Research Article

Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services

—Susanne Barth, Dan Ionita, Menno D. T. de Jong, Pieter H. Hartel, and Marianne Junger

***Abstract*—Background:** *Many countries mandate transparency and consent when personal data are handled by online services. However, most users do not read privacy policies or cannot understand them. An important challenge for technical communicators is empowering users to manage their online privacy responsibly.* **Literature review:** *Research suggests that privacy visualizations may alleviate this problem, but existing approaches are incomplete and under-researched.* **Research questions:** *1. How can we design a privacy rating that optimally empowers users with different levels of knowledge about and awareness of online privacy? 2. How do users react to such a privacy rating, in terms of usability, perceived usefulness, and trust in online services?* **Methodology:** *We developed Privacy Rating, a tool for mapping and visualizing the privacy of online services. The tool was subjected to user research (N = 30) focusing on usability, perceived usefulness, and effects on trust. To establish the effects on trust, participants were exposed to a website with either a positive or a negative privacy rating.* **Results:** *The Privacy Rating appeared to be usable and useful for lay users, and it had a significant effect on users' trust in the online service. Users indicated that they would like the visualization to become an established standard, preferably approved by an independent organization.* **Conclusions:** *The Privacy Rating is a user-friendly privacy visualization covering all relevant aspects of privacy. We aim to bring the tool to the market and make it a standard, ideally supported by an independent trustworthy organization.*

Index Terms*—Online privacy, privacy rating, privacy visualization, usability, user-centered design.*

Imagine giving a complete stranger your address and phone number, the contact information of everyone you know, unlimited access to your photos, a detailed account of your media use, all your private messages, and real-time updates on your whereabouts. It sounds extreme, but most of us risk doing just that every day—simply by using online services. Online services ranging from social media and entertainment to shopping and banking continuously handle large amounts of our personal information. The pervasiveness of digital media in modern life has resulted in a semantic web built almost entirely on personal data [1].

Using online services inevitably requires making decisions about disclosing personal data. Disclosures may have adverse consequences such as misuse, spam, or identity theft [2]–[4]. However, due to the complex, multifaceted, and intangible nature of online privacy, the vast majority of users have difficulty judging potential privacy risks and safeguarding their privacy [5], [6]. Privacy policies detail how online services handle user data, but because they are long and complex, few users try to read them, and those few face difficulties understanding them [7]–[11]. Furthermore, an analysis of privacy statements showed that such disclaimers often place little emphasis on providing users with clear-cut information designed to aid the decision-making process. In fact, self-interest and the desire to avoid litigation have much higher priorities among most online service providers [12].

The complex, multifaceted, and intangible nature of online privacy may amplify the cognitive biases that users already have, including optimism bias (underestimating the risks of unsafe behaviors), status quo bias (exhibiting an affinity for default choices), app desirability bias (adjusting privacy concerns based on the attractiveness of the app), and anchoring (taking other users' behaviors as a reference point) [13], [14]. A recent study showed that, in line with Festinger's cognitive dissonance theory [15], users tend to consider privacy less important when they think that they are not in control [6].

Online privacy does not occupy a prominent position on the research agenda in technical and professional communication, with very few research articles in the last 15 years devoted to the

Manuscript received January 9, 2021; revised April 29, 2021; accepted April 30, 2021. Date of publication November 11, 2021; date of current version November 24, 2021.
(Corresponding author: Menno D. T. de Jong.)
The authors are with the University of Twente, 7500 AE Enschede, the Netherlands (email: s.barth@utwente.nl; d.ionita@utwente.nl; m.d.t.dejong@utwente.nl; pieter.hartel@utwente.nl; m.junger@utwente.nl).

IEEE 10.1109/TPC.2021.3110617

Practitioner Takeaway

- This study describes the design and evaluation of a privacy visualization aimed at empowering users to manage and protect their online privacy responsibly.
- Functional complexity is a major design challenge: Empowering users implies making them aware of privacy risks and giving them shortcuts, as well as access to more detailed information in a clear, concise, and intuitive design.
- User research shows that the Privacy Rating fulfills the needs of users: It is usable and useful and significantly affects users' trust in online services.
- A mechanism for an objective third party to evaluate or certify the privacy visualization for online services is highly desirable.

topic [16], [17], none of which address the challenge of empowering users to act in accordance with their own privacy interests. We believe that online privacy deserves more attention within our discipline because it is an increasingly prominent and inherently complex aspect of the interaction between humans and technology, and could benefit from the verbal and visual communication competencies that typically define the strength of our discipline.

When it comes to empowering users to assume informed responsibility for their online privacy, many researchers have drawn attention to the potential of using privacy labels, visually depicting the threats to privacy associated with online services [18]–[34]. In fact, the European General Data Protection Regulation (GDPR) mandates standardized icons to provide an overview of the intended data processing [35]. In this article, we describe the development and evaluation of the Privacy Rating, a new privacy visualization that we have developed for online services. The label is the result of a research-based inventory of important privacy risks. It includes an efficient tool for mapping privacy features and is designed to raise privacy awareness among nonengaged users and to provide relevant, well-organized information to users who are already concerned about privacy. After a literature review, we describe the privacy label and its rationale before reporting on the design and results of a user test that focused on its usability, perceived usefulness, and effects on users' trust in an online service.

Literature Review

Why is There a Need to Visualize Privacy?

Although users claim to care about their online privacy and have concerns about privacy violations, they generally do not behave accordingly. They download apps, give permissions, and provide personal information without much thought about the potential ramifications of their actions. This discrepancy between attitude and behavior is known as the "privacy paradox" [36]. Research shows that there may be three underlying mechanisms.

1. Users rationally weigh the benefits of downloading an app, giving permissions, or providing personal information against the associated privacy risks.
2. Users have trouble weighing costs and benefits, and instead rely on (possibly biased) heuristics or cognitive shortcuts.
3. Users do not even consider the privacy aspects of downloading an app, giving permissions, or providing certain information [37].

The distinction between these mechanisms may not always be clear in practice. Through their behavior, users put themselves at unnecessary risk. The current situation is a vicious cycle. Virtually all privacy policies are complex and "take-it-or-leave-it." Therefore, individual users have no real choice but to accept online services on their (unclear) terms, a situation that panders to the strategies of many service providers. Although online privacy is a topic of vivid discussions in the academic literature, in practice, it is often reduced to momentary feelings of unease and uncertainty in users.

Designers and providers of online services are in the best position to make data handling processes more transparent to users. Since the end of the last century—even before the introduction of smartphones—researchers have advocated for and worked on a Privacy-by-Design paradigm [38], [39]. Its basic premise is that privacy should be incorporated into the fabric of online services instead of "bolting it on" after the fact. Many Privacy-by-Design standards and guidelines have emerged, (e.g., ISO/IEC 29100:2011) [40].

Although this approach can make a tremendous contribution to users' online privacy, several authors have warned of legal and practical complications [41], [42], as well as problems of adoption and implementation [43]–[45].

In practice, many providers of online services still try to discourage users from exercising their rights to privacy [46]. In addition, a core characteristic of online services is personalization which, by definition, involves some degree of personal data processing. Research shows that different users may have different tolerances of specific data handling practices [47].

Another solution would be empowering users to consciously take more responsibility for their online privacy. This could entail increased education: providing users with more knowledge about the business models of online services, the potential privacy risks of transactions, the exact meanings of permissions, and the best protection methods. However, research suggests that general knowledge and privacy awareness play no significant role in the privacy paradox: Advanced computer science students and even privacy and security experts appear to struggle with the same issues as lay users, exhibiting similarly unsafe behaviors [48], [49].

From a document design perspective, there may be a lot to gain from better information about privacy risks. Given the shortcomings of current privacy statements [7]–[12], some researchers investigated whether or not textual improvements could help. An experimental study showed that merely simplifying privacy statements based on document design principles does not affect users' comprehension, attitudes, or behavior [50]. On the other hand, another experimental study showed that concise and simple privacy warnings do have an effect on users' risk perceptions and online behavior [51].

Beyond their legal jargon and complexity at the word-, sentence-, and paragraph-level—all severe problems in their own right—privacy statements generally represent an intimidating information overload that does little to align with the perspective of users trying to ascertain whether to use an online service or not. It seems important to realize that there is functional complexity involved when communicating privacy risks [52], [53]. Ideally the same privacy information should do the following:

1. Raise users' awareness of the importance of privacy and privacy risks [54], [55]
2. Provide less engaged users with a shortcut to support their decision-making about the potential privacy risks associated with using an online service
3. Provide highly engaged users with user-friendly and comparable information about privacy risks (with varying levels of detail, depending on their interests and expertise)

Privacy visualizations, as advocated and developed by several researchers [18]–[34], may be a viable way to address this communication challenge. More than verbal information, visualizations can draw the attention of users who are not aware of privacy risks [24], [33], [56] and force service providers to translate complex privacy information into manageable, standardized privacy information.

Earlier Attempts to Visualize Online Privacy

Developing a privacy visualization requires two related activities: an intrinsic analysis of the relevant privacy aspects to be included and a verbal-visual communication design. Both in the academic literature and in practice, many attempts have been made to develop privacy visualizations (see Barth et al. [57] for an overview). Table I summarizes 14 earlier attempts, with special attention to the extent to which the systems provide overall advice about the privacy risks of online services (overall indicator) and detailed information about specific privacy aspects (privacy details).

Existing privacy visualizations operationalize privacy information quite differently [34], [57]. Barth et al. [57] investigated operationalizations of online privacy that manifest themselves in Privacy-by-Design guidelines and privacy visualizations, resulting in the following 15 different privacy aspects:

- Accountability
- Anonymization
- Collection
- Control
- Correctness
- Disclosure
- Functionality
- Purpose
- Pseudonymization
- Retention
- Right to be forgotten
- Sale
- Security
- Sharing
- Transparency

TABLE I
OVERVIEW OF EARLIER PRIVACY VISUALIZATIONS

Year	Source	Name	Type	Overall Indicator	Privacy Details
2007	[58]	Mehldau's data privacy declarations	Icons with tags	No	Yes
2009	[18], [19]	CyLab's privacy nutrition label	Table	No	Yes
2009	[59]	KnowPrivacy's policy coding	Icons with tags	No	Yes
2010	[60]	Mozilla's privacy icons	Icons	No	Yes
2010	[20], [21], [61]	PrimeLife privacy icons	Icons	No	Yes
2011	[62]	TrustArc's privacy short notice	Icons	No	Yes
2012	[22]	Privacy wheel	Privacy label	Yes	Yes
2014	[23], [25]	GDPR's draft privacy icons	Icons	No	Yes
2017	[28]	Data controller indicators	Data flow representation	No	Yes
2018	[29]	Renaud and Shepherd's privacy summary	Summary supported by icons	No	Yes
2018	[31]	Fox et al.'s GDPR compliant privacy label	Summary supported by icons	No	Yes
2019	[26], [27]	Data protection icon set (DaPIS)	Icons with tags	No	Yes
2019	[63]	Clever°Franke's privacy label	Privacy label	Yes	Yes
2020	[64]	Privacy label	Summary supported by icons	No	Yes

None of these privacy aspects were incorporated in each of the reviewed privacy visualizations. Three privacy aspects were quite prominent—types of data collection, purposes of data collection, and data sharing—with only one or two visualizations missing out on them. But the overall focus of the visualizations differed considerably. No agreed-upon framework of relevant privacy aspects of online services currently exists. A new privacy visualization should thus be based on a systematic analysis of relevant aspects of online privacy.

Various types of visualizations can be distinguished. Seven of the 14 visualizations listed in Table I are sets of icons expressing specific privacy characteristics. Several authors have argued that it is difficult to visualize such intangible and complex features [22], [25], [65], and several icons that were developed proved to be problematic in user tests [20], [61]. As a result, some of the icon sets use supporting tags to assist with the interpretation of visual cues. A significant drawback of icons is that they are limited to depicting specific privacy risks, thus making them unsuitable for providing users with the bigger picture, which is necessary if they are to make informed decisions about the acceptability of the combined privacy risks.

Three of the proposed visualizations downplay the role of icons by making them merely supportive for predominantly written information. In these cases, the icons have no independent meaning but only visually support the structure of a summarized privacy text. Again, it is questionable whether this approach supports users in their decisions about the combined privacy risks of online services. The difficult task of making sense of the various privacy characteristics and translating those insights into an overall judgment about privacy risks is still entirely the users' responsibility.

Two other visualizations explore very different directions. Inspired by the nutrition labels on food, Kelley and colleagues developed a privacy nutrition table, which actually consists of a listing of 10 types

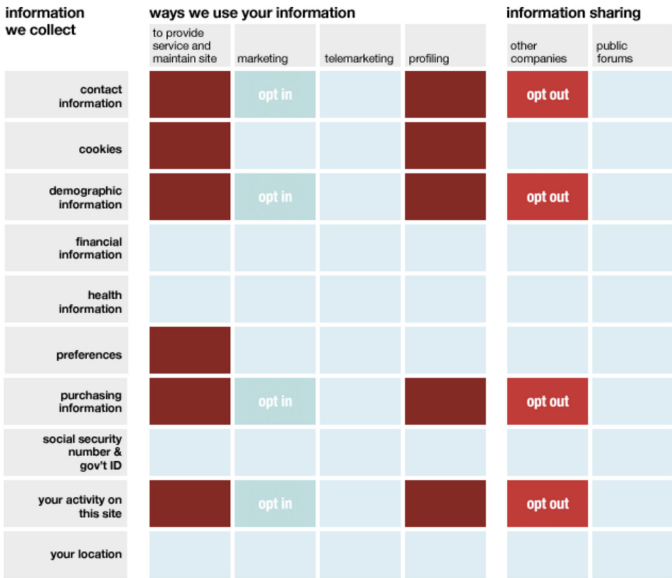

Fig. 1. Kelley et al.'s privacy nutrition label [18], [19].

Fig. 2. Van den Berg and Van der Hof's privacy wheel [22].

of user data, five types of data handling, and two different parties handling the data (see Fig. 1). In each cell of the table, four options may be entered (yes, no, opt out, and opt in) [18], [19]. The analogy with nutrition labels already suggests that the visualization does not attract less-engaged users and does not support users' overall decisions about whether privacy risks are acceptable or not. Still, a focus group study showed that users appreciated the system [18], and a comprehensive experiment showed that the label, compared to normal privacy statements, helped users to better understand the privacy aspects of online services [19].

Van Kleek et al. developed a visualization of the data flows from online services [28]. Although the resulting graphs were advanced and may be too complex to be intuitively comprehensible, a small-scale experimental study indicated that the visualization, more than written privacy information, helped users make informed decisions regarding online privacy.

Finally, two proposals for visualizations take the form of privacy ratings, providing overall indications of the privacy aspects of online services with optional in-depth information. Van den Berg and van der Hof's privacy wheel (see Fig. 2) consists of an overall privacy qualification in the middle surrounded by eight brightly colored clickable aspects of privacy [22]. Although it manages to combine an overall privacy assessment and more detailed information, the visualization has a few potential drawbacks: The overall privacy assessment in the middle might be easily overlooked, it lacks a reference point, and it is not transparently related to the eight specific privacy aspects.

Clever Franke's privacy label (see Fig. 3) is inspired by the letter classification (A-F) and color use of the EU energy label [63]. It consists of a colored circle with a privacy qualification in the middle: An A (in green) is positive; an F (in red) is negative. Around the qualification, there is a circle divided into three equal parts representing three privacy aspects: data usage, data collection, and user control. For every aspect, five questions are asked. For positive answers, the line is colored; for negative answers, it is left white. The thicker the colored circle around the privacy qualification, the more positive the online service scores on the specific privacy aspects. Users can use a quick response (QR) code for more specific information. Drawbacks of this visualization are that the specific privacy information is hidden in the design, and the system of five questions in three parts of the circle may not be clear to users.

No research reports are available on user tests with either of these two privacy labels.

Research Questions

In this article, we describe a project developing a Privacy Rating tool for online services that is

Fig. 3. Clever Franke's privacy label [63].

founded upon expert knowledge of the relevant privacy aspects and that is designed to overcome the shortcomings of earlier privacy visualizations. Furthermore, we describe a user study of the proposed visualization that focuses on usability, perceived usefulness, and effects on user trust. We investigate the following research questions.

RQ1. How can we design a Privacy Rating tool that optimally empowers users with different levels of knowledge about and awareness of online privacy?

RQ2. How do users react to such a Privacy Rating tool, in terms of usability, perceived usefulness, and trust in online services?

Methodology

A user-centered privacy visualization must be both useful (contain the right information) and usable (present the information in an understandable way). Therefore, our methodology is two-fold. First, we report on the development of the Privacy Rating visualization. At the core of the proposed visualization lies a set of 12 privacy metrics that not only provide the basic structure and content of the privacy visualization, but also serve as input for the rating system. Second, as a part of an iterative design process, we evaluated the visualization with potential users.

Privacy Rating Below, we describe the development of the Privacy Rating visualization and discuss its three main characteristics: content, visual design, and generating the Privacy Rating.

Content: The development of the Privacy Rating started with a thorough and systematic analysis of the privacy aspects of online services that should be deemed relevant and therefore included. We took the list of 15 privacy attributes gathered in earlier research [57] as our starting point (see Table II). The attributes were based on established Privacy-by-Design guidelines and earlier privacy visualizations. Research with experts and users confirmed the importance of all attributes [57].

We decided to exclude two of the original attributes for our visualization. The functionality aspect was removed because it was ambiguous and overlapped with control. Transparency was removed because having a Privacy Rating can already be seen as a positive indicator of transparency in itself. In addition, anonymization and pseudonymization were combined into one attribute because they were sometimes difficult to distinguish: pseudonymization can be seen as incomplete anonymization. From previous research, we know that privacy is subjective and context-dependent [47], [66], [67]. Therefore, we decided to use all of the remaining 12 attributes as equally rated metrics for our rating system.

Because differentiating 12 different privacy attributes is not manageable for users, we conducted a card-sort study in which we asked users to cluster the 12 attributes. Most often, the attributes were grouped into four categories. Although security turned out to be a clear group label, there was disagreement about the others. Consulting 10 privacy and cyber security experts from our network resulted in four main clusters: collection, sharing, control, and security (see Table III).

To use the metrics for rating and comparing online services, they must be operationalized. To keep the system simple and understandable for users, we defined three-point scales (good-neutral-bad) for each attribute. In iterative sessions with privacy and cyber-security experts, we arrived at the operationalized metrics presented in Table III. Online services receive penalty points depending on their score on each metric (0 points for good scores, 1 point for neutral scores, and 2 points for bad scores).

TABLE II
PRIVACY ASPECTS CONSIDERED FOR THE PRIVACY RATING [57]

Privacy Aspect	Description
Accountability	Can the service provider be held accountable for violations?
Anonymization**	Are all identifiable markers completely removed so that data can never be traced back to individual users?
Collection	Which user data are collected?
Control	Are users able to choose or decide which data to share for which purpose, and how difficult is it to do so?
Correctness	Are there mechanisms for preventing and fixing incorrect data?
Disclosure	What is the provider's attitude towards data requests from law enforcement?
Functionality*	Are users forced to choose between functionality and privacy?
Pseudonymization**	Are personally identifiable markers replaced by artificial identifiers, or pseudonyms, so that data can only be traced back to individual users with the help of additional information?
Purpose	What are the collected data used for?
Retention	How long are collected data stored?
Right to be forgotten	Can users request that all their personal data will be removed?
Sale	Are any of the data sold to third parties?
Security	Which technical measures are taken to ensure that data are protected from unauthorized or malicious access?
Sharing	Do any of the collected data leave the ownership of the provider?
Transparency*	Are users able to obtain information about how their personal data are handled?

Note: $*$ = Removed from the *Privacy Rating* attributes; $**$ = Collapsed into one attribute.

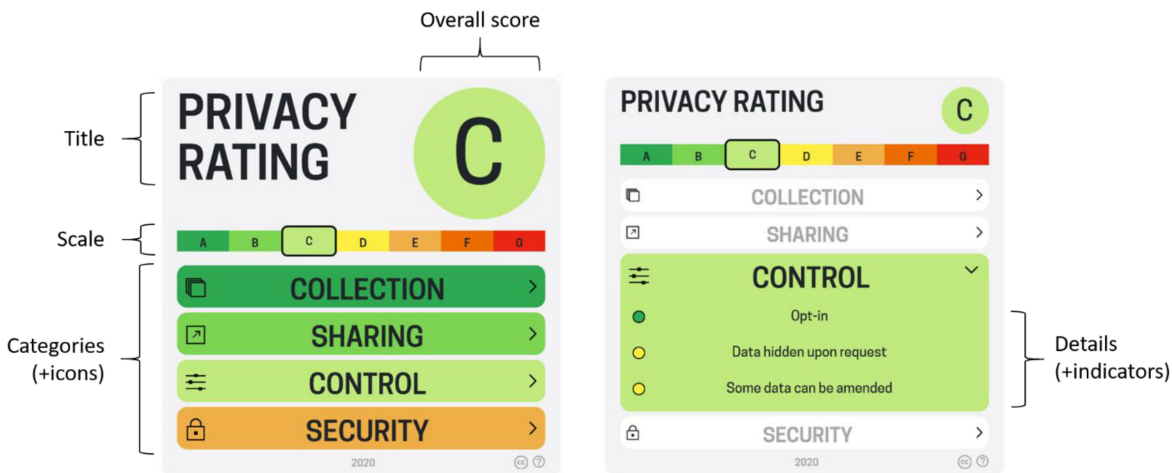

Fig. 4. Design of Privacy Rating.

The total number of penalty points is then used to categorize online services into seven classes, from A (lowest privacy risks) to G (highest privacy risks):

- Class A: 0 or 1 points
- Class B: 2 to 5 points
- Class C: 6 to 9 points
- Class D: 10 to 13 points
- Class E: 14 to 17 points
- Class F: 18 to 21 points
- Class G: 22 to 24 points

Visual Design: Our Privacy Rating (see Fig. 4) was designed through an iterative process in collaboration with a professional design agency. Simplicity, clarity, recognizability, and attractiveness were important criteria throughout the design process. With its stable and marked overall design, the visualization has the potential to draw attention to privacy issues across different online services. The use of overall privacy classes helps less-engaged users to make a quick overall

TABLE III
CLUSTERED AND OPERATIONALIZED PRIVACY ATTRIBUTES

Cluster	Attribute	Operationalization
Collection	Collection	0 - Collects anonymous data
		1 - Collects personal data, relating to an identified or identifiable person
		2 - Collects sensitive data, involving racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership, genetic or biometric data, health status, or sexuality and sexual orientation
	Purpose	0 - Used for functionality only
		1 - Used for customization (personalization in the current interaction)
		2 - Used for profiling
	Retention	0 - Data not stored
		1 - Data stored for a pre-determined limited time
		2 - Data stored indefinitely
Sharing	Sharing	0 - No sharing of user data
		1 - Sharing of anonymous user data
		2 - Sharing of user data
	Sale	0 - No sale of user data
		1 - Sale of anonymous user data
		2 - Sale of user data
	Disclosure	0 - Statutory disclosure to local law enforcement (inside user's jurisdiction)
		1 - Disclosure to local law enforcement (outside user's jurisdiction)
		2 - Disclosure to foreign law enforcement
Control	Control	0 - Opt-in (users must explicitly opt-in to allow data collection)
		1 - Opt-out (data are collected by default, but users can opt-out)
		2 - No opt-in or opt-out
	Right to be forgotten	0 - Data deleted upon request
		1 - Data hidden upon request
		2 - Data cannot be removed
	Correctness	0 - All data can be amended
		1 - Some data can be amended
		2 - Data cannot be amended
Security	Security	0 - Industry standard security (certified compliant with the latest version of either ISO 27001 or NIST 800-53)
		1 - Basic security (developed in compliance with the OWASP Top 10 standard and tested according to the OWASP Application Security Verification standard or the OWASP Mobile/Web Security Testing Guide or equivalent)
		2 - None of the above
	Anonymization	0 - Anonymous (all identifiable markers are completely removed so that collected data can never be traced back to individuals)
		1 - Partially anonymous (personally identifiable information fields within collected data are replaced by artificial identifiers or pseudonyms, so that data can only be traced back to individuals with additional information)
		2 - Not anonymous (personally identifiable information is stored)
	Accountability	0 - Legally accountable
		1 - Legally binding privacy policy
		2 - Not legally accountable

Note: 0-2 represents the number of penalty points for each alternative.

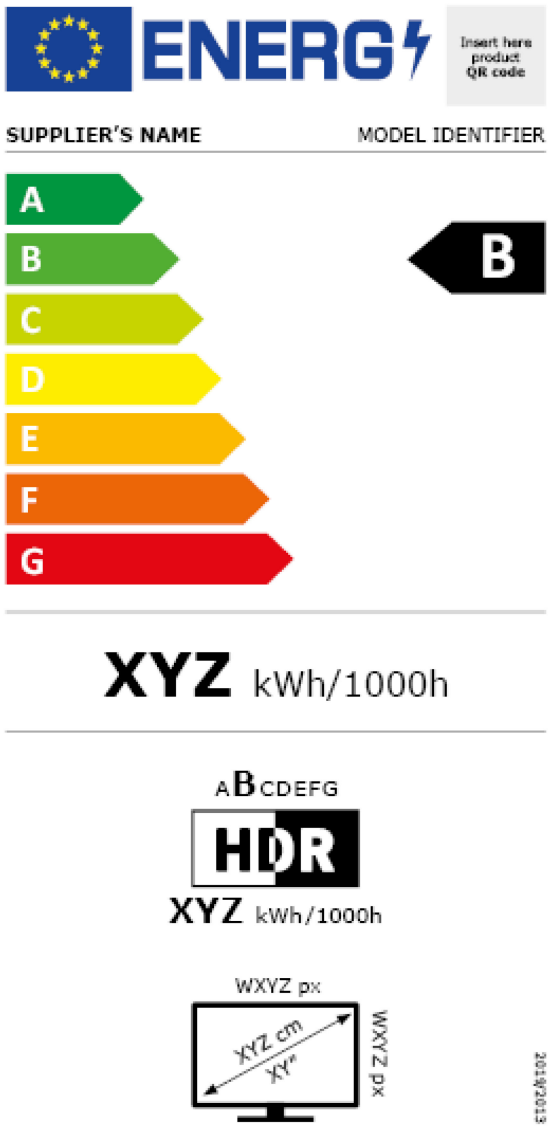

Fig. 5. Template of the European energy label for electronic displays [68], [69].

judgment about the potential privacy threats of online services. As with the familiar European Union energy label (see Fig. 5) [68], [69], privacy classes are indicated by combinations of letters and colors (ranging from A plus green for the most positive online services; to G plus red for the most negative ones). The colors also reflect the conventional color scheme of traffic lights. The presence of a full scale helps users to interpret the score of a particular online service.

Users who are more engaged with online privacy are helped with two levels of additional specific information. The first level, immediately obvious in the visualization, is the scores of the online service in the four main categories of privacy aspects (collection, sharing, control, and security), which can have different colors depending on the specific score for each one. Each category is listed with its name and an icon. The second level, which can be reached by hovering over or clicking the main categories, provides more detailed information about specific aspects of privacy.

Generating Privacy Rating: To promote the practical feasibility of the Privacy Rating, we developed a self-assessment form in a free web application (www.privacyrating.info). This form enables providers of online services to create their own tailor-made privacy label corresponding to the data handling practices of their online service. The application is designed to walk service providers through a questionnaire with each question corresponding to one of the three levels of each attribute. The questionnaire is interactive: Once the answer to a question confirms the level of an attribute, the remaining questions corresponding to that attribute are skipped, and the service provider is directed to questions about the next attribute. When all 12 attributes have been evaluated, the application computes the Privacy Rating and creates a visualization in two formats: an HTML and a smaller PNG version, both of which can be embedded into webpages or apps. The small version can be added to the footer of the page or to the cookie notice. The larger version can be included in the privacy policy or as a pop-up.

Research Design of the User Study To evaluate the potential value of the Privacy Rating, we conducted a user study. In this early phase of development, we focused on the following three aspects of the privacy label:

- Usability
- Perceived usefulness
- Effect on users' trust in an online service

Because of the COVID-19 pandemic, data collection took place in individual online sessions. The study was approved by the Ethical Committee of the Electrical Engineering, Mathematics and Computer Science faculty of the University of Twente.

Participants: Participants were recruited in three complementary ways:

- From the university's research participants pool
- From a commercial research participants pool
- Via social media

Participants from the university's pool received participant credits required by their study

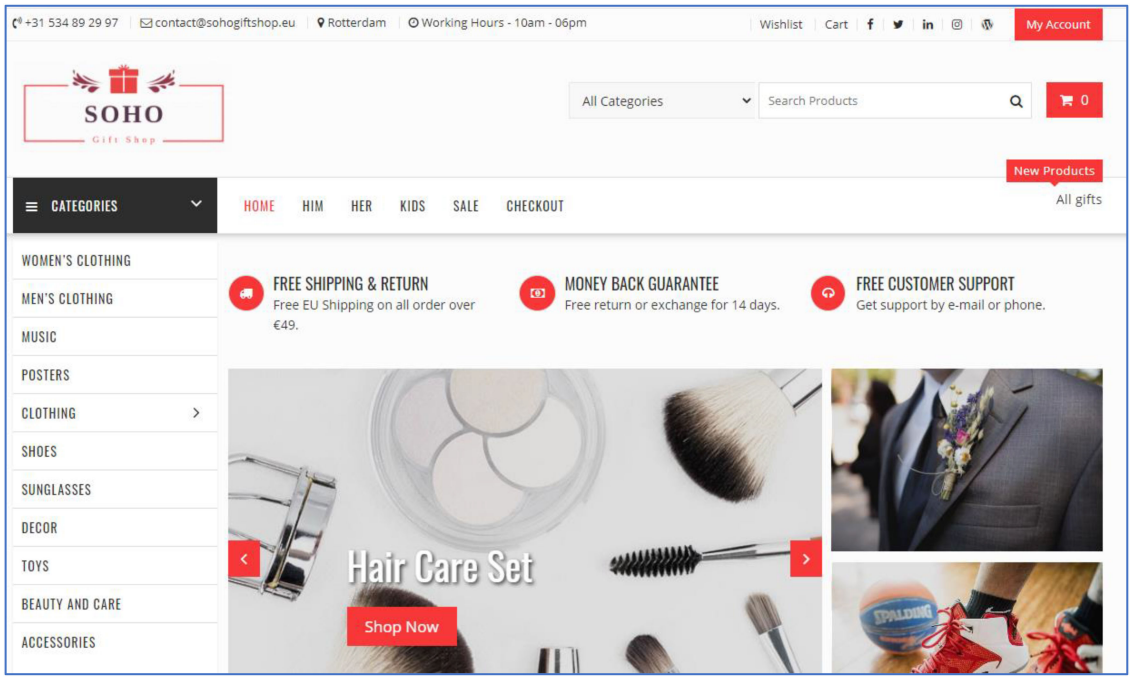

Fig. 6. Screenshot of the web shop for the user study.

programs, participants from the commercial pool received a monetary compensation, and participants from social media volunteered to participate without compensation. In our recruitment messages, we called for participants aged 18 or older, with good English proficiency and access to a Google Chrome browser, a web cam, and a microphone.

A total of 30 participants took part in the study. Participants had a mean age of 28.6 years (ranging from 19 to 62). Their gender distribution was equal. Participants' educational level varied from medium (high school or vocational education: 53%) to high (bachelor, master, and PhD: 47%). Of the sample, 60% currently followed a study program, and 57% had a job. Study programs and occupations were quite diverse. Three participants had a background in cyber security or online privacy. All participants lived in Europe, most of them coming from Germany or the Netherlands. A large majority of the participants had ample experience with online tools such as email, search engines, instant messaging, social media, and teleconferencing (all 93% or higher) and with online transactions such as online banking, streaming, and shopping (all 87% or higher).

Research Materials: To evaluate the Privacy Rating in a realistic setting, we built an online web shop (see Fig. 6), using a real, SSL-protected domain (www.sohogiftshop.eu). The web shop used a prebuilt, highly rated WordPress theme. Offerings (including photos, descriptions, and prices) were selected across a broad range of product types. To prevent unintended visitors, the web shop was password protected. Participants received the password at the beginning of their session.

The web shop's Privacy Rating was included as a pop-up that appeared when users opened the homepage. Before interacting with the site, users had to click away the pop-up. The shop's Privacy Rating was also included at the bottom of the homepage, and a small version was added to the footer of every page (see Fig. 7).

To investigate the effects on participants' trust in an online service, two versions of the Privacy Rating were used: Half of the participants were exposed to the web shop with a moderately positive Privacy Rating (grade B, predominantly green), and the other half were exposed to the web shop with a moderately negative rating (grade F, predominantly red).

Procedure: The research sessions consisted of two parts. Participants began with an online questionnaire in Qualtrics covering their background characteristics and the consent information. Background questions focused on age,

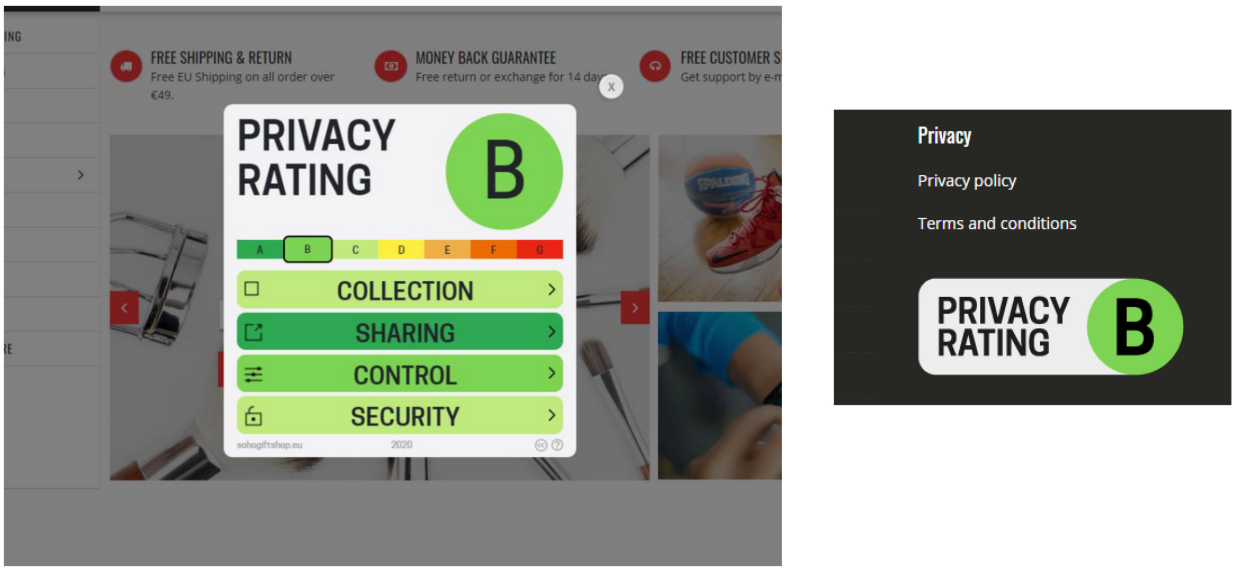

Fig. 7. Privacy Rating on the web shop, as pop-up (left) and as small label (right).

gender, country of residence, education, profession, use of online services, and expertise in online privacy and cyber security. After filling out all questions, participants received a link to a live session with one of the interviewers. In the live sessions, we used Lookback for real-time screen monitoring and interviewing. Participants were asked to install this software on their computers. In all sessions, two researchers were involved: one moderated the session and interviewed the participant; the other observed without interacting with the participant.

The session started with the following scenario-based task.

> You are looking for a gift for the birthday of your friend. You find some interesting gifts in an online gift shop you have never used before: the SOHO Gift Shop. To place an order, you must provide your first and last name, date of birth, gender, age, shipping and billing address, and credit card details. Try to determine whether you would trust this website with your personal information.

To avoid reactivity, we did not ask the participants to think aloud. However, their interactions with the Privacy Rating and the website were recorded and used in the analysis.

The task execution was followed by a semistructured interview, with questions covering the following three topics.

1. Trust in the website
   a. Decision whether to make a purchase
   b. Impression of the website
   c. First impression of the Privacy Rating
   d. Effects of the Privacy Rating on trust
2. Usability of the Privacy Rating:
   a. Name
   b. Overall rating
   c. Scale
   d. Main categories
   e. Detailed information about the categories
   f. Visual design
3. Usefulness of the Privacy Rating:
   a. Transparency (did it increase an understanding of data handling practices?)
   b. Behavioral intentions (would it affect decisions to trust online services?)
   c. Desirability (would the participant like to see it as an established standard?)

The sessions were videorecorded. Sessions lasted on average 24.4 minutes (SD = 8.3). At the end of the sessions, participants were thanked, debriefed, and given instructions for removing the Lookback extension from their browser.

Analysis All 30 interviews were transcribed verbatim, and any personal information that could be associated with participants was removed. The interview data were analyzed qualitatively in ATLAS.ti. Codes were based on the interview questions and emerged bottom-up based on participants' answers. Two independent researchers coded a random selection of 10% of the

transcripts and discussed the discrepancies in their coding. Based on the discussion, the coding scheme was refined. After that, the two researchers coded another sample of the transcripts. They reached sufficient intercoder agreement in general (Cohen's kappa = 0.85) and for the three main research topics: usability (0.87), perceived usefulness (1.0), and trust (0.78). Using this coding scheme, the remaining transcripts were then coded by the first author.

To investigate the effects of the Privacy Rating on participants' trust in the online service, the interviews were complemented with behavioral data: the amount of time participants spent looking at the Privacy Rating pop-up and their decision about placing an order in the web shop. For these behavioral data, we compared the results of the two experimental groups (positive versus negative Privacy Label).

Results

Usability

Name: Most participants (80%) found the name Privacy Rating clear and understandable and formulated correct expectations of its purpose: "It's really clear that this is about how safe a website is in terms of privacy." Others stated that they would not know immediately what the name "is trying to communicate." To come to a full understanding, they would have to see more. Interpreting the name in combination with the other elements helped them to "understand what they mean, what they tell you."

Overall Rating: Participants were generally positive (87%) about the clarity of the overall rating: "It's understandable enough to make me not want to share my information." For most participants, the color was important: "If there would be no color, it could be like, what does B mean? But green is always good and red is bad." Some participants related the overall rating to other familiar grading or rating systems: "the labels for energy consumption," "the American paper grading system," or "the alphabet; where the alphabet starts, the better it is." Participants with difficulties understanding the overall rating stated that the meaning became clearer when they also looked at other elements (for example, the colored scale).

Scale: Most participants (80%) found the scale clear: "A would mean that this is the best rating of privacy that you could have as a website, and G would be the worst." Some called the scale "intuitive" and "nothing to misunderstand." The use of colors makes it easy to interpret.

> A is green. So like a traffic light, green is good. Green, you go, you're safe to go. Yellow as well, you can go. … And then red is no, you don't go. Not very good.

Some participants stated that a scale without colors would be harder to understand. Others said that they needed a point of reference to interpret the scale. Interestingly, two participants expected that the scale would be interactive with clickable letters.

Main Categories: The four main categories (collection, sharing, control, and security) were clear to most of the participants, although some argued that the terms alone did not suffice and were understandable only when looking at the details corresponding to the categories. The categories collection and sharing were easiest to understand (93% and 87%, respectively). Control and security were somewhat less clear to the participants. Regarding control, several participants (77%) found the term "a bit vague" and "difficult to understand." Some thought it referred to the control service providers have—"maybe what the website can do remotely to your computer"—and did not see that it is meant to refer to the control users have regarding their personal data. Regarding security, participants (70%) found the term "a bit ambiguous" or "too general." Some thought that it involved only financial transactions: "Should I give my Visa number or should I use PayPal?"

Detailed Information: Most participants (63%) found the more detailed information underlying the four categories clear. Although participants appreciated the conciseness of the descriptions, some suggested adding more information because it "is very much open to interpretation depending on how much knowledge the individual has." Some participants found the wording too technical and would have appreciated explanations in "more human [layman's] words." Table IV summarizes the specific problems participants mentioned about the detailed information.

Visual Design Elements: Three participants found the separate colors used for the four categories confusing. One participant found the green color difficult to see against its background. Another

TABLE IV
PROBLEMS IDENTIFIED IN THE DETAILED INFORMATION

Collection	Sharing	Control	Security
What does "functionality" mean? (n = 4)	What does "legally required disclosure to local law enforcement" mean? (n = 5)	What does "opt-out" mean? (n = 7)	What does 'basic security' mean? (n = 2)
How long is stored for a limited time? (n = 3)	Is not sharing data realistic? (n = 1)	What does "amended" mean? (n = 2)	What does "industry-standard security" mean? (n = 2)
Which personal data does it collect? (n = 2)			"No anonymization" is a vague term (n = 1)
What does "data stored indefinitely" mean? (n = 1)			What does "legally accountable" mean? (n = 1)

participant understood this color scheme differently, stating that "sharing and using data is red. So I'm assuming that means that they don't share my data," whereas the color red actually means the opposite. In addition, three participants were confused that the categories expanded both automatically (when hovered over) and manually (when clicked).

Several participants (33%) did not realize that the indicators were ratings of the single statements. "The color of the overall rating and the color of the subcategories are the same. I did not notice that those are ratings." Another participant thought that the colored dots were "just simple bullet points that don't have any meaning." Especially the green dots were difficult to recognize "because the background is all green and the bullet points are all green."

The icons used to support the meaning of the four categories were correctly understood and appreciated by 44% of the participants. The other participants had difficulties with one or more of the icons. One participant questioned whether or not the icons are really necessary. The interactivity of the icons, intended to catch the user's attention, proved especially confusing for some participants.

> The fact that they move … I can get a little distracted and it makes it look a little less trustworthy to me and not necessarily helping me better understand what it is about.

Another participant assumed that the icons would be clickable and have a personalization function integrated.

In all, the usability evaluation yielded a positive overall impression as well as several suggestions to further optimize the Privacy Rating (see Fig. 8 for an overview). Some of the detailed problems mentioned with specific elements are actually solved when participants consider the complete visualization. However, the results revealed the need for more attention to the wording of categories and detailed information, with an important balance between clarity and conciseness. In addition, the participants mentioned several ambiguities in the visual design that deserve attention.

Perceived Usefulness Overall, participants were very positive about the Privacy Rating, one of them calling it "the most useful tool I've seen." The vast majority of participants (90%) considered the label to be an effective tool for visualizing how online services handle users' personal data.

> I think it's pretty good for a normal homepage because usually it's not so easy to find this information and I don't usually read all of it unless it's a new company.

The similarities to the existing EU energy label appeared to enhance the label's usefulness. "It reminds me a bit of when you buy a fridge and you get the label in terms of the efficiency levels." Some participants explicitly appreciated that the label was the first thing they saw when opening the website. "It gives a pretty clear overview. And it's also nice if I click on the website and it's right there."

Three participants were somewhat more critical, arguing that the information provided by the label only "gives an impression but not a full clear explanation of how this website is handling my data." Their objections involved the conciseness and clarity of the information, as discussed above.

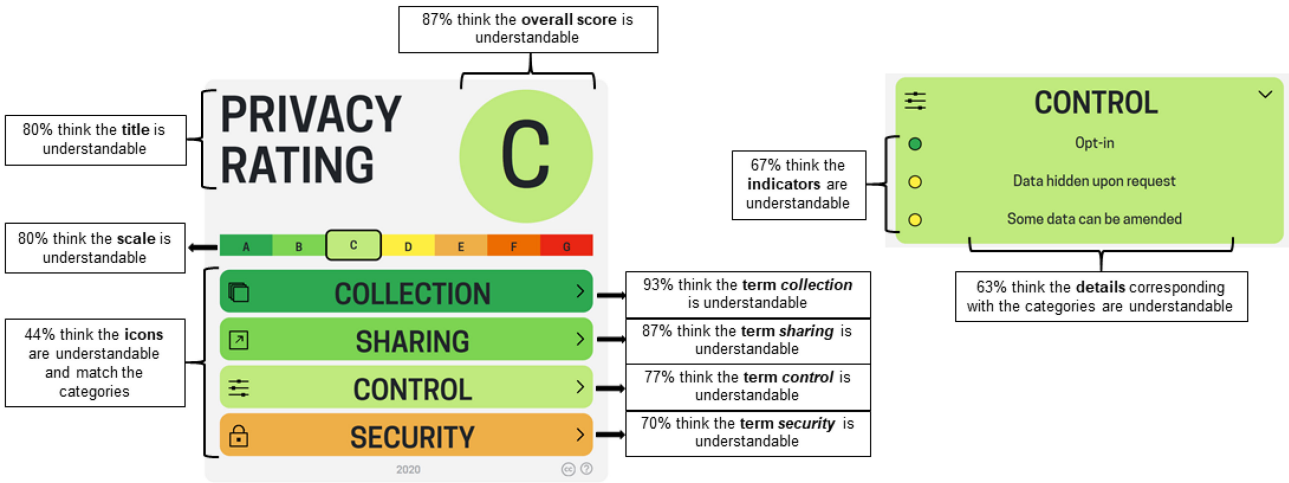

Fig. 8. Usability of the various elements of the Privacy Rating.

Most participants (83%) felt that the Privacy Rating would influence their decisions on trusting and using websites or other online services. They would appreciate such a label, especially when sharing sensitive data such as credit card details with an online service. The label would help them to judge unknown websites or compare services offering the same product. It makes evaluating online services less time-consuming and limits the role of subjectivity in their judgments. Interestingly, some participants argued that a negative rating would influence them more than a positive rating.

All 30 participants would like the Privacy Rating to become an established standard under the responsibility of an independent organization because such standardization would enhance people's awareness of online privacy and the risks of data sharing. It would also educate users, satisfy the needs of users who care about their personal data, and decrease vulnerability to fraud.

> I would be happy to see something like that on a website, generally. It would help educate people as to the good and the bad out of the internet, and shopping online and banking online. I surprised myself … how many online systems I actually use. I worked in IT, but I'd like to think of myself as being able to disconnect from it. But clearly not. Everything I do is connected to technology in some way.

Effects on Trust A first step in our analysis of the effects that the Privacy Rating had on participants' trust in the web shop involved the attention that participants paid to the pop-up. On average,

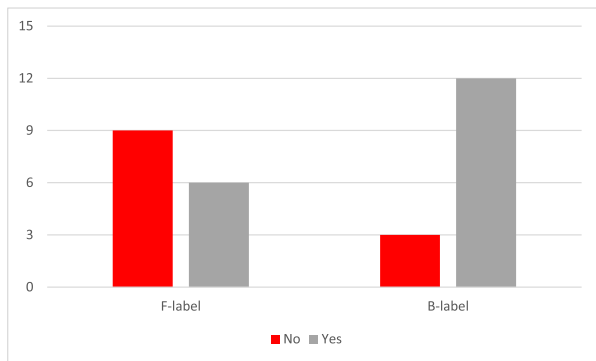

Fig. 9. Effects of the Privacy Rating on participants' decision whether to place an order.

participants spent 33.4 seconds ($SD = 18.5$) looking at the label (with a range between 6 and 78 seconds). There were no significant differences between the groups that had been exposed to a positive or negative label. In the interview afterwards, almost all participants (93%) indicated that they recognized the label; only two participants were not sure whether they had seen it.

A second step was to determine whether the label affected participants' online ordering decisions. A chi-square test showed that this was the case (χ^2 $(1, N = 30) = 5.0$, $p < 0.05$). In the group of participants exposed to the negative privacy rating, only 40% would place an order in the web shop, compared to 80% in the group of participants exposed to the positive rating (see Fig. 9).

Many participants indicated that a negative rating would influence them more than a positive one.

Indeed, participants who saw a negative rating displayed were less likely to place an order compared to those who were shown a positive rating. Furthermore, although a good Privacy Rating increased trust in the website for 66% of the participants, a bad rating decreased trust for 91% of the participants. This finding indicates that, in our sample, a negative rating had a greater influence on trust than a positive rating did.

From the interviews, two possible factors could be identified that might limit the effectiveness of the Privacy Rating. The first is that the pop-up format is not always appreciated. Some of the participants saw it as annoying and disturbing.

> I don't like websites where you have a pop-up straight away. …When I go to a landing page of a website, I want to have a look at the actual website and not deal with pop-ups.

The second is that the label is not yet officially established and therefore unfamiliar. This provoked suspicion among some participants:

> I think it's a bit weird for a website to have that because on other websites that are trustworthy, I don't see it there. … This was a bit unexpected, but unexpected in a negative sense …. it could be that they do this in order to make their website look trustworthy while they're not.

Discussion

Online privacy is an increasingly important issue. Rapid technological developments in information and communication technologies and artificial intelligence have accelerated the impact of computers and mobile phones in our lives as well as the possibilities for online service providers to invade our privacy. Interfaces have become deceptively simple and user-friendly, whereas the processes going on in the background are increasingly complex and opaque. Researchers have spent a lot of time and energy unraveling people's privacy-related attitudes and behaviors, and exploring the privacy paradox, but so far, research-based attempts to empower users with the means to assume responsibility for their online privacy have been limited and unsuccessful.

In this article, we described the design and evaluation of a new privacy visualization called Privacy Rating. To inform users about potential consequences of information disclosure and to raise awareness of data handling practices, a risk-based and multilevel approach was chosen for the design of the Privacy Rating. At the core of the privacy visualization lies a set of 12 privacy aspects derived from a literature review [57]. To avoid information overload, the 12 aspects were divided into four main groups: collection, sharing, control, and security. Dividing otherwise complex information into smaller text passages, in combination with colors and navigation options for more information, makes the information accessible and tailored to individual information needs.

The label acknowledges the functional complexity involved in communicating privacy aspects and supports both less engaged users and privacy-aware users. If widely implemented, it may contribute to privacy awareness among users in general, as it sheds light on the privacy aspects of online services, transforming them from a hidden feature into a conspicuous and comparable characteristic. For less engaged users who may worry about privacy but are unwilling to invest time and effort into evaluating all privacy characteristics, the overall Privacy Rating provides a visual shortcut to support their decision-making process about downloading or using online services. For more engaged users who want to know more about privacy but who may be hesitant to examine the entire privacy policy, the Privacy Rating offers prestructured detailed information in two layers. With these contributions, the Privacy Rating may play a positive role in balancing the unfavorable equilibrium between users and online service providers, in which privacy considerations currently play an inferior role.

The user research that we conducted underlined that the Privacy Rating can be a promising tool to help users safeguard their online privacy and thus limit the privacy paradox [36]. Barth et al. [37] identified three underlying mechanisms of the privacy paradox:

1. A more or less rational weighing of costs and benefits
2. An incomplete and biased weighing of costs and benefits
3. A neglect of privacy considerations

The Privacy Rating should help reduce the influence of the latter two mechanisms. The label urges users to consider privacy aspects in their decisions and reduces biases that they might have when judging privacy risks. As a result, the weighing of costs and benefits will be more systematic and more rational than may currently be the case. That does not mean that the privacy paradox is solved. It is still imaginable that users

could decide in favor of an online service despite privacy risks that they are aware of.

But the discrepancy between attitude and behavior may not be at the core of the problem. People have to make tradeoffs between desires and preferences all the time. The core of the problem is the fact that their decisions are often uninformed. Tackling this deficit is the main purpose of the Privacy Rating tool. The results of our user research suggest that this design is a step in the right direction. With regard to usability, the Privacy Rating did quite well, although participants also uncovered several problems that need to be addressed in future iterations of the label. The problems found mainly concerned the formulation of privacy risks and aspects and details in the visual design. The perceived usefulness was judged very favorably by our users, and the label appeared to significantly affect our participants' decisions on whether to use a particular web shop. User feedback will play a significant role in our future efforts to further optimize the Privacy Rating.

In addition, the results of our user research can be used to inform other privacy visualization projects. Two insights stood out. The first is that connecting a privacy visualization explicitly to users' existing interpretation frames is beneficial. In all parts of our user research, we heard positive remarks about the resemblance of the Privacy Rating to the well-established and familiar energy label, which made our label easy to understand and may have also contributed to the persuasiveness and perceived urgency of the rating. The second is that the development of the label is only half of the story. Several participants in the user research doubted the independence and authoritativeness of the label, letting on that it would make a big difference to them if the label were issued by a trusted source.

Finally, our findings drew attention to two tradeoffs in designing a privacy visualization. The first involves finding a balance between conciseness/simplicity and informativeness. The feedback from some of our participants suggested that they found even the second layer in the information about privacy insufficient. Having said this, we are by no means certain that adding information will make the label better. Our findings lend support to previous work stating that grouping and segmenting information across multiple layers has a positive effect on the understandability of complex information [24] and that color schemes can increase granularity and provide shortcuts for quickly assessing risks [32], [34]. Also, in line with previous work, we found that privacy and security icons have poor understandability [26], [34].

The second tradeoff is between annoying intrusiveness and sheer invisibility. Some of our participants complained about the use of a pop-up, but whether a less intrusive exposure would glean the necessary attention and provide similar effects is questionable. Prior research showed that the timing of users' exposure to privacy notices is very important [70]. The development of any viable privacy visualization must include its effective placement. It is quite possible that the methods of exposure may become less important once the label becomes an established standard [25].

Limitations and Future Work

To our knowledge, this is the first initiative to develop a privacy visualization covering a systematic selection of relevant privacy attributes available in the academic literature, law, and practice. It is also one of the few initiatives to explicitly incorporate user feedback in the process. Still, it is important to keep the following limitations in mind when interpreting the results.

First, the Privacy Rating is still in development. In our user study, we tested a prototype of the privacy label that reflected our knowledge after various studies into user perspectives on online privacy [47]–[49], after a thorough analysis of relevant privacy aspects and earlier privacy visualizations [57], and after an iterative design process including expert and user input. The user study reported in this article provided us with more food for thought, which we will use to further optimize the privacy rating. Specifically, we will look into using simpler language and including links to further information.

Moreover, we foresee three additional developments in the period ahead. We will try to further explore the implementation of the label, which involves gaining support from online service providers, platforms, and legislation. Any advancements may have consequences for users' perceptions of the Privacy Rating. We will also try to make the input for the Privacy Rating more objective and trustworthy. The score that online services currently receive is based on service providers' self-reports in the questionnaire. That is not necessarily a bad option, as service providers can be held responsible for any discrepancy between their privacy policies and their answers in the questionnaire. But ideally, the privacy ratings

would be obtained directly from the privacy policies, either by natural language processing or by the intervention of an independent authority. Future developments in this respect may also have a positive impact on users' perceptions. We will try to set up communication about the Privacy Rating itself. In the current user study, participants saw nothing but the visualization. We are planning to develop a series of short persuasive messages explaining the system, its background, and the need for it.

Second, the user research described in this article was, in line with the state of development of the Privacy Rating, limited to specific aspects of the label after artificial exposure. In the usability test, we focused predominantly on the perceived understandability of the various elements of the Privacy Rating. It would be interesting in follow-up research to focus more on participants' interpretations and actual use of the label as a whole. The research into the effects of the Privacy Rating was limited to the explicit question whether the participants would trust the web shop enough to do business with it. Follow-up research in a more natural setting would less exclusively and explicitly focus on the trust question and ask how the privacy label might, for instance, affect the image or reputation of the online service provider. The question whether a positive Privacy Rating can be good for business would be very relevant, as it could convince online service providers to embrace transparency regarding privacy and include the Privacy Rating in their communication.

Third, experimental research is needed to further investigate the two tradeoffs that we mentioned: between conciseness/simplicity and informativeness (which balance is most effective for which user groups) and between annoying intrusiveness and sheer invisibility (how can we make a privacy label optimally visible without annoying users). Finally, it would be interesting to extend research in laboratory settings with real-life research into the users' appreciation of and behavior toward the Privacy Rating.

Conclusion

We propose Privacy Rating, which addresses the inherent functional complexity of privacy communication by visually synthesizing information across multiple layers of increasing detail. It thereby increases awareness, provides less engaged users with shortcuts, and supports privacy aware users in making informed decisions. Usability testing showed that the label was perceived as useful and usable. It also had a significant effect on trust in the online service. All participants indicated they would appreciate such a label becoming an established standard. More generally, we learned that privacy visualizations should use familiar design elements and ideally be supported by a trustworthy organization.

In our future work, we will concentrate on refining the Privacy Rating and making it market-ready. We are therefore looking for prospective partners and organizations interested in future collaboration to bring the Privacy Rating to the market. A privacy visualization that satisfies these requirements can empower users by significantly improving privacy awareness and helping achieve truly informed consent.

Acknowledgment

This work was supported by the Dutch Research Council (NWO; grant number: 628.001.011) in collaboration with the Netherlands Organisation for Applied Scientific Research (TNO), the Dutch Research and Documentation Centre (WODC), and Centric.

References

[1] T. Berners-Lee, J. Handler, and O. Lassila, "The semantic web," *Sci. Amer.*, vol. 284, no. 5, pp. 34–43, 2001.
[2] G. R. Milne, A. J. Rohm, and S. Bahl, "Consumers' protection of online privacy and identity," *J. Consum. Affairs*, vol. 38, no. 2, pp. 217–232, 2004.
[3] K. Huckvale, J. T. Prieto, M. Tilney, P.-J. Benghozi, and J. Car, "Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment," *BMC Med.,* vol. 13, no. 1, 2015, Art. no. 214.
[4] S. C. Matz, R. E. Appel, and M. Kosinski, "Privacy in the age of psychological targeting," *Curr. Opin. Psychol.*, vol. 31, pp. 116–121, 2020.
[5] M. Alsaleh, N. Alomar and A. Alarifi, "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods," *PLoS ONE*, vol. 12, no. 3, 2017, Art. no. e0173284.
[6] J. A. Mourey and A. E. Waldman, "Past the privacy paradox: The importance of privacy changes as a function of control and complexity," *J. Assoc. Consum. Res.*, vol. 5, no. 2, pp. 162–180, 2020.

[7] M. Rudolph, D. Feth, and S. Polst, "Why users ignore privacy policies. A survey and intention model for explaining user privacy behavior," in *Human-Computer Interaction: Theories, Methods, and Human Issues*. M. Kurosu, ed. Cham, Switzerland: Springer, 2018, pp. 587–598.
[8] R. W. Proctor, M. A. Ali, and K.-P. L. Vu, "Examining usability of web privacy policies," *Int. J. Hum. Comput. Interact.*, vol. 24, no. 3, pp. 307–328, 2008.
[9] J. Prichard and K. Mentzer, "An analysis of app privacy statements," *Issues Inf. Syst.*, vol. 18, no. 4, pp. 179–188, 2017.
[10] C. Jensen and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2004, pp. 179–188.
[11] A. Sunyaev et al., "Availability and quality of mobile health app privacy policies," *J. Amer. Med. Inf. Assoc.*, vol. 22, pp. e28–e33, 2015.
[12] Z. Papacharissi and J. Fernback, "Online privacy and consumer protection: An analysis of portal privacy statements," *J. Broadcast. Electron. Media*, vol. 49, no. 3, pp. 259–281, 2005.
[13] A. Acquisti et al., "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Comput. Survey*, vol. 50, no. 3, 2017, Art. no. 44.
[14] J. Gu et al., "Privacy concerns for mobile app download: An elaboration likelihood model perspective," *Decis. Support Syst.*, vol. 94, pp. 19–28, 2017.
[15] L. Festinger, *A Theory of Cognitive Dissonance*. Stanford, CA, USA: Stanford Univ. Press, 1957.
[16] S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao, and S. J. Upadhyaya., "Internet and online information privacy: An exploratory study of preteens and early teens," *IEEE Trans. Profess. Commun.*, vol. 52, no. 2, pp. 167–182, Jun. 2009.
[17] S. Young, "Zoombombing your toddler: User experience and the communication of zoom's privacy crisis," *J. Bus. Tech. Commun.*, vol. 35, no. 1, pp. 147–153, 2021.
[18] P. G. Kelley et al., "A 'nutrition label' for privacy," in *Proc. 5th Symp. Usable Privacy Secur.*, 2009, Art. no. 4.
[19] P. G. Kelley et al., "Standardizing privacy notices: An online study of the nutrion label approach," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2010, pp. 1573–1582.
[20] L.-E. Holtz, K. Nocun and M. Hansen, "Towards displaying privacy information with icons," in *Privacy and Identity Management for Life*. S. Fischer-Hübner et al., eds. Heidelberg, Germany: Springer, 2011, pp. 338–348.
[21] L.-E. Holtz, H. Zwingelberg, and M. Hansen, "Privacy policy icons," in *Privacy and Identity Management for Life*. J. Camenisch et al., eds. Heidelberg, Germany: Springer, 2011, pp. 279–285.
[22] B. van den Berg and S. van der Hof, "What happens to my data? A novel approach to informing users of data processing practices," *First Monday*, vol. 17, no. 7, 2012.
[23] J. Petterson, "A brief evaluation of icons in the first reading of the European Parliament on COM (2012) 0011," in *Privacy and Identity Management For the Future Internet in the Age of Globalisation*. J. Camenisch et al., eds. Heidelberg, Germany: Springer, 2012, pp. 125–135.
[24] L. Edwards and W. Abel. (2014-2015). The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services. CREATe working paper. Centre for Copyright and New Business Models in the Creative Economy (CREATe), 2014, Glasgow, UK. [Online]. Available: https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf
[25] S. Esayas et al., "Is a picture worth a thousand terms? Visualising contract terms and data protection requirements for cloud computing users," in *Current Trends in Web Engineering*. S. Casteleyn et al., eds. Cham, Switzerland: Springer, 2016, pp. 39–56.
[26] A. Rossi and M. Palmirani, "A visualization approach for adaptive consent in the European data protection framework," in *Proc. Int. Conf. E-Democracy Open Govern.*, Krems, Austria, 2017, pp. 159–170.
[27] A. Rossi and M. Palmirani, "DAPIS: An ontology-based data protection icon set," in *Knowledge of the Law in the Big Data Age*. G. Peruginelli and S. Faro, eds. Amsterdam, the Netherlands, IOS Press, 2019, pp. 181–195.
[28] M. Van Kleek et al., "Better the devil you know: Exposing the data sharing practices of smartphone apps," *Proc. CHI Conf. Human Factors Comput. Syst.*, 2017, pp. 5208–5220.
[29] K. Renaud and L. A. Shepherd, "How to make privacy policies both GDPR-compliant and usable," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment*, 2018.
[30] W. B. Tesfay et al., "PrivacyGuide: Towards an implementation of the EU GDPR on internet privacy policy evaluation," in *Proc. 4th ACM Int. Workshop Secur. Privacy Analytics*, 2018, pp. 15–21.
[31] G. Fox et al., "Communicating compliance: Developing a GDPR privacy label," in *Proc. 24th Am. Conf. Inf. Syst.*, Atlanta, GA, USA: Association for Information Systems, 2018.
[32] Z. Efroni et al., "Privacy icons: A risk-based approach to visualisation of data processing," *Eur. Data Prot. Law Rev.*, vol. 5, no. 3, pp. 352–366, 2019.
[33] A. Soumelidou and A. Tsohou, "Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram," *Inf. Tech. People*, vol. 33, no. 2, pp. 502–534, 2019.
[34] S. de Jong and D. Spagnuelo, "Iconified representations of privacy policies: A GDPR perspective," in *Trends and Innovations in Information Systems and Technologies*. vol. 2, A. Rocha et al., eds. Cham, Switzerland: Springer, 2020, pp. 796–806.
[35] The European Parliament and the Council of European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 On the Protection of Natural Persons With Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC*, vols. Legislation OJ L vol. 119, 2.5, Luxembourg, Europe: Publ. Office Eur. Union, 2016.
[36] S. B. Barnes, "A privacy paradox. Social networking in the United States," *First Monday*, vol. 11, no. 9, 2006, doi: 10.5210/fm.v11i9.1394.

[37] S. Barth and M. D. T. de Jong, "The privacy paradox. Investigating discrepancies between expressed privacy concerns and actual online behavior. A systematic literature review," *Telematics Inf.*, vol. 34, no. 7, pp. 1038–1058, 2017.
[38] M. Langheinrich, "Privacy by design. Principles of privacy-aware ubiquitous systems," in *Ubicomp 2001: Ubiquitous Computing*. G. D. Abowd, B. Brumitt, and S. Shafer, eds. Berlin, Germany: Springer, 2001, pp. 273–291.
[39] A. Cavoukian. (2011 Jan.). Privacy by design. The 7 foundational principles. Tech. rep. (revised version), Information and Privacy Commissioner of Ontario. [Online]. Available: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf
[40] ISO/IEC 29100:2011, *Information Technology—Security Techniques—Privacy Framework*. Geneva, Switzerland: International Organization for Standardization and International Electrotechnical Commission. [Online]. Available: https://www.iso.org/standard/45123.html
[41] B.-J. Koops and R. Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law," *Int. Rev Law, Comput. Tech.*, vol. 28, no. 2, pp. 159–171, 2014.
[42] D. Klitou, "A solution, but not a panacea for defending privacy: The challenges, criticism and limitations of privacy by design," in *Annual Privacy Forum*, B. Preneel and D. Ikonomou, eds. Berlin, Germany: Springer, 2012, pp. 86–110.
[43] F. Bu et al., "Privacy by design implementation: Information system engineers' perspective," *Int. J. Inf. Manage.*, vol. 53, Art. no. 102124, 2020.
[44] A. A. Gerunov, "Attitudes towards privacy by design in e-government: Views from the trenches," *J. Soc. Admin. Sci.*, vol. 7, no. 1, pp. 1–17, 2020.
[45] A. Cavoukian, "Understanding how to implement privacy by design, one step at a time," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 78–82, Mar. 2020.
[46] Forbrukerrådet, *Deceived By Design, How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*. Oslo, Norway: Forbrukerrådet [Consumer Council], 2018.
[47] S. Barth et al., "Toward an understanding of online privacy perceptions: Using the Q-sort method to identify different user perspectives," 2021.
[48] S. Barth et al., "Putting the privacy paradox to the test. Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics Inform.*, vol. 41, no. 1, pp. 55–69, 2019.
[49] S. Barth et al., "Lost in privacy? Online privacy from a cybersecurity expert perspective," 2021.
[50] O. Ben-Shahar and A. Chilton, "Simplification of privacy disclosures: An experimental test," *J. Legal Studies*, vol. 45, no. S2, pp. S41–S67, 2016.
[51] R. LaRose and N. J. Rifon, "Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior," *J. Consum. Affairs*, vol. 41, no. 1, pp. 127–149, 2007.
[52] L. Lentz and H. Pander Maat, "Functional analysis for document design," *Tech. Commun.*, vol. 51, no. 3, pp. 387–398, 2004.
[53] M. D. T. de Jong and Y. Wu, "Functional complexity and web site design: Evaluating the online presence of UNESCO world heritage sites," *J. Bus. Tech. Commun.*, vol. 32, no. 3, pp. 347–372, 2018.
[54] A. Deuker, "Addressing the privacy paradox by expanded privacy awareness. The example of context-aware services," in *Privacy and Identity Management For Life*. M. Bezzi et al., eds. Berlin, Germany: Springer, 2009, pp. 275–283.
[55] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?," in *The Future of Identity*. V. Matyáš et al., eds. Berlin, Germany: Springer, 2008, pp. 226–236.
[56] X. Sheng et al., "Sight unseen: The role of online security indicators in visual attention to online privacy information," *J. Bus. Res.*, vol. 111, pp. 218–240, 2020.
[57] S. Barth et al., "Understanding online privacy: A systematic review of privacy visualizations and privacy by design guidelines," 2021.
[58] M. Mehldau. Iconset for data-privacy declarations. v0.1. 2007. [Online]. Available: https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf
[59] J. Gomez, T. Pinnick, and A. Soltani. (2009). KnowPrivacy. UC Berkeley, School Inf., Berkeley, CA, USA. [Online]. Available: http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf
[60] B. Moskowitz and A. Raskin. (2011). Privacy icons. Mozilla Wiki. [Online]. Available: https://wiki.mozilla.org/Privacy_Icons
[61] C. Graf et al., eds., (2011). PrimeLife—Privacy and identity management in Europe for life: Final HCI Res. Rep., 2011. [Online]. Available: http://primelife.ercim.eu/images/stories/deliverables/d4.1.5-final_hci_research_report-public.pdf
[62] T. Pinnick, *Privacy Short Notice Design*. San Francisco, CA, USA: TrustArc, 2011. [Online]. Available: https://trustarc.com/blog/2011/02/17/privacy-short-notice-design/
[63] G. Franke, T. Clever, W. van Dijk, J. Raider, and R. de Jonge, *Privacy Label*. Blog series part I-IV. Sensor lab, 2019. [Online]. Available: https://medium.com/sensor-lab/the-privacy-illusion-994ed98ec3ab
[64] *Upgrade Your Privacy Statement: Privacy Label Helps You Communicate How You Use Data*. Privacy Label, 2020. [Online]. Available: https://www.privacylabel.org/learn/how-does-it-work
[65] M. Hansen, "Putting privacy pictograms into practice. A European perspective," in *Informatik 2009–Im Focus das Leben*. S. Fischer et al., ed. Bonn, Germany: Gesellschaft für Informatik, 2009, pp. 1703–1716.
[66] H. Nissenbaum, "A contextual approach to privacy online," *Daedalus*, vol. 140, no. 4, pp. 32–48, 2011.

[67] H. Nissenbaum, "Contextual integrity up and down the data food chain," *Theoritical Inquiries Law*, vol. 20, no. 1, pp. 221–256, 2019.
[68] European Parliament and Council of European Union. *Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 Setting a Framework For Energy Labelling and Repealing Directive 2010/30/EU. Legislation OJ L 198, 28.7.2017*. Luxembourg, Luxembourg: Publ. Office Eur. Union, 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1369&rid=4
[69] European Commission, *Energy Label Templates*. Directorate-General for Energy, Brussels, Belgium, 2020. [Online]. Available: https://ec.europa.eu/energy/topics/energy-efficiency/energy-label-and-ecodesign/energy-label-templates_en?redir=1
[70] R. Balebako et al., "The impact of timing on the salience of smartphone app privacy notices," in *Proc. 5th Annu. ACM CCS Workshop Security Privacy Smartphones Mobile Devices*, 2015, pp. 63–74.

Susanne Barth received the Ph.D. degree in Communication Science from the University of Twente, Enschede, the Netherlands, in 2021. Her Ph.D. project centered on privacy and security requirements for mobile applications. She is a Postdoctoral Researcher within the Communication Science Group, BMS faculty, and the Services and CyberSecurity group, EEMCS faculty at the University of Twente. Her research expertise is strongly rooted within communication science and psychology, primarily with a focus on the human factor in technology and societal challenges intertwined with new media and technologies these days.

Dan Ionita received the bachelor's degree in Electrical Engineering from the Polytechnic University of Bucharest, in 2011 and the M.Sc. degree in Information Systems Engineering and the Ph.D. degree in Information Security Risk Assessment from the University of Twente, Enschede, the Netherlands, in 2013 and 2018, respectively. He is a Postdoctoral Researcher within the Services and Cyber-Security Department of the University of Twente. He is currently researching, teaching, and providing consultancy in the field of privacy and information security.

Menno D. T. de Jong received the Ph.D. degree in Communication Science from the University of Twente, Enschede, the Netherlands, in 1998. He is currently a Full Professor of communication science with the University of Twente. Between 2009 and 2015, he was the Editor-in-Chief of *Technical Communication*, the flagship journal of the Society for Technical Communication. He has authored or coauthored in a broad range of academic journals. His research interests include the fields of technical and organizational communication. Prof. de Jong was the recipient of various awards for his research, including two Rudolph J. Joenk, Jr. awards from the IEEE Professional Communication Society for Best Paper in the TRANSACTIONS, the Ken Rainey Award for Excellence in Research from the STC, and the Alfred N.Goldsmith Award for Outstanding Achievement in Engineering Communication from the IEEE Professional Communication Society.

Pieter H. Hartel received the Ph.D. degree in Computer Science from the University of Amsterdam, Amsterdam, the Netherlands, in 1989. He is Professor Emeritus of cyber security with the Delft University of Technology, Delft, the Netherlands, and the University of Twente, Enschede, the Netherlands, and an Adjunct Faculty with the Singapore University of Technology and Design. His research interests include cybersecurity, cybercrime, and block-chain technology.

Marianne Junger received the Ph.D. degree in law from the Free University of Amsterdam, Amsterdam, the Netherlands, in 1990. She is the Emeritus Professor of Cyber Security and Business Continuity with the University of Twente, Enschede, the Netherlands. Her research investigates the human factors of fraud and cybercrime. More specifically, she investigates victimization, disclosure, and privacy issues. She founded the *Crime Science* journal together with Pieter Hartel and was an Associate Editor for 6 years. Her research was sponsored by, among others, the Dutch Police, NWO, ZonMw (for health research), and the European Union.