Privacy at a Glance: A Process to Learn Modular Privacy Icons During Web Browsing

Maximiliane Windl
LMU Munich
Munich, Germany
maximiliane.windl@ifi.lmu.de

Anna-Marie Ortloff
University of Bonn
Bonn, Germany
ortloff@cs.uni-bonn.de

Niels Henze
University of Regensburg
Regensburg, Germany
niels.henze@ur.de

Valentin Schwind
Frankfurt University of Applied Sciences
Frankfurt, Germany
valentin.schwind@fb2.fra-uas.de

ABSTRACT

Privacy policies (PPs) are currently the only way to inform users about their rights and choices during web browsing and searching. However, users avoid engaging with them, because of their length and abstract legal language, which makes them hard to read and understand. We propose to support the understanding of PPs by using modular icons. Icons have already proven to be helpful in visualizing concepts with high information density. However, the value of using icons to supplement PPs lacks a scientific foundation. Thus, we conducted two studies to evaluate existing icon sets for their understandability and to teach participants their meaning in situ. We show that modular privacy icons can be taught using our process, which has the potential to aid quicker and easier comprehension of PPs. We contribute a set of tested modular privacy icons and a verified process on how to teach them to users incidentally during web browsing.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing** → *Web-based interaction*; *Human computer interaction (HCI).*

KEYWORDS

privacy, privacy policy, icons, web browsing, survey, online study

ACM Reference Format:
Maximiliane Windl, Anna-Marie Ortloff, Niels Henze, and Valentin Schwind. 2022. Privacy at a Glance: A Process to Learn Modular Privacy Icons During Web Browsing. In *Proceedings of the 2022 ACM SIGIR Conference on Human Information Interaction and Retrieval (CHIIR '22), March 14–18, 2022, Regensburg, Germany*. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3498366.3505813

1 INTRODUCTION

Searching and browsing the web is an ubiquitous part of people's daily lives. However, invasion of privacy is an inherent cost of our interaction with the web, in the way it is currently structured and monetized. An increasing amount of personal data is being collected, such as for advertising, localization, and customization of services, but also for more nefarious purposes. Online users are confronted with news about their data being leaked and then misused for criminal activities, such as the attack on Microsoft Exchange [5]. This is not only problematic for those who become victims of hackers, but also for companies, which face a long journey of trying to gain back the trust of their users, e.g. in the case of Facebook and Cambridge Analytica [19]. For users to be able to consciously decide which personal data to disclose online, they need a clear understanding of what kinds of data are being collected, how they are processed, and what possible consequences can arise [17].

Previous attempts to standardize PPs are not widely adopted in practice [6]. Thus, it is still necessary to familiarize oneself with the full PP of an online service, to be able to make conscious decisions regarding the safety of one's personal information. Even after reading PPs, users are unlikely to remain aware of them – particularly considering the plethora of services and irregular updates of PPs. Even though plain text PPs are rarely read and understood due to various reasons including their length, their difficult legal language, and abstract nature, PPs are still the primarily used way to inform users about the usage of their personal information [27, 30, 34]. According to Obar [34], the described issues with PPs lead to 74% of users not reading PPs at all.

One attempt trying to overcome the gap between the provision of information and the actual understanding is enriching PPs by visualizing their core concepts via icons [14, 17, 44]. These icons could be provided on search engine result pages (SERPs) to help users make privacy protecting decisions during web search, on the website itself, or in PPs. Diverse visualizations during search tasks have been explored, e.g. situating search results in 2D space [1], taking advantage of spatial memory using a data mountain metaphor in a 3D environment [43], using different thumbnail representations to investigate website refinding [55], as well as visualizing concepts not directly related to task-relevance, such as credibility [48], or as in this work, privacy [64]. Icons have already been proven to be helpful when visualizing various concepts, e.g. on mobile phones,

CHIIR '22, March 14–18, 2022, Regensburg, Germany
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9186-3/22/03…$15.00
https://doi.org/10.1145/3498366.3505813

maps, or on aircraft safety cards, but their visualization can be difficult when the concept is very abstract as is the case with PPs [17]. Icons aid quick comprehension, take up less space, and tend to have a higher information density than plain text [37]. However, to understand the precise concept of new and abstract icons, it is necessary to learn their underlying meaning from scratch. Earlier attempts trying to construct an icon set, suitable for enhancing and visualizing privacy policies, often either lacked a scientific foundation in the design phase [14, 17], are meanwhile outdated because the topic was no longer pursued [32] or have not been released yet, like sets of icons such as from the Unicode Consortium. But most importantly, even when the aforementioned limitations did not apply, previously proposed icon sets were not thoroughly evaluated for their understandability, due to small sample sizes [14, 45] or comparisons with two different versions of icons, instead of with a ground truth [17]. In addition, there is no indication of whether a complex construct such as PPs can be expanded through the modularity of icons.

Aiming to thoroughly evaluate existing privacy icons and to find a usable approach to teach their underlying meaning, we conducted two studies. Firstly, we collected existing icon sets and evaluated their comprehensibility according to the ISO-Standard 9186-1 and 9186-2 [20, 21]. Subsets were then used for an in-situ-study, where participants were provided with a browser extension that showed an icon and a corresponding excerpt from the PP. We provide a modular tested set of thoroughly evaluated privacy icons and verified the process of how to teach their meaning incidentally during web browsing. The icons are separated into main category and attribute value icons. This modularity makes it easier to visualize the abstract concept of privacy and allows for a flexible usage of the icon set in the future. We also provide the extension's source code and the icon set on Github to enable future research and development[1].

2 RELATED WORK

We present previous work on online privacy and PPs, the problems they suffer from, and possible solutions. We also report how icons can be used to visualize abstract concepts, such as the ones in PPs. Additionally, we outline the way privacy icons are currently used in practice.

2.1 Online Privacy

Online privacy and data protection in the EU is governed by the General Data Privacy Regulation (GDPR), which became active in Europe on May 25 2018 [38]. How and which data is collected and used by online services and by software in general is communicated mostly by using PPs. They aim to inform users about how their data is being processed, and about the choices available to control and limit the collection as well as the usage of their data. This is called *the principle of notice and choice* [46, 62]. Unfortunately, users often do not read PPs [34] and do not understand them the way they are currently implemented, so they do not fulfill their aim of informing the users [42]. Among other reasons, their length and the complexity of their legal language are problematic for users [12]. This contributes to the generally abstract nature of privacy policies in their current state. It is hard for users to connect the general information given in privacy policies to their current context of using the software [12].

It is important that users understand the data practices of online services because online consumers' trust is influenced by a feeling of security concerning private data [13]. When information on privacy is displayed to the users clearly and concisely, it can become a relevant factor in decision making [56]. Some users are even willing to pay more if their privacy is protected [56]. This makes it desirable both for companies and users to have understandable and accessible privacy policies.

Research has also evaluated other techniques to preserve privacy, such as k-anonymity [26, 54] or concealing a single user's data in communities for specialised search interests [49]. Differential privacy is another method which has been investigated in the scope of web browsing [11, 63].

2.2 Icons and their Usage with PPs

The term *icon*, as used in this work, and in the literature referring to graphical user interfaces (GUIs), means a small graphical element in a GUI, which represents a functionality of a system or information about it.

There have been several previous attempts to visualize privacy. On the one hand, privacy indicators have been proposed for SERPs [9, 56, 64], as well as app stores [23], which provide a general rating, but do not provide information on specific privacy risks. Icons to visualize the content of privacy policies have been investigated both in the industry [c.f. 31, 32, 41], and in research [14, 17, 22]. More recent attempts have been driven by the GDPR which explicitly states in Article 12 that "[the information] may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing" [38]. However, visualizing privacy with icons is notoriously difficult, since privacy is such an abstract concept [47]. Additionally, privacy is not users' main goal when searching online, so while icons can be an additional information source and inform decision making [56], they could also be distracting. Consequently, none of the current suggestions have been adopted in practice. Mozilla has developed several sets of privacy icons, starting with a simple alphanumerical approach [32], which was then adjusted to more pictographic icons [31], which were later redesigned to result in an alpha-version [41]. Unfortunately, little is known about the design and evaluation process of these icons, and since 2011, there has not been a publication by Mozilla on the topic. The icons designed by Gerl [14] support the layered privacy language which they developed to facilitate informed consent. However, these icons only cover very specific areas of PPs and were not evaluated very thoroughly. While Efroni et al. [8] propose a risk-based methodology to design privacy icons, no icons have yet been published. Holtz et al. [17] compare two sets of privacy icons, but the development process of these icons is vague and it is unclear whether users were included early on, or just in the evaluation stage. A more rigorous participatory design process basing icons on an ontological foundation was followed by Rossi and Palmirani [44, 45]. Their evaluation of DaPIS (Data Protection Icon Set) focused on legibility and ease of understanding but sample size was limited [44] and they acknowledge that

[1] https://github.com/Maxikilliane/privacy-at-a-glance

learning of icons should be evaluated in more longitudinal studies [45]. Habib et al. investigated icon-text combinations specifically for icons representing privacy choices [15].

In a limited scope, icons are already used in the context of privacy. One example is mobile permissions that are labeled with icons [39]. The closest to PPs is probably the icon and dialog, which some browsers, e.g. Firefox [2] present when a website requests permission to access the user's location. Prior work showed that combining icons with text helps comprehension [15]. This way of presenting icons in the context of additional information could also be used to teach their meaning to the users in a naturalistic way.

Processes exist which evaluate icons for comprehensibility, for example the ISO-norms 9186-1 and 9186-2 [20, 21], or processes based on it [61]. An icon judgment test asks evaluators to judge the percentage of people who would understand the meaning of an icon as given [61]. In a comprehension test, subjects are requested to explain the meaning of an icon given its context and the icon itself [21]. ISO 9186-1 specifies evaluation procedures to be used for these tests [21]. These tests, as well as other work contributing and evaluating icons, be they graphical [e.g. 53, 58], haptic [4] or auditory [52], take place in a laboratory setting. Participants learn icon meanings, like vocabulary, and are queried on them after a certain period to assess longer-term learning. While training like this may be realistic in some scenarios, such as for software in security-relevant domains, it is not possible to train all users affected by something as ubiquitous as PPs. More realistically, for icons to be useful in enhancing PP comprehension, they should be learned incidentally. This means that users are confronted with icons and their meanings during their normal system usage, which has been shown to be beneficial to learning [3].

2.3 Summary

In summary, PPs, the way they are currently presented, are not sufficient to inform users about the usage, collection and choices concerning their data [27, 30, 34]. Icons have the potential to aid quick comprehension by taking up less space and having a very high information density compared to plain text [37]. Consequently, enriching PPs with icons seems to be a very promising approach. In a limited scope, icons are already used in the context of privacy, but there is still no evaluated icon set available [14, 17, 31, 32]. Since PPs depict very abstract concepts and since there is currently no icon set for PPs available to provide familiarity, a process to teach users the meaning of those icons is also necessary.

3 STUDY 1: ICON COMPREHENSION

To acquire a usable set of icons whose meaning is easy to understand at a glance and which are distinguishable from each other, we first evaluated icon comprehensibility in a procedure derived from ISO 9186 [21]. We collected different icon sets from existing publications [17] and online sources [29, 31, 40, 41]. Some additional icons were collected from Fontawesome[2], by searching for "privacy". These icons were grouped into 10 categories based on [59]. Participants then assessed them for comprehension and comprehensibility.

3.1 Icon Choice

To be able to visualize concepts from PPs and to obtain an icon set that can be used for all PPs, privacy statements have to be categorized. In previous work, possible categories for privacy statements were formed based on the content of current PPs [59] or were developed based on legal regulations and problems concerning PPs the way they are currently implemented [33].

We used the categories suggested by the Usable Privacy Policy Project[3], resulting in ten categories: nine main categories, and one 'others' category [59]. In addition to these categories, privacy information has also been associated with category-specific attributes. Not all of those are named in the paper by Wilson, but we extracted them from the accompanying dataset[4]. Three researchers classified the icons separately and assigned categories as well as attribute values, where appropriate. Using the method of Wolff and Götzfried [61], we applied comprehensibility scores to the icons. Classification took place in two rounds, and the researchers discussed differences before going over their classifications the second time.

To select icons for the survey, we first excluded any icons which did not fit into the classification scheme. Icons where all the researchers differed in their classification decision, or where the comprehensibility judgment of the agreeing researchers was lower than 50% were also excluded. We subdivided the remaining icons into icons suited to represent the main categories, and icons suitable to represent attribute values.

To decrease the workload for our participants, we further reduced our initial icon set to one icon for each unique category or attribute value by choosing the one with the highest comprehensibility score, resulting in a final icon set consisting of 9 icons for main categories and 13 icons for attribute values. Since these icons came from different sources, we changed them to make them more similar. Changes included removing any color, removing explanatory texts, adding a black circular border, and ameliorating the quality of several pixelated icons. The final set of icons we tested can be found in the supplemental material.

3.2 Study Design

We used a study design as detailed in ISO 9186-1 and 91861-2 for our first study [20, 21]. These standards define a procedure on how to test the comprehensibility of graphical symbols. The first part is a comprehension test, where participants are presented with an icon and have to answer the question "What do you think this symbol means?" In our survey, each icon was presented in isolation within the survey environment, but the participants were informed about the context in which they can expect the symbol to appear, which we defined as the browser's address bar when visiting certain websites. After the first task, the participants perform a judgment task, where they have to rate how many out of 10 people they assume to understand the meaning of the icons correctly. The icons from the first task were used for that, but this time they were accompanied by explanatory texts. Since each of our icons depicts a category or attribute-value from the taxonomy of Wilson et al. [59], we also used their explanations for the categories and attribute values for this judgment task.

[2] https://fontawesome.com/

[3] https://explore.usableprivacy.org/

[4] https://usableprivacy.org/data

3.3 Procedure

We first acquired informed consent from the participants and informed them about the general nature of the survey. Participants then took part in a comprehension test, as detailed in ISO 9186-1 [21]. They were presented with the icons in a randomized order to avoid sequence effects and responded to the question "What do you think this symbol means?" in free-text. The participants were instructed to answer with "don't know" in case they were unable to provide a proper answer.

In a second step, participants judged the comprehensibility of the icons. They saw all icons again in a randomized order. The icons were presented together with their name, meaning, and the context in which they would typically appear. Participants then rated each icon for comprehensibility, by stating the percentage of people which they expect to understand the icon [61]. We used a method of simplification from previous work [10], where participants stated how many out of ten people they expect to understand an icon, instead of asking for a percentage outright. Participants answered two questions on their previous experience with privacy policies and privacy related icons. Demographic data was collected before the participants were debriefed. We include the survey in our supplemental material.

3.4 Participants

Our participants were recruited via mailing lists of our institution and by word of mouth. We aimed to reach a more diverse target group by using snowball sampling starting with this convenience sample. In total, 38 people took part in our first study, (21 female, 16 male, one diverse), aged between 20 and 55 ($M = 26.4$, $SD = 7.36$). Most (30) of the participants were students, some (7) were working, and one person was retired. Fourteen had previously encountered privacy icons before, while 24 had not. Six participants gave more detailed information on their experiences with privacy icons, including two who stated that they had encountered them before. However, both of those described their contact with privacy icons as only fleetingly.

3.5 Data Analysis

We followed the recommendation given in the ISO 9186-1 on analysis of the data and categorized the responses [21]. Three researchers separately coded the participants' answers to the comprehensibility test, marking them from 0 to 3, where 0 was 'don't know', 1 was 'wrong', 2 was 'somewhat correct' and 3 was 'correct'. We deviated from [21] by including 'somewhat correct' as an option, because the complex nature of the concepts which the privacy icons represent, makes it hard for participants to grasp the entire meaning, and we wanted our results to reflect answers going in the right direction. Disagreements were resolved by discussion. To analyze the icon judgment task, we calculated descriptive statistics for presumed comprehensibility for each icon.

3.6 Results

To assess the correctness of the meanings that participants assumed for the icons, scores were assigned by comparing the participants' answers to the original description of each category.

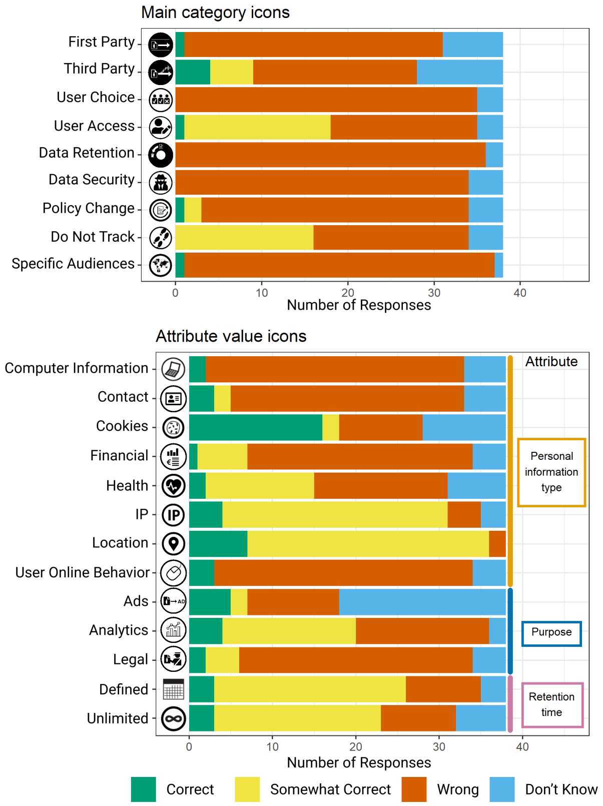


Figure 1: Correctness judgments (majority opinion of three raters) of participant's descriptions of main category and attribute value icons

The interrater reliability for three raters was determined using Krippendorf's alpha [24], which is an extension of classical measures of interrater reliability, such as Cohen's Kappa, for ordinal variables and two raters. Assuming ordinal variables, Krippendorf's alpha resulted in a value of 0.897 for the complete set of 836 answers. According to Krippendorf, a value which is greater than 0.8, passes as reliable [24]. In the first rating results, there were 4 answers that the raters did not agree on, meaning every rater assigned a different score to an answer. After discussing these outliers and agreeing on a consistent score, Krippendorf's alpha improved to a final value of 0.9 and we used majority ratings in our further analyses.

Out of all 836 answers, 13.3% were rated as 'don't know', 57.18% as 'wrong', 22.25% as 'somewhat correct', and 7.3% as 'correct'. However, when analyzing the main category icons and attribute value icons separately, there is a discrepancy between how many icons are labeled correctly by the participants (see Figure 1).

While there are still answers classified as 'don't know' or 'wrong', the attribute value icons were generally understood better than the main category icons. This could be since main category icons usually depict more abstract and complex concepts than attribute value icons, which describe more concrete things. For example, the 'cookie' icon depicted a cookie food item, which many participants recognized and correctly related to the principle of online cookies.

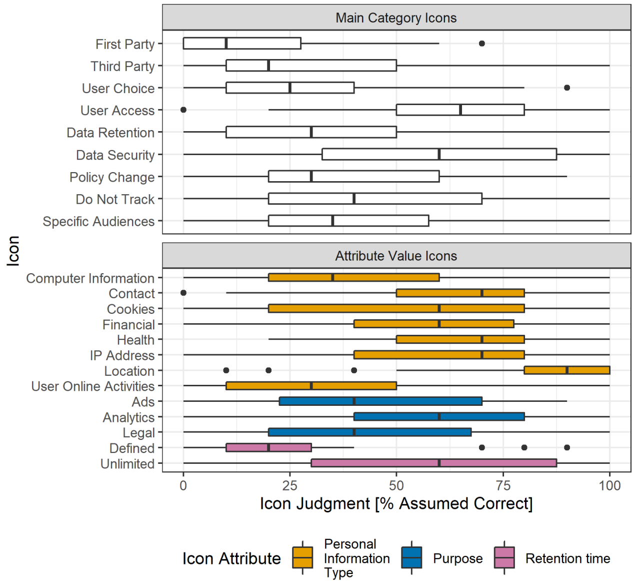


Figure 2: Judgment ratings for main category and attribute value icons

Another category that received many correct answers, was the 'location' category. The icon used for depicting that the user's location is being tracked is also used within many popular sites and apps (in slight variations), such as Google Maps. Therefore, the participants already knew the icon and successfully recognized it. When analyzing the judgment task, the main category icons were deemed less understandable in general than attribute value icons (see Figure 2).

This can most likely again be explained because the attribute value icons involve more concrete concepts, which are more easily recognized and depicted within a single icon. These results are similar to those in the comprehension task in this study: the 'location' icon reached better comprehension scores than others and was also judged to be well understood in this study segment. However this relationship does not always hold true, seeing as the 'Retention Time: Defined' - icon had an above average comprehension rating but was then judged to be the least understandable.

4 STUDY 2: LEARNING OF PRIVACY ICONS

As we found that the majority of the privacy icons were not understood correctly by the participants in our first study, we conducted a second study with a different set of participants to teach their meaning. For that, we developed a browser plugin for Firefox and Chrome browsers, which shows a pop-up with an icon and related information once every hour. After two weeks of using the plugin, the participants completed a comprehension test, which verified the learning success for both types of icons.

4.1 Study Design

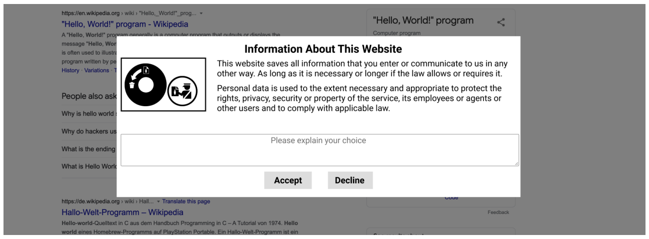
We evaluated a subset of icons in situ during a two week deployment on the participants' computers using a browser plugin in a repeated measures design. We elected to present icons on websites in general and not only SERPs because this is more widely applicable. The icons were present during participants' normal usage of the web, and the participants were not informed prior to the experiment that their actual task was to learn the icons' meanings. We decided to protect our participants' privacy by not tracking participants' website visits, but this meant that we were not able to present accurate information about the website's privacy policies. To counter misrepresentation of websites, we informed participants about this decision both before the study, and in a debriefing afterwards. From the icons in study 1, we selected three categories which shared the attributes *Purpose* and *Personal Information Type to enable a full factorial design. For each of these attributes, we selected three attribute value icons to achieve variety in the data collection.* The hourly presentation and the randomized permutation of all icons ensured that no icon was overlooked, and icons were presented equally often. We measured how well the icons were understood at two different times, once before, and once after the two-week intervention, and thus measurement time was the first factor. The second factor was the type of the icons, where we compared the main category and attribute value icons to similarly complex medical icons, which we used as a control.

4.2 Procedure

The participants were informed about the procedure of the experiment before they signed an informed consent form. The participants then took part in a comprehension test for the icons we used in the study. The comprehension was measured by showing each participant seven statements about the presented icon, for which they had to judge the correctness. We generated true statements by adapting the description of the categories and attribute values in previous work [59] and false statements by using participants' wrong answers from the first study. We also added additional random icons related to medicine to obfuscate the true intent of the study beforehand. These medical icons were chosen, because they were of a similarly abstract level as the privacy icons.

By not informing the participants that measuring the learning success of icons was our intention, we ensured that participants did not try harder than they normally would to learn the meaning of the icon set. The participants were then given installation instructions for the browser plugin and were told to otherwise use their browser as usual for the two weeks of study. During that time period, the plugin periodically showed pop-ups consisting of icons and information from PPs, as depicted in Figure 3. The pop-up was displayed to the participants on the first website they visited after opening their browser, and then only once every hour, so as not to disturb them too much. We also ensured that participants would see each icon and information equally often in a randomized order. The pop-up could not be closed before selecting a choice concerning agreement with the privacy information and giving a reason for that choice, to ensure interaction with the icons. The answers were saved in a log file on the participants' computers.

After two weeks, we obtained the log files from their computers. Afterward, they had to complete the same comprehension test as before the study. The participants completed an additional matching task [25, 28], where they had to match a category description



Information About This Website

This website saves all information that you enter or communicate to us in any other way. As long as it is necessary or longer if the law allows or requires it.

Personal data is used to the extent necessary and appropriate to protect the rights, privacy, security or property of the service, its employees or agents or other users and to comply with applicable law.

Please explain your choice
Accept
Decline
https://en.wikipedia.org › wiki › "Hello,_World!"_prog...
"Hello, World!" program - Wikipedia
"Hello, World!" program
Computer program
People also ask
https://de.wikipedia.org › wiki › Hall... Translate this page
Hallo-Welt-Programm – Wikipedia
Feedback

Figure 3: Example of a Pop-Up. The bigger icon depicts the main category, whereas the smaller one depicts the attribute value. Explanatory texts are provided for both icons.

to its correct icon. We also asked several questions about the participants’ understanding of the icons’ presentation in the pop-up and measured their subjective understanding [57] concerning syntax and content of the privacy statements presented with the icons. Finally, we asked the participants for some demographic data and thanked them for taking part in the study, before debriefing them. Students received course credits for their participation.

4.3 Apparatus

The system was developed as a browser plugin for Firefox and Chrome browsers, which are the most used browsers in the population of the country, where the study took place [51]. It displayed pop-ups with icons and privacy information, see Figure 3.

The privacy information consisted of real snippets from PPs mapped to the categories and attribute values discussed in subsection 3.1. We collected them using usableprivacy.org. To make the information more realistic, we replaced mentions of website names in the PP text with "this website", however, we did not present text from participants’ actual current website, since we did not want to track their browsing behavior.

We always showed two icons to our participants. The larger one represented a main category, and the smaller one an attribute-value. We combined the category icon with only one smaller icon at a time, to isolate effects. For the main categories, the icons and information snippets are presented in Table 2. The attribute-values, their corresponding icons, information snippets, and attributes are shown in Table 1. The plugin showed the information in a randomized order. A unique combination of icons and information was only shown a second time, after all other combinations of icons and information had already been shown once.

4.4 Participants

For the second study, a different set of 30 participants was recruited by first using institutional mailing lists, followed by using snowball sampling starting with this convenience sample. The ages of the 8 female and 22 male participants ranged between 20 and 33 (M=23.4, SD=3.0). 27 of the participants were students, and three worked as a programmer, technician and in customer service respectively. Most students (19) were majoring in media informatics, and one each in performance-studies, psychology, media production, law, geoecology, marketing, cultural studies, and linguistics. The majority (24) of the participants stated that they had not encountered privacy icons before. We compensated the students with course credits[5].

4.5 Data Analysis

First, we calculated descriptive statistics for the log-data collected by the plugin about the exposure of the participants to privacy icons, and checked how many pop-ups participants had seen. To validate our method of measuring icon comprehension, we then compared the results of the post-intervention icon comprehension survey with those of the post-intervention icon matching test. The comprehension tests were evaluated using aligned rank transform (ART) [60], a non-parametric form of ANOVA, with icon type and time of measurement as independent variables and percentage of correctly classified statements about icons as the dependent variable. We hypothesized that the number of times an icon was seen by the participants during the study could influence their comprehension, so we additionally used multilevel modeling to include viewing frequency as a covariate. Since participants differed in the usage time of their computers, this value could vary for different participants. Qualitative feedback from the participants was analyzed using affinity diagrams [16].

4.6 Quantitative Results

We first examined participants’ general understanding of the way icons were presented. The plugin showed two icons at once – a bigger main category icon to the left and a smaller attribute icon to the right. We wanted to investigate whether the participants generally understood that the bigger icon represented the main category, while the smaller one described it further. Out of 13 statements about icon presentation, which had to be classified as either correct or wrong, participants classified on average 73% correctly (min = 46%, max = 100%). We take this to mean that the structure of the icon combination and their mode of presentation was reasonably well understood. The participants also answered two questions on their subjective comprehension of content and syntax of the text accompanying the icons [57]. Both were measured on a Likert scale from 1 (strongly disagree) to 5 (strongly agree). The subjective comprehension of the content was relatively high ($M = 4.17$, $SD = 0.46$), with the subjective comprehension for syntax being a bit lower ($M = 3.93$, $SD = 0.69$). This is understandable since the statements accompanying the privacy icons came from real PPs, which are known for their complex style of writing. Still, the comprehension levels of the participants were still relatively high.

During the two weeks, each of the participants saw the pop-ups on average 30.9 times ($SD = 25.0$). The maximum viewing frequency was 85, while the minimum was 1. The pop-ups asked the participants to decide for each case, whether they would accept the data practices stated there, or not. There were differences between the individual participants regarding their acceptance of data practices. On average, the participants accepted 47% of the practices presented to them (SD = 22%, min = 12%, max = 100%). However, because the presented icons did not relate to the current

[5] At our institution, students have to earn a certain amount of study credits towards the completion of their degree, where one hour equals one course credit. The participation is anonymous so that the students receive the same amount of compensation, no matter their responses.

Table 1: Snippets, icons and values used in plugin for attribute-values.

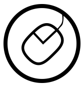
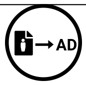
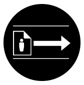
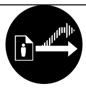
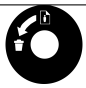
Attribute	Attribute Value	Icon	Information Snippet used
Personal Information Type	Contact Information		Contact information is collected. For example your name and address. Possibly also your telephone number or email address.
	Financial Information		Payment and invoice information is collected, as well as credit information from credit bureaus that are used to prevent and detect fraud and to provide certain credit or financial services.
	User Online Activity		Certain information is collected automatically and stored in server logs. This includes: Details about how you used our service, such as: Your searches, the time you spend on the page, the pages you visit, mouse movements and clicks, etc.
Purpose	Advertisements		This information is used to offer you customized content. For example, advertisements adjusted to your interests.
	Analytics		The information collected, such as demographic data, interests and behaviors, is used for research and analysis purposes in order to better understand users and to improve products and services.
	Legal		Personal data is used to the extent necessary and appropriate to protect the rights, privacy, security or property of the service, its employees or agents or other users and to comply with applicable law.

Table 2: Snippets and icons used in plugin for main categories.

Category	Icon	Information Snippet used
First Party Collection/Use		This website collects and uses data about you.
Third Party Collection/Use		Some of the content, advertising and functions of our service may be provided by third parties, e.g. from the advertisers. These third parties may collect or receive certain information about your use of the services.
Data Retention		This website saves all information that you enter or communicate to us in any other way. As long as it is necessary or longer if the law allows or requires it.

website's actual data practices, and since we assume that the information context has an influence on the acceptance of different data practices [18], we do not think the acceptance or rejection of these practices is meaningful. Consequently we do not report further details.

To validate our method of measuring the participants' comprehension of the privacy icons, we compared it to the results of a matching task, which has been used in the literature to assess comprehension of icons [25, 28, e.g.]. We assumed that participants who were able to match the description of an icon's meaning to the right icon would also classify a higher percentage of the statements from the icon comprehension test correctly. We used a one-sided Wilcoxon rank sum-test because the assumption of normality in the two groups was not valid. It showed that the percentage of correctly classified statements for those icons which were matched correctly ($M = 75.5, SD = 19.9$) was significantly larger ($W = 6770, p < .001$) than those who were matched wrongly ($M = 61.8$, SD=25.6). Thus we consider our approach of measuring the participants' comprehension of privacy icons valid.

For our main analysis, we used ART as a non-parametric alternative to ANOVA [60], since the assumption of normality within groups was not satisfied. We investigated the effect of time of measurement (pre and post-intervention) and icon type (control icon, main category icon, and attribute value icon) on the knowledge about icons. There was a significant main effect of time, $F(1, 1039) = 15.3, p < .001$, but no significant main effect of icon type on knowledge about icons, $F(2, 1039) = 0.24, p = .79$. Additionally, there was a significant interaction between time and icon type, $F(2, 1039) = 13.1, p < .001$.

Since significant effects cannot be interpreted in the presence of a significant interaction, we only conducted post-hoc tests for the interaction and calculated differences of differences using the *testInteractions* function from the phia package for R [7]. Participants' knowledge of icons pre- and post-study differed significantly between diversion and main category icons $\chi^2(1) = 18.4, p < .001$, as well as between diversion and attribute value icons $\chi^2(1) = 16.1$, $p < .001$, but not between main category and attribute value icons $\chi^2(1) = 1.11, p = .29$. This relationship is depicted in Figure 4.

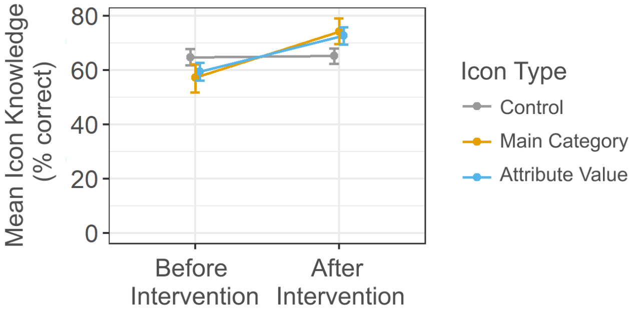


Figure 4: Means of icon knowledge compared by time and icon type

The participants' comprehension of both types of privacy icons increased significantly through the intervention, but the comprehension of the medical icons did not. Thus regular exposure to the privacy icons, together with related text, was a successful way to increase comprehension of complex modular icons.

Since there was no viewing frequency for the diversion icons which served as a control group, we could not incorporate viewing frequency into this type of analysis, which would have become unbalanced. So, we reverted to a linear mixed-effects model maximizing the log-likelihood to assess the effect of including icon viewing frequency as an independent variable, in addition to time of measurement and icon type. The relationship between intervention and icon comprehension showed significant variance in intercepts across participants, $SD = 4.43$ $(95\%CI : 2.81, 6.98)$, $\chi^2(1) = 13.0$, $p < .001$ for this model. However, viewing frequency did not significantly affect knowledge about icons, $b = 0.13$, $t(1020) = -0.63$, $p = .53$. We did not further interpret the other effects in this model, since they were already accounted for in the ART ANOVA.

It becomes evident that the participants learned the meanings of the privacy-related icons during the study, but their knowledge about the control icons, to which they were not exposed, did not increase significantly. The increase in knowledge was slightly more dominant for the main category icons than for the attribute value icons. The more abstract main category icons were harder to understand without previous knowledge, that is to say prior to the intervention, as shown in study 1 presented above. However, during the study, the participants were exposed more frequently to the main category icons, since each of those could be combined with six attribute value icons. Even though the effect of the number of times an icon was seen by a participant was not significant, the higher viewing frequency could be a reason for the larger increase in comprehension for main category icons, as seen in Figure 4.

4.7 Qualitative Results

At the end of study 2, we asked the participants which component (the icon, the text, or both) they considered most important. Additionally, we asked for any other feedback regarding the plugin, the icons, or the texts. We used affinity diagrams [16] to evaluate the participants' statements by first coding the statements, then identifying relationships and connections between themes and giving each theme a representative name. All quotes in this section have been translated into English by the authors.

4.7.1 *Evaluation of feedback on icons and texts.*

When comparing the importance of icons and text, a majority (23/30) of participants regarded the text as being more important than the icons. Only one person answered that the icons were the most important part of the pop-up, and six participants rated both icons and text as equally important. We identified three themes, which we labeled as "conciseness of text", "icon usefulness progression" and "icon-text synergy".

Conciseness of text. Participants found, that "icons are not meaningful enough" (P23), while "[...] the text is unambiguous" (P9). Other participants stated that the "text was always easily understandable, the icons were not" (P11) and "[the text] explains exactly what is happening, the icons don't convey a concrete meaning and are heavily context-dependent" (P24). This points towards the issue that users are not comfortable with looking at complex and unknown icons and rather default back to reading textual explanations.

Icon usefulness progressions. Participants saw the benefit of the icons after having some time to get used to them. "At the start [I read] the text for explanations, but later on I only looked at the icons" (P29). More answers that support this are "at first, the icons did not make sense. After getting to know the icons, the text became less relevant" (P21) and "[...] after some time you could remember the icons, which allowed one to often just look at the icons and know what the pop-up is about at a glance." (P13).

Icon-text synergy. This theme revolves around the relationship between icons and text. "The meaning of the icons is strengthened by the text" (P22), which means that the participants looked at both the icon and the text in order to fully understand the meaning of the popup message. Other participants stated that having a text as a supplement for the icons makes "understanding and learning [them] easier" (P6). Overall most participants focused mostly on the text and found it more useful than the icons. This stresses the importance of introducing the icons together with text.

4.7.2 *Evaluation of additional feedback.*

We identified three themes, which we labeled as "feedback on the plugin", "feedback on the icons" and "conceptions about data collection".

Feedback on the plugin. Participants could see the benefit of the plugin and could imagine using it in the future, but only if some changes were made to make the plugin less intrusive "I can imagine using such a plugin if the icons are shown at some inconspicuous place in the browser" (P17). Suggestions for improvement mostly revolved around the usage of pop-ups. While participants generally did not like the use of them: "please do not use pop-up windows in the finished application" (P1), one participant saw them as beneficial "I felt that the pop-ups severely disrupted my natural use of the internet, but that also gave me a level of reflection to improve awareness of my data, which is why I didn't think it was bad." (P9) One participant suggested having "[...] symbols next to the search results in Google or next to links so that end-users know about the data that is collected [...] before they visit the website." (P4) General feedback included feedback on the design "I wanted to refuse to collect the data. However, the green button suggested that I could confirm my entry." (P23) and remarks on the frequency of the pop-up "The pop-up windows were only ever shown to me during my first Google search of the day. This was probably because I was not using the browser for very long." (P2)

Feedback on the icons. The design of the icons was generally well-received "I think the icons are a good solution to prevent a lot of text" (P17) and "I find the icons meaningful and neither too complex nor too simple designed." (P13). Nevertheless, participants still thought the text was necessary to get the full meaning of the icons "The icons are usually only understandable with the text" (P12). Participants also commented on how they interacted with the icons. They considered it important to repeatedly be introduced to the meaning of the icons "I doubt that the icons really make sense if you only read their meaning once" (P17), but the longer they interacted with the plugin, the less they focused on the text. "The more familiar I was with the tool, the more I paid attention to the icons and only skimmed the text for keywords." (P9)

Conceptions about data collection. Participants also commented on the collection of their data, stating their agreement with it or their interest in protecting their privacy. The plugin forced the participants to reflect on their behavior regarding data and to think about which data they wanted to disclose. One participant observed their behavior with data and stated that "it turned out that I am very liberal with the disclosure of my data". (P9), but this did not include address- or financial-data. The participant only disclosed such data, when they "[...] really saw the need to disclose these types of data to be able to use the service." (P9) Another participant did not want to disclose any of their data, because there were no advantages big enough to outweigh the interest in protecting their privacy. "I understand that it can be beneficial for the advertising industry and website improvement, but I don't see any benefit in it that would be more important to me than my privacy." (P6)

5 DISCUSSION

In two studies, we evaluated existing icon sets for their quality and understandability according to an ISO-Standard procedure and taught participants their meaning in situ using a web-based browser extension. We found that, even though our participants were a tech-savvy young sample, which represents an ideal situation the meaning of most icons was not easily comprehensible, even as some icons were understood correctly by our participants. This shows the need for a process to teach the meaning of complex icons.

We developed and tested such a process by providing our participants with a browser extension for two weeks, which periodically showed icon combinations alongside explanatory texts. With our approach, we were able to increase the icon comprehension of our participants significantly. It remains to be investigated whether understanding and identifying icons also means that the complex concepts, which they represent, such as data retention, or third party collection, are understood by participants. By collecting quantitative and qualitative data, we could also determine the perceived usefulness of adding icons to privacy information, and gained further insight into the learning process. A finding from these data is the importance of accompanying icons with explanatory texts, especially at the beginning, but also that this text can be gradually reduced as time passes.

A major strength of our icon set is its modularity, which allows for several "mix and match" approaches. We provide separate icons for the main categories, and icons for the attribute values, which can be used to describe these practices in more detail. A main category icon could depict "First Party Collection and Usage", while the attribute value icons describing that practice in more detail could be "Purpose: Advertisement" or "Information Type: Contact". This makes our icon set very flexible and allows for diverse applications in practice, allowing to set the level of detail as it is needed.

We conclude that, even though privacy icons are harder to understand on first encounters due to their abstract nature, their meaning can be taught incidentally during browsing, at least when they are introduced alongside explanatory texts. We were able to show that modular icons and their meaning can be learned using browser-based message boxes and we assume that they can also be used in context. This knowledge forms the basis for anchoring modular icons in context. Our study shows, that users see the benefit of those icons in making it easier and faster to get the gist of the usually long and complicated privacy texts. Thus, modular privacy icons are a promising approach to supplement PPs to make them more accessible and easier to understand.

5.1 Limitations

Even though our studies show the benefit of enriching PP statements with icons, there are also several limitations which need to be addressed in more detail.

To be able to represent a whole PP with icons, we would need to have a complete icon set encompassing all attributes, and attribute values. We were limited in the number of privacy icons, because we collected them from previous research and also excluded those, where we assessed their comprehensibility to be low.

Further, the procedure of our second study is not very likely to be implemented as such in practice, since we used a pop-up which covered the whole screen and therefore heavily interfered with the users' work flow. This approach was necessary to ensure that the participants actually saw all icon combinations. However, ensuring privacy is not users' main aim when searching online, so it is important to ensure that informing them, and also teaching them the meaning of privacy icons, does not interfere with their search task. Since we proved that the meaning of complex icons can be taught incidentally, more subtle representations can be used in the future. Such a more discreet representation could be e.g. realized using a similar approach to the Firefox browser's permission dialogue, which is shown near the address bar [2], or on hovering over a search result. It remains to be investigated how the presentation of multiple icons at the same time, e.g. when representing all the information about the privacy policy of a search result, influences learning. To reduce the amount of icons shown at the same time, approaches like contextual PPs could be used [12].

Another limitation of our study was the sample, which consisted mainly of students, most of whom majored in a technical field. Thus, our sample might be more technically savvy and has more background knowledge about online privacy than the average person and results might not generalize well to a larger population. Our research used this edge case demographic, in a first attempt to explore how privacy icons are understood and can be used. Our study 1 shows the necessity of teaching the meaning of privacy icons, even for a tech-savvy sample, and our study 2 provides a possible process to do this. Additionally, previous work in the field of usable privacy showed that a student sample did not produce significantly different results than a more representative sample [50].

Although our approach faces several limitations, like not having a complete icon set, and a constructed experiment setting which is not very likely to be used as such in practice, our findings can be applied in practice. We showed that learning complex icons incidentally during web browsing is possible, which allows moving to more subtle forms of representation and provides a simple and adaptable procedure on how to assess the comprehensibility of privacy icons. This approach can be used for future work, e.g. by designing the missing icons, and teaching their meaning using our process.

5.2 Future Work

By providing our icon set we enable others to build on this set to design the missing icons and directly test them using the approach as described in this paper. On the other hand, the extension's source code can be a good starting point for developing more subtle forms of representation, while still teaching the meaning of those icons.

Previous work showed that contextual privacy policies, where the information is shown exactly when it becomes relevant, are perceived as very beneficial by the users [35, 36]. Privacy icons could be used for that approach, e.g. the icon depicting advertisement could be displayed directly next to an online ad. Likewise, other applications of privacy icons are imaginable, like enriching PPs in their current state to not only make it easier to skim the texts, but also to help with their legal language and phrasing, because the familiar icons can help getting the gist of those texts.

Our participants stated that as time passed they did not read the text anymore, but only looked at the icons. That leaves one of the most important challenges to future work as to decide when and how to gradually decrease the amount of text needed to understand the meaning of complex icons. Another interesting question is if and how users' behavior changes when they interact with privacy icons.

6 CONCLUSION

Our paper provides a set of thoroughly evaluated privacy icons. The main contribution of this paper is a proven process of how to teach the meaning of complex privacy icons. We showed that, while it is hard to deduce the meaning of privacy icons from only looking at an image, the complex meaning of PPs can be taught incidentally during web browsing using modular privacy icons. This is encouraging since privacy icons are a promising way to condense complex information. They can be used to enrich PPs, making it easier to skim the texts or could even be used by themselves showing relevant information at a glance, e.g. as an information box when visiting new websites or in the address bar of the browser. Privacy icons have the potential to help users understand what is happening to their data, enabling them to make conscious decisions in terms of online privacy. A challenge left for future work is to explore when and how to gradually reduce the amount of text and information presented until there are only the icons left and users are able to assess privacy practices of websites at a glance.

ACKNOWLEDGMENTS

The authors are grateful to Lukas Jackermeier for contributing to the first version of this manuscript.

REFERENCES

[1] Christopher Ahlberg and Ben Shneiderman. 2003. Visual Information Seeking: Tight Coupling of Dynamic Query Filters with Starfield Displays. In *The Craft of Information Visualization*, Benjamin Bederson and Ben Shneiderman (Eds.). Morgan Kaufmann, San Francisco, 7–13.

[2] Alice Wyman, Tonnes, Michele Rodaro, hoosteeno, Marcelo Ghelman, and yoasif. n.a.. Does Firefox share my location with websites? https://support.mozilla.org/en-US/kb/does-firefox-share-my-location-websites. Last accessed: 2022-01-06.

[3] John Robert Anderson, Franklin Boyle, Robert Farrell, and Brian Reiser. 1984. *Cognitive principles in the design of computer tutors.* Technical Report. Carnegie-Mellon University Pittsburgh.

[4] Andrew Chan, Karon MacLean, and Joanna McGrenere. 2008. Designing haptic icons to support collaborative turn-taking. *International Journal of Human-Computer Studies* 66, 5 (2008), 333 – 355.

[5] Kevin Collier. 2021. U.S. issues warning after Microsoft says China hacked its mail server program. https://www.nbcnews.com/tech/security/u-s-issues-warning-after-microsoft-says-china-hacked-its-n1259522. Last Accessed: 2022-01-06.

[6] Lorrie Cranor and Lawrence Lessig. 2002. *Web Privacy with P3P.* O'Reilly & Associates, Inc., Sebastopol, CA, USA.

[7] Helios De Rosario-Martinez. 2015. *phia: Post-Hoc Interaction Analysis.* https://CRAN.R-project.org/package=phia R package version 0.2-1.

[8] Zohar Efroni, Jakob Metzger, Lena Mischau, and Marie Schirmbeck. 2019. Privacy Icons: A Risk-Based Approach to visualisation of Data Processing. *European Data Protection Law Review (EPDL)* 5, 3 (2019), 352 – 366.

[9] Serge Egelman, Janice Tsai, Lorrie Cranor, and Alessandro Acquisti. 2009. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. ACM, New York, 319–328.

[10] European Telecommunications Standards Institute. 2006. *Human Factors (HF); Access symbols for use with video content and ICT devices; Development and evaluation.* Technical Report.

[11] Liyue Fan, Luca Bonomi, Li Xiong, and Vaidy Sunderam. 2014. Monitoring Web Browsing Behavior with Differential Privacy. In *Proceedings of the 23rd International Conference on World Wide Web* (Seoul, Korea) *(WWW '14)*. ACM, New York, NY, USA, 177–188.

[12] Denis Feth. 2017. Transparency through Contextual Privacy Statements. In *Mensch und Computer 2017-Workshopband*, Manuel Burghardt, Raphael Wimmer, Christian Wolff, and Christa Womser-Hacker (Eds.).

[13] Carlos Flavián and Miguel Guinalíu. 2006. Consumer trust, perceived security and privacy policy. *Industrial Management & Data Systems* 106, 5 (2006), 601–620.

[14] Armin Gerl. 2018. Extending layered privacy language to support privacy icons for a personal privacy policy user interface. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32.* 1–5.

[15] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, New York, NY, USA, Article 63, 25 pages.

[16] Gunnar Harboe and Elaine M. Huang. 2015. Real-world affinity diagramming practices: Bridging the paper-digital gap. *Conference on Human Factors in Computing Systems - Proceedings* 2015-April (2015), 95–104.

[17] Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. 2011. Towards Displaying Privacy Information with Icons. In *Privacy and Identity Management for Life*, Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, and Ge Zhang (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 338–348.

[18] Chiung-wen (Julia) Hsu. 2006. Privacy concerns, privacy practices and web site categories. *Online Information Review* 30, 5 (01 Jan 2006), 569–586.

[19] Jim Isaak and Mina J. Hanna. 2018. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer* 51, 08 (aug 2018), 56–59.

[20] ISO Central Secretary. 2008. *Graphical symbols — Test methods — Part 2: Method for testing perceptual quality.* Standard. International Organization for Standardization, Geneva, CH. https://www.iso.org/standard/43484.html

[21] ISO Central Secretary. 2014. *Graphical symbols – Test methodsg – Part 1: Method for testing comprehensibility.* Standard ISO 9186-1:2014(E). International Organization for Standardization, Geneva, CH. https://www.iso.org/standard/62711.html

[22] Timo Jakobi, Mandy Balthasar, Martina Borkowsky, and Harmut Schmitt. 2020. Transparenz & Datenschutz: Privacy Icons aus Sicht von UX Professionals. In

Mensch und Computer 2020 - Usability Professionals, Holger Fischer and Steffen Hess (Eds.). Gesellschaft für Informatik e.V. und German UPA e.V., Bonn.

[23] Patrick Gage Kelley, Lorrie Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. ACM, New York, 3393–3402.

[24] Klaus Krippendorff. 1980. *Content analysis: An introduction to its methodology.* Sage publications.

[25] Rungtai Lin. 1994. A study of visual features for icon design. *Design studies* 15, 2 (1994), 185–197.

[26] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. 2007. L-Diversity: Privacy beyond k-Anonymity. *ACM Trans. Knowl. Discov. Data* 1, 1 (March 2007), 52 pages.

[27] Aleecia McDonald and Lorrie Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543–568.

[28] Siné McDougall and Sarah Isherwood. 2009. What's in a name? The role of graphics, functions, and their interrelationships in icon identification. *Behavior Research Methods* 41, 2 (01 May 2009), 325–336.

[29] Matthias Mehldau. 2007. Iconset for Data-Privacy Declarations v0.1. https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf. Last accessed: 2022-01-06.

[30] George R. Milne, Mary J. Culnan, and Henry Greene. 2006. A Longitudinal Assessment of Online Privacy Notice Readability. *Journal of Public Policy & Marketing* 25, 2 (2006), 238–249.

[31] Ben Moskowitz, Mozilla, and Aza Raskin. 2011. Privacy Icons project (beta release). https://wiki.mozilla.org/Privacy_Icons. Last Accessed 2022-01-06.

[32] Mozilla. 2011. Privacy Icons v0.2 – MozillaWiki. https://wiki.mozilla.org/Privacy_Icons_v0.2. Last Accessed: 2022-01-06.

[33] Sandra R. Murillo and J. Alfredo Sánchez. 2014. Enhancing Privacy Awareness Through Interaction Design. In *Proceedings of the XV International Conference on Human Computer Interaction* (Puerto de la Cruz, Tenerife, Spain). ACM, New York, NY, USA, Article 44, 4 pages.

[34] Jonathan A. Obar. 2016. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *SSRN Electronic Journal* (2016).

[35] Anna-Marie Ortloff, Lydia Güntner, Maximiliane Windl, Denis Feth, and Svenja Polst. 2018. Evaluation kontextueller Datenschutzerklärungen. In *Mensch und Computer 2018 - Workshopband*, Raimund Dachselt and Gerhard Weber (Eds.). Gesellschaft für Informatik e.V., Bonn.

[36] Anna-Marie Ortloff, Maximiliane Windl, Valentin Schwind, and Niels Henze. 2020. Implementation and In Situ Assessment of Contextual Privacy Policies. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (Eindhoven, Netherlands) *(DIS '20)*. ACM, New York, NY, USA, 1765–1778.

[37] Preethy Pappachan and Martina Ziefle. 2008. Cultural influences on the comprehensibility of icons in mobile–computer interaction. *Behaviour & Information Technology* 27, 4 (2008), 331–337.

[38] European Parliament and Council of European Union. 2016. *General Data Protection Regulation. Regulation (EU) 2016/679.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

[39] Anand Paturi, Patrick Gage Kelley, and Subhasish Mazumdar. 2015. Introducing privacy threats from ad libraries to android users through privacy granules. In *Proceedings of NDSS Workshop on Usable Security (USEC'15)*, Vol. 1. Internet Society, 2–1.

[40] Privacy Tech. 2018. Privacy Icons. https://www.privacytech.fr/privacy-icons/. Last accessed: 2022-01-06.

[41] Aza Raskin. 2011. Privacy Icons: Alpha Release. http://www.azarask.in/blog/post/privacy-icons/. Last Accessed 09-December-2019, still accessible here https://web.archive.org/web/20190302212004/http://www.azarask.in:80/blog/post/privacy-icons/; images also at https://www.flickr.com/photos/azaraskin/5304502420.

[42] Joel R. Reidenberg, Travis Breaux, Lorrie Carnor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, and Florian Schaub. 2014. Disagreeable Privacy Policies: Mismatches Between Meaning and Users Understanding. *Berkeley Technology Law Journal* 30, 1 (2014).

[43] George Robertson, Mary Czerwinski, Kevin Larson, Daniel C. Robbins, David Thiel, and Maarten van Dantzich. 1998. Data Mountain: Using Spatial Memory for Document Management. In *Proceedings of the 11th Annual ACM Symposium on User Interface Software and Technology* (San Francisco, California, USA) *(UIST '98)*. ACM, New York, NY, USA, 153–162.

[44] Arianna Rossi and Monica Palmirani. 2019. Dapis: An ontology-based data protection icon set. *Frontiers in Artificial Intelligence and Applications* 317 (2019), 181–195.

[45] Arianna Rossi and Monica Palmirani. 2020. Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection. *Design Issues* 36, 3 (2020), 82–96.

[46] Kanthashree Mysore Sathyendra, Shomir Wilson, Florian Schaub, Sebastian Zimmeck, and Norman Sadeh. 2017. Identifying the Provision of Choices in Privacy Policy Text. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing.* 2774–2779.

[47] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 1–17.

[48] Julia Schwarz and Meredith Morris. 2011. Augmenting Web Pages and Search Results to Support Credibility Assessment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. ACM, New York, NY, USA, 1245–1254.

[49] Barry Smyth, Jill Freyne, Maurice Coyle, Peter Briggs, and Evelyn Balfe. 2004. I-SPY — Anonymous, Community-Based Personalization by Collaborative Meta-Search. In *Research and Development in Intelligent Systems XX*, Frans Coenen, Alun Preece, and Ann Macintosh (Eds.). Springer London, London, 367–380.

[50] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 2011. On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on SSL Warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. ACM, New York, NY, USA, Article 3, 18 pages.

[51] Statcounter - GlobalStats. 2022. Desktop Browser Market Share Germany. http://gs.statcounter.com/browser-market-share/desktop/germany. Last accessed: 2022-01-06.

[52] Karen L. Stephan, Sean E. Smith, Russell L. Martin, Simon P. A. Parker, and Ken I. McAnally. 2006. Learning and Retention of Associations Between Auditory Icons and Denotative Referents: Implications for the Design of Auditory Warnings. *Human Factors* 48, 2 (2006), 288–299.

[53] Eric Stilan, Amy Chen, and Lulit Bezuayehu. 2011. Accessible Icon Design in Enterprise Applications. In *Proceedings of the International Cross-Disciplinary Conference on Web Accessibility* (Hyderabad, Andhra Pradesh, India) *(W4A '11)*. ACM, New York, NY, USA, Article 11, 4 pages.

[54] Latanya Sweeny. 2002. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 05 (2002), 557–570.

[55] Jaime Teevan, Edward Cutrell, Danyel Fisher, Steven M. Drucker, Gonzalo Ramos, Paul André, and Chang Hu. 2009. Visual Snippets: Summarizing Web Pages for Search and Revisitation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) *(CHI '09)*. ACM, New York, NY, USA, 2023–2032.

[56] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research* 22, 2 (2011), 254–268.

[57] Matthew W Vail, Julia B Earp, and Annie L Antón. 2008. An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management* 55, 3 (2008), 442–454.

[58] Susan Wiedenbeck. 1999. The use of icons and labels in an end user application program: An empirical study of learning and retention. *Behaviour & Information Technology* 18, 2 (1999), 68–82.

[59] Shomir Wilson, Florian Schaub, Aswarth Abhilash Dara, Frederick Liu, Sushain Cherivirala, Pedro Giovanni Leon, Mads Schaarup Andersen, Sebastian Zimmeck, Kanthashree Mysore Sathyendra, N Cameron Russell, et al. 2016. The creation and analysis of a website privacy policy corpus. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers).* 1330–1340.

[60] Jacob O. Wobbrock, Leah Findlater, Darren Gergle, and James J. Higgins. 2011. The Aligned Rank Transform for Nonparametric Factorial Analyses Using Only ANOVA Procedures. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '11)*. ACM Press, New York.

[61] Christian Wolff and Stefanie Götzfried. 2009. "I can"-Design: Methodik für das benutzerzentrierte Design nicht-standardisierter Icons. In *Tagungsband UP09*, Henning Brau, Sarah Diefenbach, Marc Hassenzahl, Kirstin Kohler, Franz Koller, Matthias Peissner, Kostanija Petrovic, Meinald Thielsch, Daniel Ullrich, and Dirk Zimmermann (Eds.). Fraunhofer Verlag, Stuttgart, 119–125.

[62] Kuang-Wen Wu, Shaio Yan Huang, David C. Yen, and Irina Popova. 2012. The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior* 28, 3 (2012), 889–897.

[63] Sicong Zhang, Hui Yang, and Lisa Singh. 2016. Anonymizing Query Logs by Differential Privacy. In *Proceedings of the 39th International ACM SIGIR Conference on Research and Development in Information Retrieval* (Pisa, Italy) *(SIGIR '16)*. ACM, New York, NY, USA, 753–756.

[64] Steven Zimmerman, Alistair Thorpe, Chris Fox, and Udo Kruschwitz. 2019. Investigating the Interplay Between Searchers' Privacy Concerns and Their Search Behavior. In *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval* (Paris) *(SIGIR'19)*. ACM, New York, 953–956.