Computers in Human Behavior Reports 2 (2020) 100034

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.journals.elsevier.com/computers-in-human-behavior-reports

Identifying the values associated with users' behavior towards anonymity tools through means-end analysis

Andreas Skalkos [a,*], Aggeliki Tsohou [b], Maria Karyda [a], Spyros Kokolakis [a]

[a] University of the Aegean, Samos, Greece
[b] Ionian University, Corfu, Greece

ARTICLE INFO

Keywords:
PETs
Anonymity tools
Means-end analysis
Laddering interview
Values

ABSTRACT

Concerns about privacy and frustration over censorship and content blocking urge a great number of users to use privacy enhancing products. This research focuses on anonymity tools, as a Privacy Enhancing Technology (PET), investigating the human values associated with users' behavior towards them. We use means-end analysis, a methodology we consider to be appropriate for investigating users' conceptions and incentives that determine acceptance and use of anonymity tools. In this context we use the laddering technique, a qualitative method based on in-depth interviews, to identify the chains of attribute-consequence-value of anonymity tools users and to construct a Hierarchical Value Map. The results show that freedom, personal privacy, economic prosperity, professional development and fear-free living are the core values users achieve as a result of anonymity tools use. The aim of our research is to provide insights and enhance understanding of anonymity tools users' behavior, which we expect to benefit both researchers and software engineers to design more effective tools.

1. Introduction

Privacy is recognized as a fundamental human right (Warren & Brandeis, 1890). The concept of privacy involves social, cultural, legal, economic, political and technical aspects (Wang, 2009, pp. 203–227). Clarke (1999) identifies four features of privacy: personal communication privacy, privacy of a person, personal data privacy and personal behavior privacy. Nowadays, due to the digitization of communications and data archiving, data privacy and personal communication privacy can be consolidated within the notion of information privacy. Therefore, information privacy can be considered as a subset of the comprehensive notion of privacy.

Privacy issues have drawn considerable attention in society, as a result of the rapid spread and progress of novel information technologies, such as the Internet, mobile computing, and ubiquitous computing (Wang, 2009, pp. 203–227). The adoption of the General Data Protection Regulation (GDPR) (EU General Data Protection Regulation, 2016) and the ePrivacy Directive (Directive 2002/58/EC, 2002) by the European Union indicates the importance society places on information privacy in our era. Acquisti et al. (2015) argue that "*if this is the age of information, then information privacy is the issue of our times. Activities that were once private or shared with the few now leave trails of data that expose our interests, traits, beliefs, and intentions*".

In response to the challenge of protecting Internet users' privacy, researchers in the field, as well as software industries, have developed various tools and technologies known as Privacy Enhancing Technologies (PETs) (Enisa, 2016). PETs refer to a wide range of technologies and tools that can assist users to protect their information privacy. Recent studies show that the adoption of PETs is limited. Vemou et al. (2015) conducted an empirical study and found that most of the participants in their study were not familiar with any of the PETs discussed. On the other hand, The Guardian (2014) reports that 28% of the online population surveyed by Global Web Index stated that they are using tools to disguise their identity or location.

One of the reasons why the adoption and use of PETs is challenging, according to Vemou et al. (2015), is that users seem to ignore, or underestimate, the privacy implications of permissions given to third party applications. On the other hand, Benenson et al. (2015) argue that privacy awareness is high and emphasize that perceived ease of use determines the intention to use PETs. Another factor that may affect the adoption and use of PETs is their cost. Acquisti (2004) argues that while the real cost of using PETs is low when adopted, their adoption involves significant switching costs. Thus, research findings pertaining to the adoption of PETs are contradictory and indicate that there are

* Corresponding author.
E-mail addresses: ask@aegean.gr (A. Skalkos), atsohou@ionio.gr (A. Tsohou), mka@aegean.gr (M. Karyda), sak@aegean.gr (S. Kokolakis).

https://doi.org/10.1016/j.chbr.2020.100034
Received 11 April 2020; Received in revised form 6 October 2020; Accepted 22 October 2020
Available online xxxx

unexplored factors influencing users' decisions to use or reject using such protective mechanisms.

Some of the most popular PETs are anonymous proxy servers and onion routing networks. *Anonymous proxies* enable Internet users to browse the web anonymously by hiding the IP address and other user-related information. Anonymous proxies are provided by either commercial companies, which may request subscription fees, or nonprofit organizations (e.g., hide-my-ip.com, proxysite.com, kproxy.com). *Onion routing* is based on the concept of "mix network" (Chaum, 1983). A mix network is a sequence of proxy servers, called *mixes*. In onion routing, a layer of encryption corresponding to each mix node is added to the message. The resulting encryption is layered like an "onion" and the original message is hidden in the internal layer. As the message traverses through the network, every mix node peels its own encoding layer to see where to send the message after. Based on this method onion routing achieves untraceability, unless all mix nodes are compromised (Wang, 2009, pp. 203–227). Nowadays, The Onion Router (TOR) is the most popular anonymous communication system based on onion routing technology.

This research has been motivated by the following research question: *What are the values associated with users' behavior towards anonymity tools?* We assert that Internet users' decision to use an anonymity tool is influenced not only by the attributes and functionalities of the tool itself, but as well by personal needs fulfilment, social influence elements, and personal values. On this basis, we investigate the psychological procedures related to anonymity tools use and reveal the underlying values that drive people's anonymity-related decisions and behavior. Specifically, the objective of this research is to investigate which human values are associated with users' behavior towards anonymity technologies. To achieve this, we drew on the means-end theory and applied the laddering interview technique (Gutman, 1982) as our research method.

In the following, the paper provides a critical analysis of relevant literature, describes our research approach, and presents and discusses our findings.

2. Related work: adoption of privacy enhancing tools

Although the concept of PETs was introduced in 1995 (van Rossum et al., 1995), PETs are still considered as a technological innovation (Bagozzi & Dholakia, 1999). Xiao et al. (2014) attribute this to the fact that security tools are what Rogers (2010) calls a *preventive innovation*. Preventive innovations are technologies that reduce the risk of some undesired future events, e.g. vaccines. Preventive innovations diffuse slowly due to the time gap existing between their usage and the impacts they bring upon. Thus, PETs, considered as preventive innovations, are expected to have a slow adoption pace. Additionally, as Kokolakis (2017) pointed out, individuals are optimistic when considering a potential online privacy breach which in turn affects negatively the adoption of privacy protective behaviors. The so-called optimism bias prevents individuals from defending themselves against a privacy violation, and thus makes them less prone to use PETs. Another reason for the slow adoption of PETs can be attributed to the lack of awareness. Pavone and Pereira (2009) argues that the most important issue regarding the adoption of PETs is the inadequate comprehension of privacy risks. Due to the lack of privacy risks awareness, the demand for PETs is poor and thus there is no powerful driving force for the advancement of privacy technologies. Moreover, the fact that most Internet users have not faced the implications of losing their privacy leads to a limited understanding of its significance (META Group, 2005).

In contrast, Vemou and Karyda (2013) argued that the significance of awareness is somewhat overestimated, as many consumers are aware of specific PETs, but are still not using them. Often, individuals underestimate the hazards related to information disclosure and thus they unveil too much personal data. This behavior is partly explained by the weak connection between actions (the revealing of personal data) and consequences (e.g., fraud, profiling, identity theft, etc.). This lack of feedback also inhibits individuals from becoming cautious about their privacy (London Economics, 2010). In addition, behavioural economics research has identified various cognitive biases that may explain this phenomenon.

In various circumstances, the average user accepts losing control over his own private data. An example of this might be patients who give access of their medical records to their doctor. Another example is the acceptance of video monitoring, personal search or other privacy violations to diminish the risk of terrorist attacks. Therefore, privacy requirements are always balanced with other more significant demands (META Group, 2005).

Previous research has also found that privacy concerns can have a negative effect on the adoption of Web-based applications (Malhotra et al., 2004) and therefore these concerns are a main threat to the Internet economy. The Eurobarometer survey on Europeans' attitudes towards cyber security (European Commission, 2015) found that the most important issues of Internet users remain the misuse of private information and the safety of online payments. Nearly half (45%) of respondents are concerned about the risk of misuse of their data by a third party. The percentage of those concerned has significantly increased since 2013, when this view was retained by less than four out of ten (37%) (European Commission, 2015).

Harborth et al. (2017) pointed out that despite a growing public awareness of the need for data protection, anonymization services have not yet achieved "wide everyday and mass appeal". As a result, they argue that most Internet users today leave digital traces that can be used by Internet Service Providers (ISP) or third parties to construct comprehensive profiles without the user's awareness.

Smith et al. (1996) associated personal values with concerns about information privacy by noting the connection between information privacy concerns of individuals and their level of trust, distrust and social criticism. What causes people to worry about something in life can be clarified by the importance they attach to it based on their own personal values. Values are illustrated as "*trans*-situational goals which differ in importance as guiding principles in a person's or group's life" (Schwartz et al., 2012, p. 664). Values can be perceived as "what matters to us in life" (Schwartz, 2012, p. 3), and what guides an individual in pursuing a goal is the trade-off between related and competitive values (Schwartz, 2012). Hup (2017) explains that key values of privacy are of utmost significance as a motivating factor for PET adoption and diffusion. In this paper we extend this stream of research by identifying the human values that drive users to adopt and use anonymity tools.

Conclusively, though related research indicates that privacy protection behavior is shaped, among others, by personal values and beliefs, the relationship between personal values and privacy protection remains largely unknown and understudied. Moreover, empirical research on how and why people dismiss or obtain various protective measures is rare (Cho et al., 2009). Therefore, this paper aims to bridge this gap, by identifying how personal and social values shape privacy behavior.

3. Theoretical background: means-end theory and the laddering technique

3.1. Means-end theory

The means-end chain analysis model has as focal point the connection among product's or service's *attributes*, *consequences* and *values* (Gutman, 1982) and illustrates the way the use of a product or a service facilitates the individual's understanding of his/hers ends needs. Attributes are connected to product or service features and consequences are specified as the psychological or physiological outcomes obtained directly or indirectly by the consumer from product or service usage. The core feature of this approach is that "… consumers choose actions that produce desired consequences and minimize undesirable consequences" (Reynolds & Gutman, 1988). The model of Gutman has two fundamental assumptions: (a) values are associated with consequences, as far as the connotations of consequences are positive or negative, and (b) consequences have a direct connection with the characteristics of the product since the users acquire the product that can lead to the anticipated outcomes (Gutman, 1982). The means-end chain is a model that seeks to clarify how the choice of products or services makes it easier to achieve the required end states (Gutman, 1982). The means-end theory conceptually considers users to be goal-driven decision makers who choose behavior that will probably lead to desired results (Bagozzi & Dabholkar, 1994). Users' perceptions of the attributes of the product contain different degrees of abstraction. These degrees of abstraction are attributes, consequences and values, which are hierarchically related (Reynolds & Olson, 2001). A hierarchical goal system is a system that provides the motivational basis to determine what is the goal of a user (Bagozzi & Dholakia, 1999). Therefore, we investigate the association between the values of a user and a set of product's attributes (Pieters et al., 1995).

In the context of the means-end theory consumers select actions that generate desirable consequences and/or reduce unwanted ones. Thus, consumers learn to combine tangible implications with product attributes. This knowledge facilitates consumers to select products that have the respective attributes and enable them to achieve their desired purpose. A major hypothesis of the means-end theory is that consumers' product or service understanding exhibits a hierarchical order, with solid thoughts connected to more abstract thoughts in a chain that advances from means to end. Hence, the more solid features of a product or service, the *attributes* (A), are linked to notional concepts about social or psychological *consequences* (C) of the attributes. These socio-psychological consequences or advantages emerging from product use are successively associated to the utmost abstract component, the *values* (V).

3.2. Laddering technique

The laddering technique is the approach employed to disclose the means-end structure (Reynolds & Gutman, 1988). Its goal is to recognize the characteristics of a specific product which offer preference to a certain class of products, where product class is defined as a class of products that provides a substitute for another category. The attributes of services or products and the consequences relate to their use are the "means". The "ends" are the results articulated regarding the consumer's personal values (Reynolds & Gutman, 1988). The term ladder is assigned to the connection among *attributes*, *consequences* and *values*. It is a conceptual representation of the relationship between the product and the mental process of the consumer that drives to a direct and helpful knowledge of his/her perception regarding the product or service. Laddering involves an in-depth individual interview seeking to understand the choices of the individual. It translates product attributes into relations appropriate to individual's "self" (Reynolds & Gutman, 1988).

Typically, in the laddering interview the interviewee is at start encouraged to recognize notable attributes of a certain product class, often initiated by asking for distinctive choice alternatives between instances of a product class. After this initial attribute extraction phase, the interviewer attempts to disclose the product attribute which the interviewee associates with a ladder, by asking: "Why is this attribute important to you?". This question also aims to challenge the interviewee to understand what motivates his/her attribute selection by describing the anticipated and favored related consequences. (Vanden Abeele et al., 2012). Therefore, the laddering technique can provide a valuable tool for understanding behavior (Veludo-de-Oliveira et al., 2006).

Recent studies have employed means-end analysis to explore users' behavior in various domains, such as online document management systems (Chiu, 2005), online shopping (Lin & Wang, 2008), Second Life (Jung & Kang, 2010), e-learning systems (Sun et al., 2009), mobile service usages (Mcmanus, 2009), and social networking sites (Pai and Arnott, 2012). Due to the similarity of these online contexts with the use of anonymity tools, laddering can be considered appropriate for investigating users' incentives for adopting anonymity tools. In addition, the laddering interview technique is a flexible method. Using open-ended questions, interviewees are unrestricted to respond in their own way and these responses tend to be more detailed than just simply "yes" or "no." Participants have the convenience to reply more sophisticated and in greater detail. In turn, researchers also have the chance to react to what the respondents say instantly by customizing sequential questions.

Further to the above, taking into consideration that means-end chain is a model that aims to clarify how the choice of product or service facilitates the accomplishment of desired end states (Gutman, 1982), it can be applied to the investigation of anonymity tools use.

4. Research method

4.1. Sampling

Basic threshold for laddering interviews is considered to be 20 respondents (Pai & Arnott, 2013; Reynolds, Dethloff, & Westberg, 2001; Saaka et al., 2004). In this research, we interviewed twenty-seven participants, which ensures the sample size is sufficient for an exploratory research that provides insight into the key attributes, consequences, and values relating to anonymity tools use. Due to the exploratory character of our research, the only essential prerequisite for sampling was that participants had used anonymity tools before. Participants were selected randomly, and the sample consisted of Greek Internet users. Male respondents dominated the sample (n = 24). 93% of the sample were aged between 25 and 54 years old, and 85% were university graduates while 85% of them stated that were employees.

The interviews were conducted in the Greek language. Sample demographics are presented in the Appendix (Table 1).

4.2. Data collection

According to Reynolds and Gutman (1988), it is important to select a relaxed location without distractions for the participants for laddering interviews. We conducted the interviews via a popular video conferencing application and ensured the participation of two of the authors in all of them, one having the role of interviewer the other the role of the observer. The researchers introduced the background of the research to the participants and requested their permission to record the interview. All participants agreed to recording. The interviews had an average duration of 30 min, ranging between 18:13 min and 43:04 min.

The interviewer described the scope and objective of the research to the respondent and informed him/her that there is no "right-wrong answer". This clarification is critical in the laddering technique due to the personal essence of the investigating process, which creates a slight sense of vulnerability on the part of the interviewee. Stating there is no "right-wrong answer" allows the interviewer to help the respondent realize that the interviewer is simply a qualified coordinator of this discovery process and not a judge or evaluator of the respondent's ideas. We informed the respondents that many of the questions might seem "slightly apparent and perhaps even dumb", this predicament is therefore associated with the interview method and creates the impression that the interviewer is just a coordinator following certain guidelines.

Preference differences device was used for eliciting distinctions between onion routing networks and anonymous proxy servers. Respondents were asked to classify their preferences and to explain why one is better than the other.

In order to lead the discussion into revealing the means-end hierarchy, we also emphasized on the question "why is that important to you?"

Indicative, we present some questions and responses from the pilot interview we conducted, and the way attributes, consequences and values are generated:

Q: "When and how did you first use an anonymity tool?"

A: "Friends introduced them to me, few years ago."

Q: "Which one was the most interesting attribute of the tool that you used?"

*A: "The fact that I could browse anonymously." (**Attribute**).*
Q: "Why is it important to you to browse anonymously?"
*A: "Because I want to have access to banned websites". (**Consequence**).*
Q: "Why is it important to you to have access to those websites?"
*A: "Because I want to feel free." (**Value**).*

4.3. Data analysis

Following the laddering technique guidelines provided in Grunert, Beckmann, and Sørensen (2000), data from each interview was independently analysed by two of the researchers; one of them had participated in the interview and the other had not. Both researchers listened to the recorded interview independently, performed data coding and constructed the A-C-V ladders. Coding results were then compared and discussed by the whole research team to produce the final coding.

The researchers established for each interview the extent of convergence by the two codings. If the extent of convergence was high, then the two or more sets of codes were merged into a combined set (e.g., respondents references to economic survival, personal growth, income, and price discrimination overcoming were merged into the code economic *prosperity*). If there were significant differences between the two codings, the researchers discussed further to develop a more robust set of codes. The comparison process revealed that during the independent construction of the two codings by the two participating researchers there were cases in which the same attributes, consequences, or values, were expressed by the coders with different terms. In those cases, the research team discussed and consolidated the wording accordingly.

Following this, the researchers constructed the Hierarchical Value Map (HVM), which provides a way of illustrating laddering data. HVM was produced by using aggregate data to depict "chains". Chains refer to sequences of attributes, consequences, and values. A common approach towards creating an HVM is to assign a "cut off", i.e. a least possible number of links that must be provided before one considers that item to be included in the HVM. Multiple cut-offs should be tested, to allow the researcher to choose the one with the most information and the most stable relationships (Saaka et al., 2004). After we tested multiple cut-offs, we chose a cut-off that provided us with the most information and the most stable set of relations. Pieters et al. (1995, p. 239) stated that a cut-off point is acceptable when the maps represent 60–70 percent of all relationships. Cut-off level 2 had the highest concentration index (the percentage of all links to cells) in our study and was calculated 81,28%.

Finally, in order to analyse the data and produce the HVM, we used LadderUX,[1] which is a tool designed for the quantitative analysis of laddering data and is particularly useful in the generation of HVMs. The tool is designed to help researchers register laddering data in a simple and efficient manner. It is considered a powerful tool for the data analysis and it provides a compelling designed HVM as output.

5. Research results

5.1. Content codes

All interview data were examined for sentences or words that reveal respondents' attributes, consequences, and values. We demonstrate 8 examples of phrases that participants used in favour of readability and comprehensibility. For example, participant 18 stated:

> "I like to use anonymity tools the reverse way. Not to keep my anonymity, but to hide my IP address in order to overcome company policies so I could visit useful for me banned sites thus I could get knowledge in order to develop my skills"

was coded as a "hiding IP" attribute of the tool. Consequently, the respondent in the above quote pointed out the consequence "Access to banned sites" of this attribute by saying " ....so, I could visit useful banned sites ....", and finally " ......thus I could get knowledge in order to develop my skills" which clearly refer to "professional development" value.

In another interview, participant 14 answered:

> "I just needed to visit a site that is restricted in my country to retrieve some e-books. I needed the knowledge to do my course assignment"

was coded as "hiding IP" attributed also. The consequence was the "access to banned websites" and the value was recognized as "professional development".

Another example is the participant 23 who reported:

> "By using anonymity tools, the advantage is that I can browse anonymously. I do not want to allow anyone to create a personal profile of myself so that information about my personal interests can be leaked. These are clearly personal data that I want to protect"

In this example, we identify "anonymous browsing" as attribute. The related consequence that was identified was "avoid profiling" and the associated value was "privacy".

Another example refers to participant 12 who stated:

> " I use an anonymity tool to hide my IP so that I can investigate the market as a foreigner in my country. This helped me to get better rates for goods and services"

was coded as "hiding ip" attribute. The consequence was identified as "avoiding geoblocking" which leads to the value "economic prosperity".

Participant 22 stated that

> " I want to keep my anonymity in order not to fear when I visit spicy web sites"

was coded as "anonymity" attribute. The related consequence that was identified as "hiding online activities" which leads to "fear-free living".

Also, participant 17 who stated:

> "I wanted to keep my anonymity by avoiding web sites to keep my tracks so I could protect my privacy".

was coded as "anonymity" attribute. The related consequence that was identified as "web surveillance protection" and the associated value was "privacy".

In another interview, participant 25 stated:

> "I use anonymity tools in order to protect my anonymity regarding confidential information, such as VAT number, social security number, car plate, data that will stress me if a third party could take possession of them."

was coded as "anonymity" attribute. The related consequence that was identified as "Protection of sensitive data" and the associated value was "fear-free living".

participant 25 stated:

> " I used the tool few times, but I find it really slow for me and caused me lack of usability, while we live in an era that life is fast paced"

was coded as "delay" attribute. The related consequence that was identified as "reduced connection speed" and the associated value was "living a fast paced life".

The coding process identified 14 distinct attributes (Appendix, Table 2), 50 consequences (Appendix, Table 3) and 31 values (Appendix, Table 4). Overall sampling sequence assessment revealed 91 ladders (Appendix, Table 5). The resulting data were then entered into LadderUX, in order to produce the implication matrix and the Hierarchical Value Map (HVM).

[1] See http://ladderux.org/.

5.2. Hierarchical Value Map

One critical issue in the construction of an HVM is the choice of a cut-off value. This cut-off point differs depending on the number of participants and chains. Reynolds and Gutman (1988) propose the use of a four immediate associations cut-off with 50 participants, while other researchers (e.g., Subramony (2002)) propose the use of two direct relationships with less (20–30) participants. After testing various cut-off values, we have chosen a cut-off of two direct relationships, as the resulting map maintains the balance between data reduction and retention (Gengler et al., 1995). This is also consistent with the aforementioned literature recommendations, since our respondents were 27.

After the cut-off at the HVM we obtained the following elements (the number in parenthesis indicates the number of instances):

1. Four (4) *attributes*:
   1.1. Anonymity (25)
   1.2. Anonymous Internet browsing (36)
   1.3. Hiding IP (7)
   1.4. Delay (9)
2. Twelve (12) *consequences*:
   2.1. Reduces ads (7)
   2.2. Workplace network surveillance protection (5)
   2.3. Web surveillance protection (8)
   2.4. Hiding browsing history (6)
   2.5. Access to banned websites (8)
   2.6. Hiding online activities (11)
   2.7. Avoiding profiling (6)
   2.8. Access to knowledge (2)
   2.9. Avoiding legal consequences (2)
   2.10 Reduced connection speed (6)
   2.11 Protection of sensitive data (2)
   2.12 Avoiding location tracking (2)

   Twelve (12) *values*:

2.13 Economic Prosperity (14)
2.14 Fear-free living (5)
2.15 Privacy (25)
2.16 Freedom (7)
2.17 Personal success (3)
2.18 Professional development (12).
2.19 Security (5)
3.10 Personal dignity (2)
3.11 Self-control (3)
3.12 Pleasure (2)
3.13 Avoiding frustration (4)
3.14 Reassurance (2)

The respondents valued mostly four attributes an anonymity tool should provide: anonymity, anonymous Internet browsing, hiding IP, and delay. Although the three attributes seem almost identical, the respondents associated them with different consequences, thus they gave a different meaning to each one. In terms of consequences that result from the use of an anonymity tool, the responders gave prominence to the following twelve ones: reduces ads, workplace network, web surveillance protection, hiding browsing history, access to banned websites, hiding online activities, avoiding profiling, access to knowledge, avoid legal consequences, reduced connection speed, protection of sensitive data and avoiding location tracking. Of these consequences, hiding online activities was most valued by the responders, demonstrating the need of users in privacy. Also, among the most valued consequence by responders was web surveillance protection, revealing the importance of avoiding the fear of a growing surveillance society. Concerning values, privacy, economic prosperity, professional development, freedom, fear-free living and personal success were the most significant values.

As a result, 285 distinct data points were defined, which translated into 89 distinct ladders with an average of 3.03 elements per ladder and 3.48 ladders per respondent.

Appendix (Fig. 1) presents the final HVM that summarizes the most important attributes, consequences, and values and how they relate to each other. Among the most prevalent ladders we found to be the ones stemming from the attribute's "anonymity" or "anonymous web browsing" and were connected to the consequence "hiding online activities", which was then connected to the value "privacy". This agrees with the findings of the literature on the adoption of PETs (META Group, 2005) that argues that Internet users need to understand the value of privacy and the risks involved in Internet activity.

5.2.1. 2: Anonymity

The attribute "anonymity" has strong connection with the value "fear-free living". Aligned with this finding Chiang and Tang (2020) found that the behavior of the user is dictated by whether the user experiences fear and the more fearful the user is, the less likely the user is to demonstrate high-risk behavior. According to our finding's users try to overcome this fear by using PETs. Furthermore, Kambourakis (2014) argue that the need to be anonymous is a very important issue because it includes the basis for the protection of fundamental human rights, such as the free expression of ideas and opinions, and allow people to perform their online activities in comfort and privacy.

Additionally, "anonymity" has likewise connections with the value "economic prosperity". Weitzner (2018) further demonstrates this point in his research suggesting that the economic growth of the Internet, and the ecosystem around it, relies on the continued development of the Internet as a work in progress to overcome challenges such as the extensive collection of personal data and outstanding analytical tools that place personal privacy at risk.

Our findings also indicate that users adopt anonymity tools to gain the consequence of hiding browsing history, seeking to protect themselves against potential future misuse of their data. This is aligned with Xiao et al. (2014) who argues that security tools are what Rogers (2010) calls a preventive innovation.

5.2.2. Anonymous Internet browsing

Anonymous internet browsing in our study is strongly connected with the value of privacy through the consequence of "reduces ads" and "workplace network surveillance protection" and enhances the findings of Loshin (2013) who suggests that there are several good reasons to remain private, mostly to avoid unwanted attention to your preferences, whether that attention induces itself in infinite ads targeted to you on the basis of your internet searches, or to prevent unnecessary attention from network administrators to monitor traffic for "prohibited" content.

5.2.3. Hiding IP

There are grounds for concern about the privacy of an IP address. The Internet Service Provider (ISP) may link its addresses to the account owner paying for it and thus information that can be retrieved for a variety of jurisdictional reasons. In addition, if an IP address is augmented with metadata, the true identity of a user can be uncovered—for example using geo-location (Clark et al., 2007), In our study the attribute "hiding IP" is connected with the consequence "access to banned websites" which leads to the end value of "professional development" and "pleasure".

5.2.4. Delay

Taylor et al. (2015) argue that system response delays are a reliable source of user frustration. This is aligned with our study in which we found that the attribute of "delay" is connected with "reduced connecting speed" which leads to the value of "avoiding frustration" for the users of PETs.

We have to point out a common set of relationships linking both the attributes "hiding IP" and "anonymous web browsing" with the consequence of having "access to banned sites". This consequence seems to be important because, as responders stated, it helps them to achieve their “professional development”.

6. Implications

This research identifies the human values associated with users' behavior towards anonymity tools. Additionally, this exploratory study is expected to deepen our insights and understanding of users' behavior concerning anonymity tools and results in benefits for both researchers and software developers. We provide insights to this issue by creating a Hierarchical Value Map of attribute-consequence-value chains for the adoption of anonymity tools and by providing a comprehensive analysis of the laddering data. Our research also displays the capacity of the means-end approach for studying the use of software tools.

This study identifies the drivers behind users' behavior on anonymity tools and thus informs PETs providers on how to design more user-acceptable tools, since they will be closer to their functionality needs and their personal values. Furthermore, our study reveals the relevance of social aspects as a core feature of using PETs, as we illustrate the relationship between anonymity with values such as fear-free living, personal dignity, freedom, economic prosperity.

6.1. Theoretical contributions

Our study provides several theoretical contributions adding to or supporting the current knowledge. Graf et al. (2015) suggests that relaying solely on developers to imagine what the needs of users are may not be sufficient, as the mental models of system developers and the mental models of users are hardly the same. The contribution of this research, which offers theoretical aspects, may therefore be useful for the development of mental models that are closest to reality.

We contribute to existing knowledge by revealing the role of the value of economic prosperity, which was found as crucial for the Internet users' decision to adopt anonymity tools. Another significant value that is associated with the users' behavior towards anonymity tools is the users' professional development, which they gain through various consequences of anonymity tools. This aligns with the arguments of Dudin et al. (2017) that professional progress conditions impact staff development efficiency and return on the resources invested and time. Due to privacy policies many companies restrict employees' access to social networks, news sites, software development and security hacking sites, and others. It was also mentioned that some websites are banned at a national/governmental level. However, the respondents stated that many times they seek their professional development via access to those banned sites. This points out that companies and governments may need to consider reforming their information access policies and loosening the rules on banned sites that employees/citizens think they can offer significant knowledge to them, without of course violating copyright privileges. Another important finding of our research is that the fear users feel about web surveillance (either in their work surroundings or in their personal life) may lead to the adoption of anonymity tools.

6.2. Practical implications

Our results help providers of anonymity tools to design PETs that better fit users' needs. Moreover, our results confirm conclusions of previous research, that some so-called PETs serve well in order to curb the development of technological surveillance and encourage its use where necessary (Lyon, 2001). The findings of our study also indicate that users adopt anonymity tools to gain the consequence of hiding browsing history, seeking to protect themselves against potential future misuse of their data. This is aligned with Xiao et al. (2014) who argues that security tools are what Rogers (2010) calls a preventive innovation. In addition, our findings demonstrate the importance of the value of freedom and that respondents adopt anonymity tools to hide browsing history and avoid web surveillance and legal consequences, in order to "feel free”. This supports a privacy by design principle, which requires that personal data, and their interconnections, should be hidden from plain sight (Hoepman, 2014). Nowadays, a debate on how to choose the right PET is emerging (Harborth et al., 2020; Namara et al., 2020; Srouji & Mechler, 2020). Our study contributes in this debate by clarifying the users' values towards PETs. In parallel, our study provides knowledge to the need of developing new PETs or improving the effectiveness of existing ones, as the Office of the Privacy Commissioner of Canada (2017) argues is needed. Also, Angulo (2015) suggests that a new approach is needed in which people are consider not only as consumers of privacy and security technologies but also as distributors of sources of inspiration and ideas for the development of functional PETs that meet their real needs and concerns for privacy.

6.3. Limitations

The findings of this study although it has useful insights about users' behavior towards anonymity tools, they must be seen in light of some limitations. First, since the anonymity tools aren't yet adopted in wide range in society as Abeele and Zaman (2009) argue the means-end chains that are revealed in the context of digital products are different from means-end chains that consumer researchers will find out about well-established consumer products. .

Secondly, the core principle of means-end approach is that people are rational individual decision-makers who select such way to act (e.g. using anonymity tools) that is most likely to accomplish the desired results. This assumption has two obvious flaws: first, it is overoptimizing about the rationality of choice. This could cause bias since Van den Steen (2004) argues that an agent who attempts to choose the action that he perceives most probable to succeed is more likely to choose an action of which he/she overestimated the probability of success, rather than an action that underestimated the probability of success. Second, emotions are underestimated in the decision-making process despite the fact that Zeelenberg et al. (2008) stated that emotions' importance is apparent in the fact that decision-making is always an emotional process itself.

Another limitation is that a potential selection bias exists in our sample, since we had limited capacity to gain access to the necessary type or geographical spread of participants. Besides these limitations, our study still contributes to theory and practice as we discussed above.

6.4. Further research

Future research can be focused on predicting the role of determinant factors of anonymity tools' adoption. Because of the exploratory nature of this research we limit our objectives in gaining deeper insights and understanding of the values that are associated with users' behavior towards anonymity tools. Furthermore, a means-end analysis research at both government organizations and corporations' behavior towards the PETs is needed. This is particularly significand nowadays since many people bringing work home, due to the covid-19 health crisis, and can hold organizational data on their home computers and mobile devices, exposing these data at risk of a security breach with significant impact.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

Table 1
Sample demographics.

Criterion	Description	Number of participants
Gender	Male	23
	Female	4
Age	18–24	2
	25–34	15
	35–44	9
	45–54	1
Education	Undergraduate	4
	Graduate	12
	postgraduate	11
Employment	Student	4
	Employees	23

Table 2
Attributes.

Attributes	
1: Anonymity	7: Anonymous Internet browsing
2: Protecting e-transaction	8: Delay
3: Open source	9: Not the same as a regular browser
4: Portability	10: Cost
5: Bypassing web access restrictions	11: Friendly user interface
6: Hiding IP	12: Freeware

Table 3
Consequences.

Consequences	
13: Reduces ads	32: Assurance the tool works
14: Reduce Fraud risk	33: Hiding online activities
15: Workplace network surveillance protection	34: Financial transaction protection
16: Web surveillance protection	35: Protection of spyware
17: Using the same tool in all my devices	36: Enables Configuration and development
18: Avoiding untrustworthy providers	37: Online availability
19: Avoiding legal consequences	38: Avoiding location tracking
20: Avoiding Trouble at work	39: Reduced connection speed
21: Hiding browsing history	40: Avoiding profiling
22: Playing games	41: Disability to use
23: Secure online transactions	42: Ability to search
24: Avoiding price discrimination	43: Access to knowledge
25: Avoid redirection to unacceptable content	44: Avoiding geoblocking
26: Protection of sensitive data	45: Search without constrains
27: No commercialization of software	46: More effective than opensource
28: Access to banned websites	47: Requires expert knowledge
29: Achieving professional goals	48: Easy to learn
30: Protection of spamming	49: Confidential information
31: Awareness of privacy threats	50: Future protection

Table 4
Values.

Values	
51: Personal dignity	64: Trust
52: Economic Prosperity[a]*	65: Not feeling exploited
53: Achieving goals/self-confidence	66: Reassurance
54: Responsibility	67: Self-control
55: Freedom	68: Human values respect
56: Self-esteem	69: Professional development
57: Security	70: Social welfare
58: Legality	71: Fair cost
59: Privacy	72: Control
60: Pleasure	73: Curiosity
61: Avoiding feeling shame	74: Fear- free living
62: Personal success	75: Equality
63: Avoiding frustration	76: Living a fast-paced life

[a] "Economic Prosperity includes respondents' references" to economic survival, personal growth, income, price discrimination overcoming.

Table 5
Raw matrix of identified ladders[a].

Ladder Number	Content codes				Ladder Number	Content codes			
	1st	2nd	3rd	4th		1st	2nd	3rd	4th
1	1	21	58		**46**	7	16	57	
2	1	13	52		**47**	7	28	55	
3	1	28	52		**48**	7	28	61	
4	1	29	57		**49**	7	33	59	
5	1	30	65		**50**	7	26	51	
6	1	40	59		**51**	7	19	55	
7	1	21	52		**52**	7	13	67	
8	1	16	59		**53**	7	21	59	
9	1	15	59		**54**	7	34	52	
10	1	15	59		**55**	7	21	67	
11	1	21	55		**56**	7	15	69	
12	1	33	59		**57**	7	19	20	69
13	1	16	59		**58**	7	15	59	
14	1	33	73		**59**	7	30	69	
15	1	33	69		**60**	7	40	59	
16	1	43	69		**61**	7	13	72	
17	1	21	74		**62**	7	16	59	
18	1	42	52		**63**	7	15	57	
19	1	43	52		**64**	7	38	59	
20	1	33	52		**65**	7	40	59	
21	1	45	74		**66**	7	28	69	
22	1	33	55		**67**	7	13	59	
23	1	49	74		**68**	7	16	59	
24	1	18	57		**69**	7	40	59	
25	1	50	74		**70**	7	16	55	
26	2	14	52		**71**	7	16	52	
27	3	27	55	64	**72**	7	40	51	
28	3	36	70		**73**	7	33	59	
29	3	48	75		**74**	7	13	59	
30	4	17	57		**75**	7	38	74	
31	4	37	69		**76**	8	39	63	
32	5	28	69		**77**	8	39	59	
33	6	22	60	65	**78**	8	31	66	
34	6	28	60	68	**79**	8	32	66	
35	6	44	52		**80**	8	39	69	
36	6	16	59		**81**	8	39	72	
37	6	28	69		**82**	8	39	63	
38	6	28	69		**83**	8	39	63	
39	6	33	52		**84**	8	41	76	
40	7	23	53		**85**	9	13	67	
41	7	24	52		**86**	10	33	71	
42	7	13	62		**87**	10	46	63	
43	7	33	62		**88**	11	47	75	
44	7	25	62	56	**89**	12	36	59	
45	7	26	59						

[a] Note: The table was arranged and numbered on the first content code for simplicity (i.e., attribute).

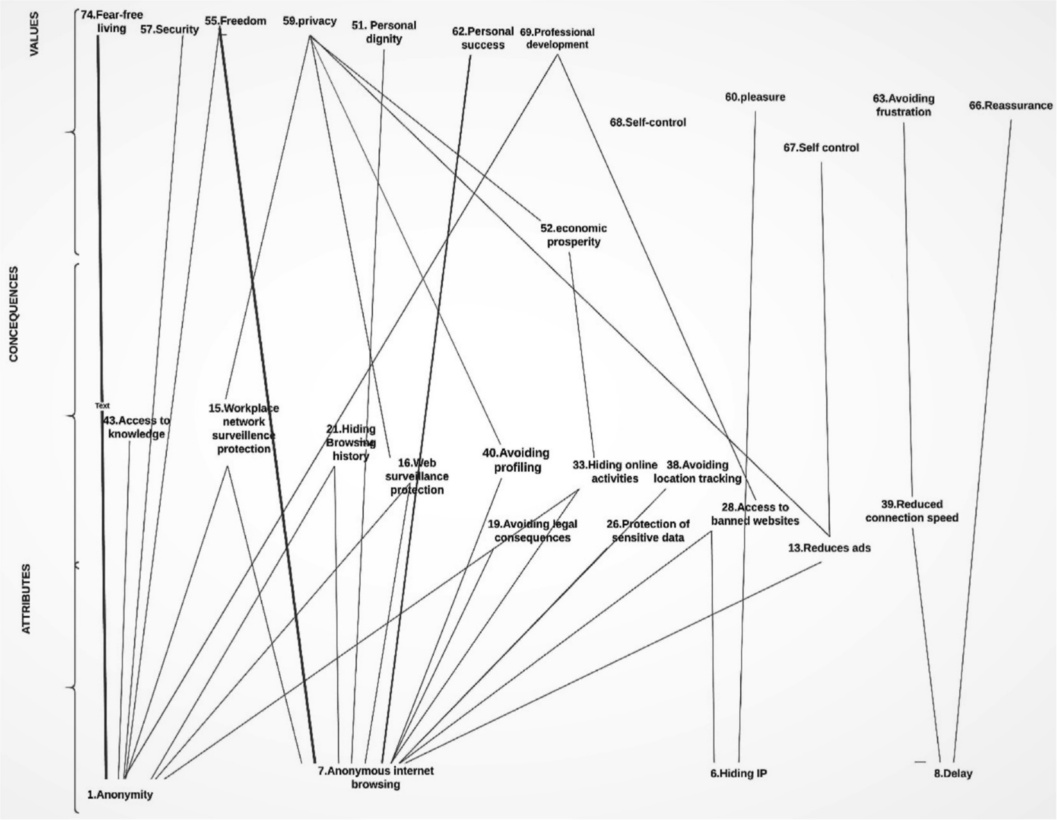
VALUES
CONCEQUENCES
ATTRIBUTES
74.Fear-free living
57.Security
55.Freedom
59.privacy
51. Personal dignity
62.Personal success
69.Professional development
60.pleasure
63.Avoiding frustration
66.Reassurance
68.Self-control
67.Self control
52.economic prosperity
Text
43.Access to knowledge
15.Workplace network surveillence protection
21.Hiding Browsing history
16.Web surveillance protection
40.Avoiding profiling
33.Hiding online activities
38.Avoiding location tracking
28.Access to banned websites
39.Reduced connection speed
19.Avoiding legal consequences
26.Protection of sensitive data
13.Reduces ads
1.Anonymity
7.Anonymous internet browsing
6.Hiding IP
8.Delay

Fig. 1. Hierarchical Value Map.

References

Abeele, V. V., & Zaman, B. (2009). Laddering the user experience. In *User experience evaluation methods in product development (UXEM'09)-workshop*.

Acquisti, A. (2004). Privacy and security of personal information. In L. J. Camp, & S. Lewis (Eds.), *Economics of information security. Advances in information security* (Vol. 12). Boston, MA: Springer.

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

Angulo, J. (2015). Users as prosumers of PETs: The challenge of involving users in the creation of privacy enhancing technologies. In *Standards and standardization: Concepts, methodologies, tools, and applications* (pp. 265–286). IGI Global.

Bagozzi, R. P., & Dabholkar, P. A. (1994). Consumer recycling goals and their effect on decisions to recycle: A means–end chain analysis. *Psychology and Marketing, 11*, 313–340.

Bagozzi, R. P., & Dholakia, U. (1999). Goal setting and goal striving in consumer behavior. *Journal of Marketing, 63*, 19–32.

Benenson, Z., Girard, A., & Krontiris, I. (2015). User acceptance factors for anonymous credentials: An empirical investigation. In *Proc. Of the 14th annual workshop on the economics of information security, 22-23 June 2015, Delft, Netherlands*.

Chaum, D. (1983). Blind signatures for untraceable payments. *Adv. Cryptol.*, 199–203, 1983. Springer.

Chiang, C. Y., & Tang, X. (2020). Use public Wi-Fi? Fear arouse and avoidance behavior. *Journal of Computer Information Systems*, 1–9.

Chiu, C. M. (2005). Applying means-end chain theory to eliciting system requirements and understanding users perceptual orientations. *Information & Management, 42*, 455–468.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM, 42*(2), 60–67.

Clark, J., Van Oorschot, P. C., & Adams, C. (2007, July). Usability of anonymous web browsing: An examination of tor interfaces and deployability. In *Proceedings of the 3rd symposium on Useable privacy and security* (pp. 41–51).

Dudin, M. N., Vysotskaya, N. V., Frolova, E.E., Pukhart, A. A., & Galkina, M. V. (2017). Improving professional competence of the staff as a strategic factor for sustainable development of companies. *J. Business Retail Manag. Res., 12*(1).

Enisa. (2016). Privacy enhancing technologies. available at https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies. (Accessed 1 May 2019).

European Commission. (2015). Data protection special eurobarometer 431/Wave EB83.1 – TNS opinion & social. available at https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf. (Accessed 10 May 2018).

Gengler, C. E., Klenosky, D. B., & Mulvey, M. S. (1995). Improving the graphic representation of means-end results. *International Journal of Research in Marketing, 12*, 245–256.

Graf, C., Hochleitner, C., Wolkerstorfer, P., Angulo, J., Fischer-Hübner, S., Wästlund, E., … Holtz, L. E. (2015). Towards useable privacy enhancing technologies: Lessons learned from the PrimeLife project. *PrimeLife Deliverable D, 4*.

Grunert, K. G., Beckmann, S. C., & Sørensen, E. (2000). Means-end chains and laddering: An inventory of problems and an agenda for research. In T. J. Reynolds, & J. C. Olson (Eds.), *Understanding consumer decision making* (pp. 63–90).

Guardian, T. (2014). Privacy tools used by 28% of the online world, research finds.".21 January 2014. available at https://www.theguardian.com/technology/2014/jan/21/privacy-tools-censorship-online-anonymity-tools. (Accessed 17 December 2018).

Gutman, J. (1982). A means-end chain model based on consumer categorization processes. *Journal of Marketing, 46*, 60–72.

Harborth, D., Herrmann, D., Köpsell, S., Pape, S., Roth, C., Federrath, H., … Rannenberg, K. (2017). *Integrating privacy-enhancing technologies into the internet infrastructure*. arXiv preprint arXiv:1711.07220.

Harborth, D., Pape, S., & Rannenberg, K. (2020). Explaining the technology use behavior of privacy-enhancing technologies: The case of tor and JonDonym. *Proc. Privacy Enhancing Technol., 2020*(2), 111–128.

Hoepman, J. H. (2014, June). Privacy design strategies. In *IFIP International Information Security Conference* (pp. 446–459). Berlin, Heidelberg: Springer.

Hup, B. (2017). *The adoption and diffusion of Privacy-Enhancing Technologies: The factors that drive and impede the adoption and diffusion of Privacy-Enhancing Technologies of private communication and data storage , master thesis*. TU Delft Technology, Policy and Management, Delft University of Technology. 11 December 2017, available at http://resolver.tudelft.nl/uuid:e1ea48b3-aee3-4cbc-985c-708949773057. (Accessed 14 January 2019).

Jung, Y., & Kang, H. (2010). User goals in social virtual worlds: A means-end chain approach. *Computers in Human Behavior, 26*, 218–225.

Kambourakis, G. (2014). Anonymity and closely related terms in the cyberspace: An analysis by example. *J. Inform. Security Appl., 19*(1), 2–17.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134.

Lin, C., & Wang, H. (2008). A decision-making process model of young online shoppers. *CyberPsychology and Behavior, 11*(6), 759–761.

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.

Loshin, P. (2013). *Practical anonymity: Hiding in plain sight online* (pp. 9–10). Newnes.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Philadelphia, PA: Open University Press.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

McManus, P., Standing, C., & Zanoli, R. (2009). A preliminary laddering analysis on mobile services usage. In *ECIS 2009 proceedings* (Vol. 12). https://aisel.aisnet.org/ecis2009/12. (Accessed 10 December 2018).

META Group. (2005). *State of the art of privacy-enhancing technology (PET)*. Danish Ministry of Science, Technology and Innovation, Denmark.

Modesto Veludo-de-Oliveira, T., Akemi Ikeda, A., & Cortez Campomar, M. (2006). Laddering in the practice of marketing research: Barriers and solutions. *Qualitative Market Research: An International Journal, 9*(3), 297–306.

Namara, M., Wilkinson, D., Caine, K., & Knijnenburg, B. P. (2020). Emotional and practical considerations towards the adoption and abandonment of VPNs as a privacy-enhancing technology. *Proc. Privacy Enhancing Technol., 2020*(1), 83–102.

Office of the Privacy Commissioner of Canada. (2017, November). Privacy enhancing technologies – a review of tools and techniques, report prepared by the technology analysis division of the Office of the privacy commissioner of Canada. retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#heading-0-0-1.

Pai, P., & Arnott, D. C. (2013). "User adoption of social networking sites: Eliciting uses and gratifications through a means–end approach". *Computers in Human Behavior, 29*, 1039–1053.

Pavone, V., & Pereira, M. (2009). The privacy vs security dilemma in a risk society. In *Proceedings of PRISE conference: "Towards privacy enhancing security technologies–the next steps* (pp. 109–127).

Pieters, R., Baumgartner, H., & Allen, D. (1995). A means–end chain approach to consumer goal structures. *International Journal of Research in Marketing, 12*, 227–244.

Regulation, G. D. P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Offic. J. Euro. Union (OJ), 59*, 294.

Reynolds, T. J., Dethloff, C., & Westberg, S. J. (2001). Advancements in laddering. In *Understanding consumer decision making* (pp. 108–134). Psychology Press.

Reynolds, T. J., & Gutman, J. (1988). Laddering theory, method, analysis, and interpretation. *Journal of Advertising Research, 28*, 11–31.

Reynolds, T. J., & Olson, J. C. (2001). *Understanding consumer decision making: The means-end approach to marketing and advertising strategy* (Mahwah, N.J., L. Erlbaum).

Rogers, E. M. (2010). *Diffusion of innovations* (4th ed.). New York: Simon and Schuster.

Saaka, A., Sidon, C., & Blake, B. F. (2004). *Laddering. A "how to do it" manual–With a note of caution. Research reports in consumer behavior: How to series*. Ohio: Cleveland State University (February).

Schwartz, S. (2012). An overview of the Schwartz theory of basic values. *Online Readings Psychol. Culture, 2*(1).

Schwartz, S., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J., Demirutku, K., Dirilen-Gumus, O., & Konty, M. (2012). Refining the theory of basic individual values. *Journal of Personality and Social Psychology, 103*(4), 663–688.

Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167.

Srouji, J., & Mechler, T. (2020). How privacy-enhancing technologies are transforming privacy by design and default: Perspectives for today and tomorrow. *J. Data Protect. Privacy, 3*(3), 268–280.

Subramony, D. P. (2002). Why users choose particular web sites over others: Introducing a" means-end" approach to human-computer interaction. *Int. J. Electronic Com. Res., 3*, 144–161.

Sun, P., Cheng, H., & Finger, G. (2009). Critical functionalities of a successful e-learning system — an analysis from instructors' cognitive structure toward system usage". *Decision Support Systems, 48*(1), 293–302.

Taylor, B., Dey, A., Siewiorek, D., & Smailagic, A. (2015). Using physiological sensors to detect levels of user frustration induced by system delays. In *Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing* (pp. 517–528).

Van Rossum, H., Gardeniers, H., & Borking, J. (1995). *Privacy-enhancing technologies: The path to anonymity* (Vol. II). Rijswijk: TNO Physics and Electronics Laboratory (Registratiekamer).

Vanden Abeele, V., Hauters, E., & Zaman, B. (2012). *Increasing the reliability and validity of quantitative laddering data with LadderUX", CHI'12 extended abstracts on human factors in computing systems* (pp. 2057–2062). ACM.

Van den Steen, E. (2004). Rational overoptimism (and other biases). *The American Economic Review, 94*(4), 1141–1151.

Vemou, K., & Karyda, M. (2013). A classification of factors influencing low adoption of PETs among SNS users. In *, Vol. 8058. Trust, privacy, and security in digital business, ser. LNCS* (pp. 74–84). Springer.

Vemou, K., Mousa, G., & Karyda, M. (2015). On the low diffusion of privacy enhancing technologies in social networking: Results of an empirical investigation. In *European, Mediterranean & Middle eastern conference on information systems 2015 (EMCIS2015) ,1st– 2nd June 2015, Athens, Greece*. http://www.icsd.aegean.gr/publication_files/Conference/492112265.pdf. (Accessed 20 February 2017).

Wang, Y. (2009). *"Privacy-enhancing technologies." Handbook of research on social and organizational liabilities in information security*. IGI Global.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193.

Weitzner, D. J. (2018). Promoting economic prosperity in cyberspace. *Ethics and International Affairs, 32*(4), 425–439.

Xiao, S., Witschey, J., & Murphy-Hill, E. (2014). Social influences on secure development tool adoption: Why security tools spread. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing, 2014. ACM* (pp. 1095–1106).

Zeelenberg, M., Nelissen, R. M., Breugelmans, S. M., & Pieters, R. (2008). On emotion specificity in decision making: Why feeling is for doing. *Judg. Decision Making, 3*(1), 18.