tracking activities in the web and with smart devices [12], users' information privacy concerns rose accordingly in recent years [10]. Thus, individuals try to address their concerns by showing privacy protections behaviors [13] or coping strategies [14]. These can be manifold and vary in scope, goal and technique [15]. Thus they follow a

multitude of specific responses. Scholars have investigated such privacy protection responses and suggested different classifications [e.g. 13, 16]. However, only few researchers visualize their work in a taxonomy or model [e.g. 17]. A structured visualization, could support users to identify behaviors that fit their needs or coincide their skills. For research a state-of-the-art classification can be a useful tool for investigating user behavior [14, 18].

There is an ongoing debate about if individuals should be responsible for their data protection and if they could protect effectively [19]. However, our work concentrates on creating a model of end-user privacy protection without considering this debate. Accordingly our research question is: *How can end-user privacy protection behaviors be represented in a comprehensive model while incorporating prior classification approaches.* To address this research question we conducted a literature review and identified 141 protection behaviors. In a next step, we mapped these behaviors to 38 distinct categories. Based on this we finally apply card sorting to created a hierarchical model.

The remainder of this article is structured as follows: In the second section, an overview of users' protection behaviors and classification approaches is presented. In the methodology (section 3), we describe the iterative literature review and model creation. Section 4 presents the model details. The article concludes with a discussion of the findings (section 5) and an outlook (section 6).

2 Related Work on End-User Privacy Protection Classification and Modeling

Researchers have proposed different classification approaches that vary in scope, criteria and the way of representation. Further they differ in denominations so that a plurality of terms is found: practices [16, 19], activities [20], strategies [14, 19, 21, 22], responses [17], mechanisms [23, 24] and reactions [14]. Other classifications involve coping strategies [14] by which users asses "the expectancy that one's response can reduce the actual danger" [14]. For simplicity reasons we subordinate coping to behavior and use this as an umbrella term in this paper. Behavior refers to "a particular way of acting" [25] and therefore includes all previously mentioned terms. Further we use the term privacy but refer to information privacy as the "access to individually identifiable personal information" as defined by [26].

Privacy protection behavior of end-users is manifold and depends on diverse characteristics, such as user concerns and willingness to take risks, digital literacy and experience [13, 14, 27, 28]. Thus, authors identify myriad protection behaviors. Some categories are simple, whereas others are more advanced and complex.

2.1 High-level classifications

Several authors suggest high-level classifications. For example Buchanan et al. [29] identifies two factors based on an analysis of users' privacy concerns: "general caution" (e.g. search for privacy certifications) and "technical protection of privacy", which needs a certain level of computer literacy to e.g. delete cookies. A similar differentiation

is found in Lwin et al. [30]. They differentiate between deflective behaviors, which means to avoid data collection, and defensive behaviors, which focusses on removing personal information from a vendor's database. Others emphasize limiting information sharing [13, 20, 28]. Xu et al. [15] classify protection behaviors by emphasizing control of information flows between data subjects and service providers. They distinguish personal control agency, which "empowers individuals with direct control over how their personal information may be gathered by service providers" [15]. Whereas proxy control agency concerns industry self-regulation and government legislation.

2.2 Active and passive

Other authors differentiate between active and passive behaviors, [e.g. 22, 31, 32 or 33]. Active behaviors means that users engage to utilize countermeasures directly. Passive behavior primarily involves the "general decision to share or not to share personal information" [19]. Other passive behaviors involves relying on external entities, such as data protection authorities [34] or to ask other individuals, e.g. parents [35].

2.3 Chronological classifications

Further, one can distinguish countermeasures adopted before or after a data disclosure. Several authors write about preventive (ex ante) and protective or reactive strategies (ex post) [22, 36]. Lampinen et al. [21] call these preventive and corrective strategies. Lwin et al. [30] differentiates between deflective (prevention-focused) and protective measures. A similar distinction is introduced by [14]. They distinguish threat appraisal (ex ante), the analyzation of "probabilistic characteristics of a potential threat" [14] and coping appraisal, where users evaluate options to diminish the threat ex post. Moshki and Barki [14] highlight three categories of coping based on a temporal sequence: before an event (anticipation period), during (impact period) and after (post-impact period). Another classification mentions prevention, avoidance and detection [24]. Prevention mechanisms try to ensure that "undesirable use of private data will not occur" (ex ante) [24]. Avoidance mechanism minimize risks associated with data exchanges "by carefully considering the context in which they take place" (ex ante) [24]. Detection mechanisms seek to find privacy incidents (ex post).

2.4 Classification from a technological perspective

Protection can be supported by technology or not [15, 29]. Several authors concentrate purely on a technological perspective. Jiang et al. [24] identifies "mechanisms" that are supported by tools. Other authors mention to use ad blockers, cookie management or enabling Do-Not-Track functions in web browsers [13]. Further authors, such as [37], focus on countermeasures utilizing privacy enhancing/preserving technologies and distinguish them on a technological basis [18].

2.5 Fine-grained approaches

As an overview Yap et al. [16] identify seven categories of what they call "privacy management practices", namely: (1) withdraw, (2) defend, (3) neutralize, (4) feint, (5) (counter) attack, (6) perception management, and (7) reconcile. Lwin et al. [38] define three defensive measures, namely: fabricate (use of false information), protect (utilization of technologies), and withhold (refusal to provide data). A quite similar wording is found in Metzger [39]. She states three behavior types, what she calls "rules": withholding information, falsifying information and information seeking (informing oneself about a company before disclosing data).

2.6 Taxonomies and Models

Taxonomies and models aim to make difficult relationships easy-understandable or to visualize hierarchical structures. However only very few authors created such to visualize the relationship of their privacy protection categories. In the next sections two models are presented, which gained wide recognition.
One prominent example is introduced by Son and Kim [17]. They define a set of responses to privacy threats, calling their model "Information Privacy-Protective Responses" (IPPR) (Figure 1). Son and Kim [17] focus on three main behavioral responses:

1. *Information provision* affects users when they are asked to disclose personal information in registration forms on websites. The authors suggest two possible responses: refuse to disclose information or to falsify them (misrepresentation). Whereas refusal often goes along with a loss of functionality, misrepresentation is considered as "a less costly and more convenient option" [17].
2. *Private action* represents the fightback once users lost control over their data, e.g. when receiving unwanted marketing emails. The authors divide this complaining behavior into removal (e.g. by opting-out) and negative word-of-mouth recommendation to damage a company's reputation.
3. *Public action* means complaining directly to the company or complaining indirectly via independent third-party privacy groups, such as data protection authorities. In contrast to private actions, these complaints are broadcasted to public.

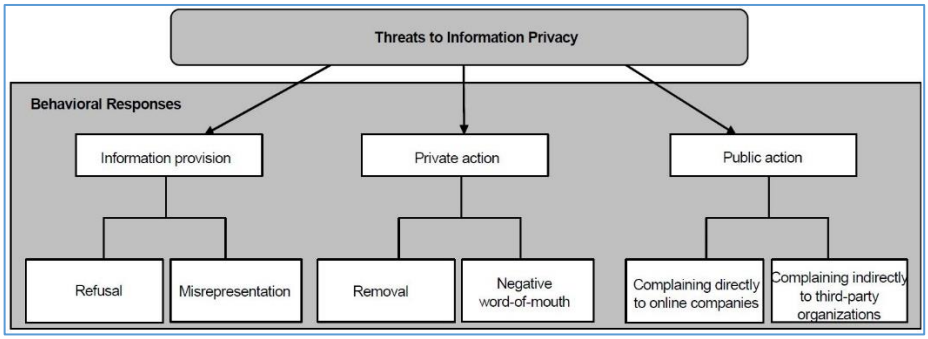

Figure 1 – "Information Privacy-Protective Responses" (IPPR) by [17]

Another model is suggested by Ochs at al. [40]. They classify protection practices in a two-by-two grid, which distinguishes between users' digital literacy and data intensity (Figure 2). Digital literacy means the ability to evaluate and manage information and to facilitate computer technologies. Data intensity concerns the amount of information on which the protection is based on. Data intensity is low for defensive practices. For example, an individual who uses the internet only temporarily create only few information and thus aim for data minimization. Whereas offensive practices are used if individuals don't want to minimize their data disclosure but instead try to obfuscate or falsify information. Accordingly there is a high data intensity.

"*Exclusion practices*" (category A) are defensive approaches that require less digital competencies in order to be successfully applied. Users do not disclose any personal information permanently. "*Controlling practices*" (category B) are defensive approaches that require a certain level of digital competency. The general idea is to control information flows of personal data individually. Whereas category A and B emphasize on individual approaches, "*Exoteric practices*" (category C) rely also on external involvement. These require less digital competency, however the amount of data that is disclosed is much higher than using exclusion practices. With "*Networking practices*" (category D) users try to codify their information exchange. For example users agree upon several abbreviations or code words for communication. Other users obfuscate their data or create fake profiles (avatars) to participate in networks but not reveal their real identity. This requires a certain level of digital literacy.

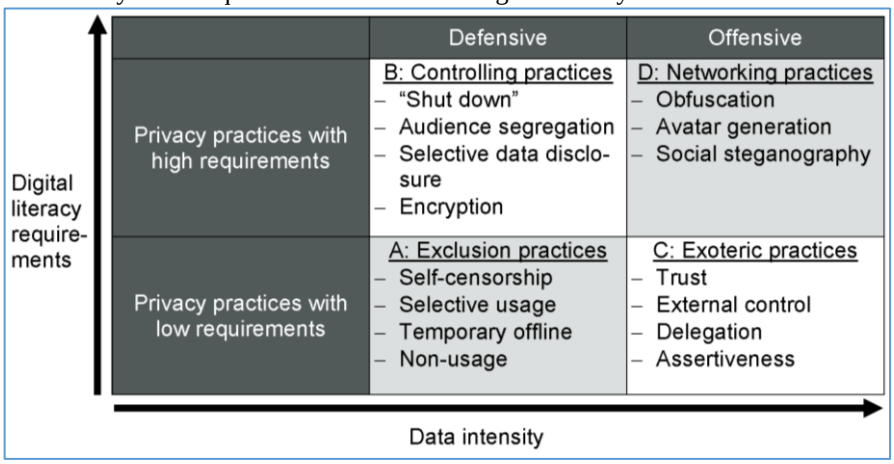

Figure 2 - Privacy practices, adopted from [40] and translated into English by the author

The literature research has shown that there is a myriad of different protection behaviors, which users can apply before and after a data disclosure. These can be of active or passive manner. A majority of behaviors aim for limiting information disclosure. Furthermore protection can be achieved with and even without technical literacy. Lastly the chapter shows two classification models, which represent two very different perceptions of classifying privacy protection behaviors.

3 Methodology

Our research approach was two-fold. First, we conducted an iterative literature review for end-user privacy protection and user-centric classifications utilizing the publication database Scopus[1]. Second, we compared and mapped the findings to create a model.

3.1 Literature review

We conducted an iterative literature search in March and April 2019 using the database Scopus to cover top peer-reviewed journals in fields like computer science, communication science, psychology and law. These seemed most promising to find suitable literature, as privacy is a multi-disciplinary concept [41]. We applied an iterative review approach, following [42] to refine and extend our initial search.

As a first step, we aimed at consolidating privacy protection behaviors of users and came up with 16 keyword strings for our search. After several search iterations (including synonyms and limited to years 2000 until 2019), we reviewed protection behaviors and created a list of their denominations and meanings – resulting in 141 entries. As a last step, we scanned the resulting literature for the keywords "classification", "categorization", "framework" or "model" to find existing approaches. The results show that only two papers [17, 40] deal with visualizing user privacy protection. We conducted a forward and backward search for both papers.

3.2 Classification of Behaviors and Model generation

We manually examined the list to compare the meanings. In cases where wordings were identical, we merged them immediately and selected the original denomination (e.g. refusal [17]). In other cases, a deeper look at the meaning was needed (e.g. feint [16]). Once there was a match with regard to wording, we set the denominations in relationship to each other and chose a coherent name. For example preventive measures [36] and threat appraisal [14] are shown before data is disclosed and therefore belong to the pre-disclosure category[2]. In some cases, the denominations in the literature could be mapped to several others. Finally, we identified 38 distinct categories.

Next, we started creating the model by applying hybrid card sorting. Originally card sorting was used in usability engineering to create menu structures [43]. However it has gained popularity in creating structures and hierarchies as well [44]. Hybrid card sorting means that users can add new categories to some pre-defined ones. To do so we wrote each category on a note. We used the model proposed by Son and Kim [17] as our starting point for the hybrid card sorting, as it has been widely used in literature. However we allowed to change the nominations of their categories. After nine rounds of sorting, a final structure was created. As a last step, we indicated if there is a need for technological or non- technological means to fulfill the protection practice in each category on the third and fourth level.

[1] https://www.scopus.com.

[2] A figure of the complete taxonomy can be found at: linksplit.io/EIPPBM.

4 Results and Explanation of the Model

Our results consist of two parts:

1. a list of privacy protection behaviors derived from a literature review and its mapping to distinct categories (see footnote 2), and
2. a classification model (Figure 3), which we call "End-User Information Privacy Protection Behavior Model" (EIPPBM).

The literature review and the classification show that protective behaviors are multifaceted. Our literature review ends up with a list of 141 behaviors, which are assigned to 38 distinct categories. Authors name behaviors very differently. This might be because privacy means different things to different people [26, 45]. To make up the EIPPBM, the categories are arranged on four hierarchical levels. In the name of model we use the term "information privacy" to make absolutely clear that we do not refer to physical privacy, even if someone watches the model without reading this paper. Same applies to the term "end-user" to make clear that the model is not addressed to developers or other high-level groups. The model indicates which behaviors are supported by technological means and which do not need any technology or digital literacy to be applied. Our results show that users can do a majority of behaviors (79 percent) with little or no digital literacy. In the following paragraph the four levels of the model are explained in detail. We want to note that the explanatory names of the levels do not necessarily correspond with the categories identified in the related work section.

Level 1 - Chronological Distinction:

In contrast to [17] the EIPPBM introduces a chronological distinction on the first level. These pre- and post-disclosure behaviors can be interpreted as preventive or defensive actions and are made by several authors [such as 14, 18, 22, 30, 46]. This distinction on the very first level seems plausible, because all subordinated behaviors can be allocated clearly to a temporal order.

Level 2 - Active vs. Passive:

The second level is characterized by the distinction between active and passive behaviors. Whereas passive behaviors involve the "general decision to share or not to share personal information" [19], active behaviors "serve to build a protected sphere" [19]. The latter need a direct involvement of the user. This distinction is widely used in literature [such as 22, 31–33].

Level 3 - Superordinate Behaviors:

Groups of behaviors are introduced on the third level. These categories are superordinate and base on behaviors found in literature. Hence, these categories do not necessarily represent a specific or direct behavior and instead signify general goals a user tries to achieve. These are manifold and thus can be split on the subjacent (fourth) level. Further, a distinction between behaviors that are supported by technological or non-technological means is introduced at this level and indicated by the black (non-technological) and grey (technological) boxes. There are the following categories:

- *Delegation* appears before and after a disclosure. Accordingly, this category occurs twice in the model. It is applied by users when they feel overstrained with internet usage and seek for external support [40].

- *Avoidance* refers to the concept of users to "strategically removing themselves from potential privacy-related situations" [16], for example by simply not using an Internet service [40]. Other authors name these approaches escape [14] and deflective behavior [30].
- *Limit information publishing* deals with all behaviors that aim at limiting information disclosure [13, 28] and consolidates many specific approaches. Son and Kim [17] identify this as an important "privacy response".
- The category *privacy protection tools* refers to the countermeasure by applying tools or apps, such as ad blockers, to prevent tracking [28]. Different authors highlight the preventive character [24, 30, 36].
- After a data disclosure users can consult *transparency enhancing tools* to get "insight about what data have been processed about them and what possible consequences might arise" [47].
- *Learning and informing* occupies a special position as users can apply it before and after a data disclosure. This can be either self-learning to avoid privacy pitfalls or as a "lessons learnt" after a privacy incident [35]. Informing refers to the idea of detection, which "assumes that some undesirable use will occur, and seeks to find such incidents" [24]. This category links both pre- and post-disclosure branches. Therefore, it can be seen as a central point of privacy protection behaviors.

Level 4 - Specific Behaviors:

This last level represents specific practices and are subjacent to the categories named in the third level. These represent behaviors, which users show when having a specific goal or are more aware of their protective options. In sum, there are thirteen categories. However, each category itself can contain a plurality of subjected behaviors (cloud shape). The cloud shape symbolizes that these behaviors are not collectively exhaustive and may contain many more.

Pre-disclosure behaviors:

- Users can *trust in proxy control* before and after a data disclosure. This can be considered as coping strategies. Users "attempt to align themselves such that they are able to gain control through powerful others" [15]. Powerful others can be *external authorities* such as data protection authorities. Further individuals can *trust in industry self-regulation* or in *general legislation* [15]. Moreover users can have *confidence in privacy enhancing technologies* [48]. As there might be several more, these practices are put in the cloud shape.
- Users can *trust in a specific company* and thus do not feel concerned with privacy issues [49, 50] (coping).
- *Non-Usage* is the most radical way of protection [40].
- With *selective usage* individuals choose to be temporarily offline or to use only services that seem trustworthy to them [40].
- Users can *refuse* to publish information [16, 17, 38], if they are not mandatory.
- If data fields are mandatory, users can provide incorrect or incomplete data [17, 20, 35], which refers to *falsifying and incompletion*.
- *Selective data disclosure* contains different approaches. Users can *select the audience* or the type of information they want to disclose [40]. With *(social)*

encryption two individuals communicate in a language that an analytical program cannot encode [40]. *Changing default privacy settings* can limit unintended data disclosure [13, 20]. Also blacken personal documents before sending them to third-party [51], called *neutralize* by [16], is a countermeasure.

- *Obfuscation* "is the production of noise modeled on an existing signal" [52]. For example consumers use multiple email addresses [16]. *Camouflage* use a similar approach, however "try[ing] to vanish from view entirely" [52].
- *Privacy calculus reconciliation* is the only practice within the model that is intrapersonal. Thus it rather represents a coping strategy than an actual behavior. Users "engage in an intrapersonal dialogue […] to rationalize away their desires and concerns for privacy […] to convince themselves that they remain in control" [16].

Post-disclosure behaviors:

- Even after a data disclosure, users can *trust in proxy control* such as *external authorities* [34]. Depending on the legal circumstances in the respective country, users can *rely on jurisdiction* [53].
- Making *public activities* users complain publicly and manifestly about a company. This behavior fits into two types: "*direct complaints* to sellers and *indirect complaints* made to third-party organizations" [17].
- Users make *private activities* when they boycott a particular company, e.g. by asking to be *removed* from a mailing list. Alternatively customers can *communicate* their negative experience to relatives or friends [17]. However, these behaviors are not done publicly. In contrast to [17], we name it "activities" instated of "actions" to emphasize that some behaviors can be permanent.
- In contrast to removal, *deleting traces* refers to data that is stored at the user's devices, such as cookies [16, 19, 54].

Summarizing, 141 protection behaviors were found and mapped to 38 distinct categories. The EIPPBM represents the relationships between these distinct categories. The model introduces several categories on four hierarchical levels. Each category is derived from a literature review based on a mapping of nomination or meanings. On the next page in Figure 3 the End-User Information Privacy Protection Behavior Model is presented.

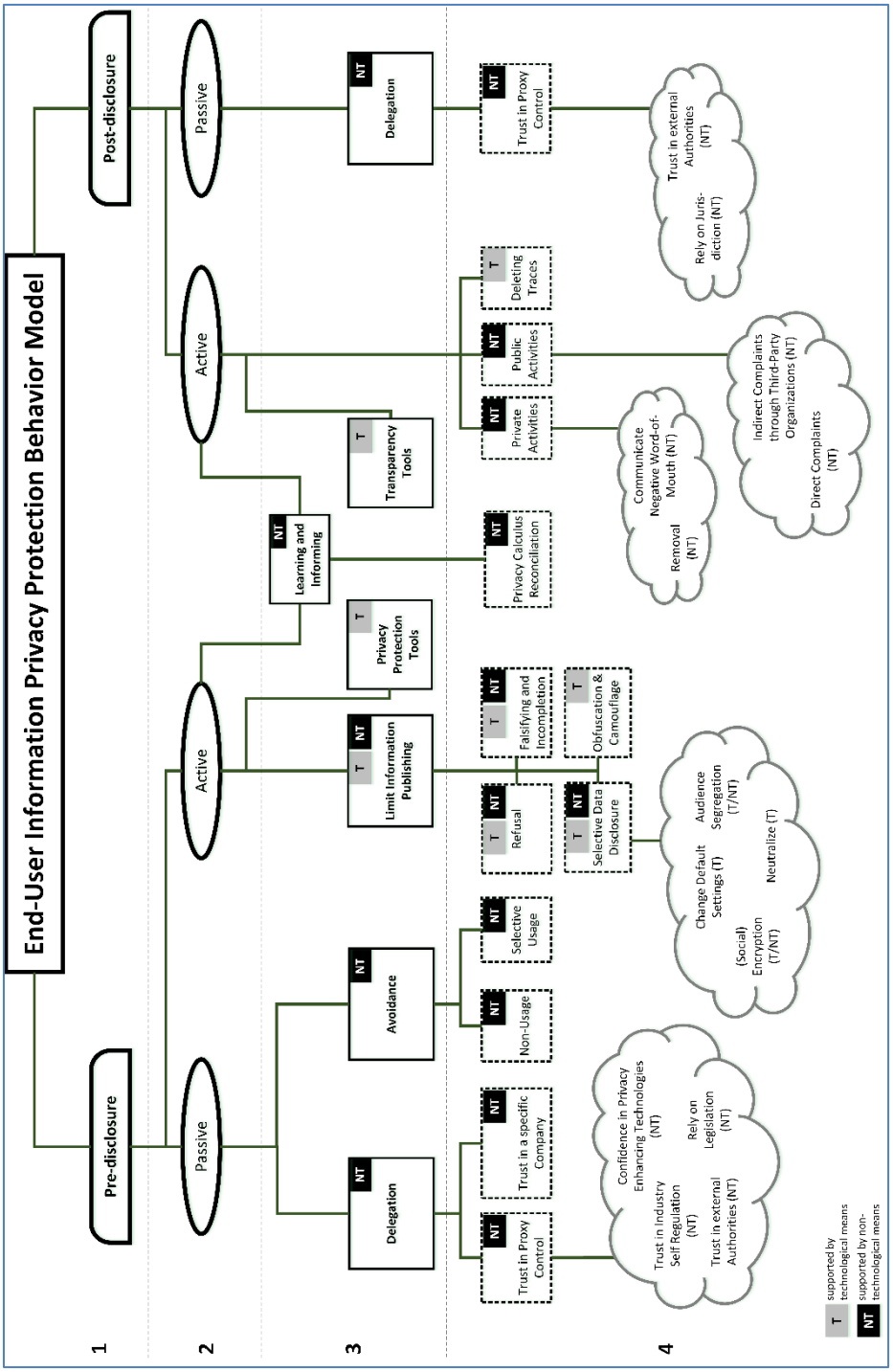

Figure 3 - End-User Information Privacy Protection Behavior Model

5 Discussion

Our models aims to create an overview of user-centric privacy protection behaviors. Although we also allude the term coping, we use "behavior", as it refers to a way of acting [25]. Whereas classifications in literature have only few categories, our model provides more categories covering a broader field of applicability, because privacy concerns "the Internet as a whole" [13]. In contrast, [17] mainly concentrated on privacy responses in electronic commerce or [29] distinguishes between "general caution" and "technical protection.
Although there is an ongoing debate about if individuals should be responsible for their data protection [19], our work purely concentrates on identifying protection behavior, without taking a position in this debate.

Nonetheless, it is not trivial or unambiguous to organize protection behaviors in a taxonomy or model, because categories could mean different things to people [26]. Whereas some authors label behaviors literally equal (e.g. fabricate [35, 38]), other scholars rely on own nominations (e.g. perturbation [55]). We tried to stick to generally recognized wordings. But sometimes there was a need to create own nominations which literature do not discuss throughout to cover the different authors' aspects (e.g. trust in proxy control). There are also some categories in literature, which did not fit into our model. For example Moshki and Barki say that coping can happen during "a stressful encounter" [14] and call this the "impact period". However, we argue that it is difficult to identify a privacy breach on the fly. Finally, sometimes authors' classifications are contradictory. For example Yap et al. [16] call withdraw as an active behavior, whereas Gurău and Ranchhod [22] consider it as passive. Furthermore we argue that the model can never be considered as complete. As technology is changing with high pace, new protective technologies and behaviors are likely to arise. Adding insights from further disciplines, such as sociology, might bring up other or new categories to the model.

5.1 Implications

Our work offers implications for theory, as well as for practice. For scholars this work offers an overview of current privacy protection behaviors of end-users and helps to understand the range of protection mechanisms [13, 16, 41]. Additionally, it shows which denominations authors use. Further it shows how behaviors could be linked to each other. As the model concentrates on a user-centric approach, it answers the call from [18]. The model is not fixed. Instead, it is highly adaptive. Researchers can edit, add or delete categories without losing the general meaning. In addition, the model is not fixed to a special domain, thus scholars can adopt the classifications to special fields of research.

For practice, our model helps end-users to identify tools and techniques to protect themselves, as users are often not aware how to safeguard their data [13, 41]. Further, data protection officers could use the insights for digital literacy programs. The fact that many protective behaviors can be applied without any technological literacy could encourage novice. However, at the current stage of research, this statement is theoretical and will need an evaluation. Additionally it could help freshmen to choose behaviors

that fit to their skills or specific situation. For example, they can distinguish on the very first level if they need advice before or after a data disclosure. Thus it serves as a guideline or manual. However, we have to mention that the usefulness and applicability of the model might depend on the individual user, its awareness and its threat perception. Moreover, users can show different behaviors simultaneously.

5.2 Limitations

Although we try to ensure a high quality of our work, there are some limitations. First to mention, our literature review has no claim to be collectively exhaustive. Some classification could be overlooked, others might be misinterpreted due to the bilingual keyword search. Interestingly very tech-savvy protective countermeasures, such as running own mail servers, did not come up in the literature review. One reason could be that it is considered more a security issues. Further, academics should not consider our classifications as mutually exclusive. Due to complexity reasons, we did not include the motivational factors or influences (such as emotions, cognitions and the characteristics of the environment [14]) on privacy protection. We excluded a consideration of the effectiveness of each behavior for two reasons. First, effectiveness depends on a specific situation and on technological advancements [18]. Second, behaviors appear together and their effects cannot be considered solely [15]. As we aim at an overview without implications or biases, we excluded an analysis of frequency of usage. Lastly we argue that some of our identified behaviors could be considered as coping strategies. E.g. rationalizing away privacy concerns trough delegation is rather a way of coping.

6 Conclusion and Future Work

Our work tried to create a comprehensive view on end-user privacy protection behaviors. To do so we conducted an iterative literature review and identified 141 protection behaviors. We mapped the results and came up with 38 distinct categories. By means of card sorting, we created the “End-User Information Privacy Protection Behavior Model”, which represents a taxonomy of behaviors. The work by [17] served as a basis for our model. Our four-level model distinguishes behaviors which users do before or after information disclosure. Further, it differentiates between active and passive behaviors. One central point is learning and information, which links pre- and post-disclosure behaviors. Furthermore, the EIPPBM indicates which behavior need technological or non- technological means. Our literature research has shown that a majority of behaviors can be done without any digital literacy.

Further work could evaluate the model in a representative user study, for example by using cart sorting with a large sample of users. In addition, users can be asked to assign specific protection practices to the proposed categories. It could be interesting to classify behaviors based on groups of privacy threats, as identified by [45] and [56]. Future work could consider involving a typology of users and show which users’ personality traits lead to a specific protection behavior. This could be accompanied by a

consideration of the effectiveness and applicability of each behavior. Lastly, we encourage scholars from different disciplines to edit our model by adding, deleting or rearranging categories.

Acknowledgement. This work is partially funded by the German Ministry of Education and Research within the project 'Forum Privacy and Self-determined Life in the Digital World', https://www.forum-privatheit.de.

7 References

1. Malekzadeh M, Clegg RG, Cavallaro A et al. (2018) Protecting Sensory Data against Sensitive Inferences. In: Maia F, Mercier H, Brito A (eds) Thirteenth EuroSys Conference 2018. ACM, New York, USA, pp 1–6
2. Crisler V, Richardson B, DiGerolamo J (2018) The State of IoT Security: It is time for action.
3. Acquisti A, Taylor C, Wagman L (2016) The Economics of Privacy. Journal of Economic Literature 54(2): 442–492. doi: 10.1257/jel.54.2.442
4. Tucker CE (2012) The economics of advertising and privacy. International Journal of Industrial Organization 30(3): 326–329. doi: 10.1016/j.ijindorg.2011.11.004
5. Barathi JJ, Kavitha G, Imran MM (2015) Building a Mobile Personalized Marketing system using multidimensional data. In: 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials: ICSTM : 6th-8th May 2015 : proceedings. IEEE, Piscataway, NJ, pp 133–137
6. Junglas IA, Johnson NA, Spitzmüller C (2008) Personality traits and concern for privacy: An empirical study in the context of location-based services. European Journal of Information Systems 17(4): 387–402. doi: 10.1057/ejis.2008.29
7. Belanger F, Xu H (2015) The role of information systems research in shaping the future of information privacy. Information Systems Journal 25(6): 573–578. doi: 10.1111/isj.12092
8. DIVSI (2018) Internetnutzung - Risikowahrnehmung unter Jugendlichen und jungen Erwachsenen in Deutschland 2018. https://de.statista.com/statistik/daten/studie/943840/umfrage/befuerchtete-risiken-der-internetnutzung-unter-jungen-menschen-in-deutschland/. Accessed 17 Jul 2019
9. Bennett CJ, Raab CD (2017) The Governance of Privacy: Policy Instruments in Global Perspective, 1st. Routledge
10. CIGI-Ipsos (2019) 2019 CIGI-Ipsos Global Survey on Internet Security and Trust. https://www.cigionline.org/internet-survey-2019. Accessed 23 Apr 2019
11. GPRA (2018) Datenschutz - Vertrauen in Internetunternehmen in Deutschland 2017. https://de.statista.com/statistik/daten/studie/790373/umfrage/vertrauen-in-den-datenschutz-von-internetunternehmen-in-deutschland/. Accessed 23 Sep 2019

12. Wambach T, Bräunlich K (2017) The Evolution of Third-Party Web Tracking. In: Camp O, Furnell S, Mori P (eds) Information Systems Security and Privacy, vol 691. Springer International Publishing, Cham, pp 130–147
13. Boerman SC, Kruikemeier S, Zuiderveen Borgesius FJ (2018) Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. Communication Research 25: 1-25. doi: 10.1177/0093650218800915
14. Moshki H, Barki H (2016) Coping with Information Privacy Breaches: An Exploratory Framework. In: Pär J. Ågerfalk, Natalia Levina, Sia Siew Kien (eds) Proceedings of the International Conference on Information Systems - Digital Innovation at the Crossroads, ICIS 2016, Dublin, Ireland, December 11-14, 2016. Association for Information Systems
15. Xu H, Teo H-H, Tan BCY et al. (2012) Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research 23(4): 1342–1363. doi: 10.1287/isre.1120.0416
16. Yap JE, Beverland MB, Bove LL (2012) "Doing Privacy": Consumers Search for Sovereignty through Privacy Management Practices. In: Scott LM, Belk RW, Askegaard S (eds) Research in consumer behavior. Emerald, Bingley, U.K
17. Son J-Y, Kim SS (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly 32(3): 503–529. doi: 10.2307/25148854
18. London Economics (2010) Study on the Economic Benefits of Privacy-enhancing Technologies (PETs): Final Report to The European Commission, DG Justice, Freedom and Security. London Economics
19. Matzner T, Masur PK, Ochs C et al. (2016) Do-It-Yourself Data Protection—Empowerment or Burden? In: Gutwirth S, Leenes R, Hert P de (eds) Data protection on the move: Current developments in ICT and privacy/data protection. Springer, Dordrecht, Heidelberg, New York, London, pp 277–305
20. Büchi M, Just N, Latzer M (2016) Caring is not enough: The importance of Internet skills for online privacy protection. Information, Communication & Society 20(8): 1261–1278. doi: 10.1080/1369118X.2016.1229001
21. Lampinen A, Lehtinen V, Lehmuskallio A et al. (2011) We're in it together: Interpersonal Management of Disclosure in Social Network Services. In: Tan D, Fitzpatrick G, Gutwin C et al. (eds) The 29th Annual CHI Conference on Human Factors in Computing Systems: Conference proceedings and extended abstracts. ACM, New York, NY, pp 3217–3226
22. Gurău C, Ranchhod A (2009) Consumer privacy issues in mobile commerce: A comparative study of British, French and Romanian consumers. Journal of Consumer Marketing 26(7): 496–507. doi: 10.1108/07363760911001556
23. Singh N, Singh AK (2018) Data Privacy Protection Mechanisms in Cloud. Data Science and Engineering 3(1): 24–39. doi: 10.1007/s41019-017-0046-0
24. Jiang X, Hong JI, Landay JA (2002) Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing. In: Borriello G, Holmquist LE (eds) UbiComp 2002: Ubiquitous Computing. Springer Berlin Heidelberg, pp 176–193
25. Heacock P (ed) (2009) Cambridge academic content dictionary, 1. ed. Cambridge Univ. Press, Cambridge

26. Smith H, Dinev T, Xu H (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35(4): 989–1015
27. Acquisti A, Brandimarte L, Loewenstein G (2015) Privacy and human behavior in the age of information. Science 347(6221): 509–514. doi: 10.1126/science.aaa1465
28. Baruh L, Secinti E, Cemalcilar Z (2017) Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal of Communication 67(1): 26–53. doi: 10.1111/jcom.12276
29. Buchanan T, Paine C, Joinson AN et al. (2007) Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology 58(2): 157–165. doi: 10.1002/asi.20459
30. Lwin MO, Wirtz J, Stanaland AJS (2016) The privacy dyad: Antecedents of promotion- and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern. Internet Research 26(4): 919–941. doi: 10.1108/IntR-05-2014-0134
31. Gurung A, Jain A (2012) Antecedents of Online Privacy Protection Behavior: Towards an Integrative Model. In: Chen K (ed) Cyber crime: Concepts, methodologies, tools and applications. IGI Global, Hershey, Pa, pp 69–82
32. Dolnicar S, Jordaan Y (2007) A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing. Journal of Advertising 36(2): 123–149. doi: 10.2753/JOA0091-3367360209
33. Li Y, Dai W, Ming Z et al. (2016) Privacy Protection for Preventing Data Over-Collection in Smart City. IEEE Trans. Comput. 65(5): 1339–1350. doi: 10.1109/TC.2015.2470247
34. Xu H, Dinev T, Smith J et al. (2011) Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems 12(12)
35. Youn S (2009) Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. Journal of Consumer Affairs 43(3): 389–418. doi: 10.1111/j.1745-6606.2009.01146.x
36. Anderson CL, Agarwal R (2010) Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. MIS Quarterly 34(3): 613–643
37. Fritsch L (2007) State of the art of Privacy-enhancing Technology (PET): Deliverable D2.1 of the PETweb project
38. Lwin M, Wirtz J, Williams JD (2007) Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science 35(4): 572–585. doi: 10.1007/s11747-006-0003-3
39. Metzger MJ (2007) Communication Privacy Management in Electronic Commerce. Journal of Computer-Mediated Communication 12(2): 335–361. doi: 10.1111/j.1083-6101.2007.00328.x
40. Ochs C, Büttner B, Hörster E (2018) Das Internet als »Sauerstoff« und »Bedrohung«: Privatheitspraktiken zwischen analoger und digital-vernetzter Subjektivierung. In: Friedewald M (ed) Privatheit und selbstbestimmtes Leben in der digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes. Springer Vieweg, Wiesbaden, pp 33–80

41. Bélanger F, Crossler RE (2011) Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly 35(4): 1017–1042
42. Vom Brocke J, Simons A, Riemer K et al. (2015) Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. CAIS 37. doi: 10.17705/1CAIS.03709
43. Benyon D (2014) Designing interactive systems: A comprehensive guide to HCI, UX and interaction design, 3. ed. Pearson, Harlow
44. Spencer D (2009) Card Sorting: Designing Usable Categories. Rosenfeld Media
45. Solove DJ (2006) A Taxonomy of Privacy. University of Pennsylvania Law Review 154(3): 477. doi: 10.2307/40041279
46. Folkman S, Moskowitz JT (2004) Coping: Pitfalls and Promise. Annual Review of Psychology 55(1): 745–774. doi: 10.1146/annurev.psych.55.090902.141456
47. Murmann P, Fischer-Hubner S (2017) Tools for Achieving Usable Ex Post Transparency: A Survey. IEEE Access 5: 22965–22991. doi: 10.1109/ACCESS.2017.2765539
48. ENISA (2016) Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. https://www.enisa.europa.eu/publications/pets. Accessed 14 Jun 2017
49. Teo HH, Wan W, Li L (2004) Volunteering personal information on the Internet: Effects of reputation, privacy initiatives, and reward on online consumer behavior. In: Sprague RH (ed) Proceedings of the 37th Annual Hawaii International Conference on System Sciences. IEEE Computer Society Press, Los Alamitos, Calif, 1-10
50. Bitkom (2018) Datenschutz - Vertrauen in Organisationen im Umgang mit persönlichen Daten in Deutschland. https://de.statista.com/statistik/daten/studie/936247/umfrage/vertrauen-in-organisationen-im-umgang-mit-persoenlichen-daten-in-deutschland/. Accessed 09 Jul 2019
51. Kung A, Kargl F, Suppan S et al. (2017) A Privacy Engineering Framework for the Internet of Things. In: Leenes R, van Brakel R, Gutwirth S (eds) Data Protection and Privacy. Springer International Publishing, Cham, pp 163–202
52. Brunton F, Nissenbaum H (2015) Obfuscation: A User's Guide for Privacy and Protest. MIT Press
53. ROLAND-Gruppe (2019) Roland Rechtsreport 2019. https://www.roland-rechtsschutz.de/unternehmen/presse_2/publikationen/publikationen.html. Accessed 16 Jul 2019
54. Statista (2017) Datenschutz - Maßnahmen in Deutschland 2017. https://de.statista.com/statistik/daten/studie/712775/umfrage/massnahmen-zum-datenschutz-in-deutschland/. Accessed 10 Jul 2019
55. Shin KG, Ju X, Chen Z et al. (2012) Privacy protection for users of location-based services. IEEE Wireless Commun. 19(1): 30–39. doi: 10.1109/MWC.2012.6155874
56. Kasper DVS (2005) The Evolution (or Devolution) of Privacy. Sociological Forum 20(1): 69–92. doi: 10.1007/s11206-005-1898-z