On Using Privacy Labels for Visualizing the Privacy Practice of SMEs

Challenges and Research Directions

Mortaza S. Bargh*
Research Center Creating 010, Rotterdam University of Applies Sciences, Rotterdam, The Netherlands, Email: m.shoae.bargh@hr.nl and Research and Documentation Center, Ministry of Justice and Security, The Hague, The Netherlands, Email: m.shoae.bargh@wodc.nl

Maud van de Mosselaar
Research Center Creating 010, Rotterdam University of Applies Sciences, Rotterdam, The Netherlands, Email: mvandemosselaar@outlook.com

Paul Rutten
Research Center Creating 010, Rotterdam University of Applies Sciences, Rotterdam, The Netherlands, Email: p.w.m.rutten@hr.nl

Sunil Choenni*
Research Center Creating 010, Rotterdam University of Applies Sciences, Rotterdam, The Netherlands, Email: r.choenni@hr.nl and Research and Documentation Center, Ministry of Justice and Security, The Hague, The Netherlands, Email: r.choenni@wodc.nl

ABSTRACT

Privacy is a comprehensive notion which is hard to grasp for the layman. To make the privacy notion tangible, creating transparency about privacy practices is an important necessity. Transparency about privacy practices is traditionally (sought to be) established via providing privacy policies and privacy seals. These traditional transparency mechanisms have resulted in limited success in society, where digital transformation takes place with a fast pace. To address these challenges, privacy visualization via a label representation, like energy and food labels, is considered a promising solution direction. Visualizing privacy, in general, and using privacy labels, in particular, are not straightforward in practice due to, among others, the subjectivity and context dependency of privacy and the adverse (side) impacts of privacy violations. This practicality issue is more evident for Small and Medium-sized Enterprises (SME's) because, compared to large enterprises, they have limited resources for protecting and managing the personal data they process. In this contribution, we investigate the capabilities and limitations of a privacy label and its labeling tool for use by SMEs in three business domains. Accordingly, and within SME settings, we identify the following directions for future research: Enhancing trust in privacy labels, dealing with network aspects, adopting privacy labels and labeling tools, using the labeling process and outcome for auditing own privacy practice, and improving the current privacy labels and labeling tools.

CCS CONCEPTS

• **Security and privacy, Human and societal aspects of security and privacy, Privacy protection**;

KEYWORDS

Online services, privacy label, SMEs, transparency, trust

ACM Reference Format:
Mortaza S. Bargh*, Maud van de Mosselaar, Paul Rutten, and Sunil Choenni. 2022. On Using Privacy Labels for Visualizing the Privacy Practice of SMEs: Challenges and Research Directions. In *DG.O 2022: The 23rd Annual International Conference on Digital Government Research (dg.o 2022), June 15–17, 2022, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3543434.3543480

1 INTRODUCTION

Digital transformation is accelerating across all sectors of our society. As citizens, on the one hand, we use more and more online services and apps to facilitate our daily life activities. On the other hand, the number of enterprises, organizations, and institutions that utilize digital technology is rising. This rise of digital transformation is noticeable also for Small and Medium Sized Enterprises (SMEs), among which are retail, media and cultural enterprises. Retailers with brick-and-mortar location are not future-proof without an online platform nowadays. Media SMEs, which have been operating in the digital domain for a relatively long time, combine online curations with their traditional media services. In the cultural sector, the digital selection of cultural services, besides the physical interactions, is growing. In the last two years, the online cultural offerings have even been boosted because of the COVID-19 related restrictions imposed on cultural events.

*Corresponding author.

dg.o 2022, June 15–17, 2022, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-9749-0/22/06…$15.00
https://doi.org/10.1145/3543434.3543480

Often using and offering online services and apps, as a downside, require processing (e.g., collecting, analyzing, and sharing) personal information about individuals such as citizens, customers, and consumers [10]. Inappropriate use of personal information within these online services and apps can lead to the infringement of privacy. Therefore, individuals, civil institutions, supervisory bodies, and watchdogs should (establish) trust in the privacy practice of the providers of these online services and apps (i.e., how the providers protect privacy). Establishing trust in such privacy practices is a key challenge facing the currently ongoing digital transformation.

Creating transparency about privacy practices helps establishing trust and is considered necessary in many privacy laws and regulations such as the General Data Protection Regulation [12]. This transparency is traditionally (sought to be) established via providing privacy policies and using privacy seals. These traditional transparency mechanisms have resulted in limited success in practice [8]. To address these challenges, privacy visualization via a label representation, like energy and food labels, is considered a promising solution direction. Privacy labels can be seen as a means of explaining privacy practices in that how service and app providers process and deal with personal information. However, in practice, visualizing privacy in general and using privacy labels in particular are far from being simple or straightforward. This complexity stems from, among others, the subjectivity and context dependency of privacy and the adverse (side) impacts of privacy violations [5]. This practicality and complexity issue is prominent for SMEs because, compared to large enterprises, they have limited resources for protecting and managing personal data. Having limited resources makes it difficult for SMEs to easily figure out which privacy requirements are (not) implemented in their online services and apps, and to comprehend the corresponding privacy implications. Privacy labels may assist SMEs to gain insight in these privacy requirements and their implications, to prioritize the privacy requirements, and to safeguard the most relevant privacy demands.

Our research objective is to investigate how privacy labels may contribute to the transparency of enterprises about their privacy practices when providing online services (e.g., websites and mobile services) and/or apps, and to study the capabilities and limitations of current privacy labels and identify some directions for future research and development. We limit our focus to SMEs from different business domains because they have limited (inhouse) resources and therefore it is necessary to investigate whether and how they can appropriately exploit these privacy labels to the full potential. As a benchmark, we will use the privacy label and the labeling tool developed in the SERIOUS project executed between 2014 and 2020 [17]. The project was carried out by a partner institution. The privacy label and the labeling tool of the SERIOUS project are developed based on scientific research and are evaluated in a limited scale among university students and some experts from businesses and public organizations. Therefore, there is a need to examine their usage, capabilities and limitations within a wide range of businesses, enterprises and consumers (i.e., conducting a thorough investigation and translation of the privacy label and the labeling tool to the work field). One limitation of the current privacy label is that it does not take the business domain into consideration. Depending on the business domain, one might expect that certain privacy attributes can be more important than others, which requires tailoring of the current label.

Considering the above-mentioned research objective, we investigate the following research questions in this paper:

- What are the advantages and limitations of the SERIOUS privacy label and its labelling tool when used by SMEs?
- Can the SERIOUS privacy tool be used by SMEs to gain insight into their own privacy practice (and to improve their privacy protection practice)?
- In which directions can the current privacy label and labelling tool be improved for use by SMEs? What are the challenges (or research directions) for further developing the label and the labeling tool for use by SMEs?

For this study, we adopt an explorative and qualitative feasibility study. To this end, we use literature study and semi-structured interviews with the employees of three SMEs who were responsible for operation of the online services within those SMEs. These SME employees could be considered as responsible stakeholders within those SMEs to issue and adopt privacy labels for those online services. The structuring of these interviews is informed by our literature study on technology adoption theories.

The organization of the paper is as follows. In Section 2, we explain the study context and the theoretical foundation of the study. In Section 3, we describe how we conducted the semi-structured interviews and analyzed the results. In Section 4, we discuss the results by categorizing the directions for future research and developments. Finally, in Section 5, we draw some conclusions.

2 STUDY CONTEXT AND RELEVANT THEORETICAL PRINCIPLES

In this section we describe the study context, particularly presenting the theoretical foundation of the study.

2.1 Transparency of the privacy practice

Transparency about the privacy practice is traditionally (sought to be) established via providing privacy policies and privacy seals. These traditional transparency mechanisms have resulted in limited success and effect in practice [8]. On the one hand, consumers cannot understand privacy policies due to their lengthy and cumbersome legal content. Therefore, despite being concerned about their privacy, consumers download apps and use online services; and accept their privacy policies blindly, without thinking (seriously) about the privacy ramifications of their decisions. The discrepancy between consumers' privacy concerns and their reckless behavior in blindly using these apps and services is referred to as the privacy paradox [7]. Blindly accepting privacy policies weakens their effectiveness and their legally binding impacts as such consents may not be considered as informed and freely given. The privacy seals are trust seals issued by third parties to assure the consumers of an online service that the service meets a certain standard of privacy protection. On the other hand, privacy seals have their own limitations as they are not correlated with trustworthiness [11] and even those based on crowdsourcing have not been successful so far [8].

Privacy policies and seals may be enhanced by educational mechanisms to raise the awareness of consumers about the privacy practice, thus empowering consumers to take their responsibility for privacy protection. Nevertheless, general knowledge and privacy awareness have no significant role in the privacy paradox as "advanced Computer Science students and even privacy and security experts appear to struggle with the same issues as lay users, exhibiting similar unsafe behaviors", see [8] pp. 192. This low impact of privacy awareness can be attributed to the functional complexity associated with (a) communicating the importance of privacy and privacy risks to users, (b) providing less engaged users with clear decision-making shortcuts to contain privacy risks, and (c) providing highly engaged users with user-friendly and personalized information (thus of varying details) to contain privacy risks (ibid).

2.2 Privacy visualization

Privacy visualizations can be designed and used to communicate some relevant aspects of the privacy practice to the consumers. Based on a systematic literature study, [8] provides an overview of 13 privacy visualizations. As these visualizations are meant for average consumers, they intend to convey those aspects of data practice and usage that are somehow interesting for these consumers. For example, the Privacy Short Notice of TrustArc project analyzed the previous approaches for providing a simplified summary of privacy policies and decided to visualize those aspects that are invisible for consumers of these services like, among others, secondary use and third-party tracking. As privacy concerns are context dependent and subjective [5, 6], it is a challenge to determine the relevant aspects of the privacy practice and, therefore, to adopt a suitable privacy visualization beforehand.

Further, for different reasons, creating transparency about the privacy practice is relevant for both consumers and providers of online services and apps. The consumers, on the one hand, need to gain trust in (the providers of) these services and apps for sharing their personal data with them. The providers, on the other hand, need to gain the trust of consumers, authorities, and society by showing how well they respect and adhere to human values including protecting the privacy of their customers and service consumers. To inform the providers of online services and apps, there have been many design guidelines proposed to facilitate embedding privacy protection principles in the fabric of these apps and services. The development of these so-called Privacy by Design (PbD) guidelines is inspired by privacy laws and regulations as well as by privacy engineering best practices. Based on a systematic literature study, [8] provides an overview of 14 sets of privacy by design guidelines. As the target group for these guidelines are system developers and providers of online services and apps, they cover the privacy protection aspects of the system development process mainly. Further, these PbD guidelines are useful for privacy engineering experts and enterprises who have enough resources to hire such experts and develop (inhouse) privacy protection solutions based on these guidelines. For those enterprises with limited resources, like SMEs, it is a challenge to get insight in these PbD guidelines, yet alone to implement them by themselves (inhouse).

As mentioned above, providing a user-friendly privacy visualization, with varying levels of details, is needed for informing less or highly engaged consumers about the privacy risks and empowering them for actively seeking for appropriate privacy protection measures. In this contribution, we are interested in exploring whether providing such a user-friendly privacy visualization might also be relevant for enterprises with limited resources (like SMEs). The underlying assumption is that the developers and providers of online services and apps with limited privacy protection expertise can use such user-friendly and rich privacy presentations to gain insight into the privacy risks of their online services and apps as well as into the appropriate measures needed for mitigating these privacy risks in them. The need for a privacy visualization for enterprises with limited resources (like SMEs) asks for adequately covering the PbD guidelines in the desired privacy visualization. This adequate coverage of the PbD guidelines can also enable both less engaged and highly engaged consumers to learn about the privacy risks and deal with these risks accordingly, depending on their interests and the levels of their expertise and engagement.

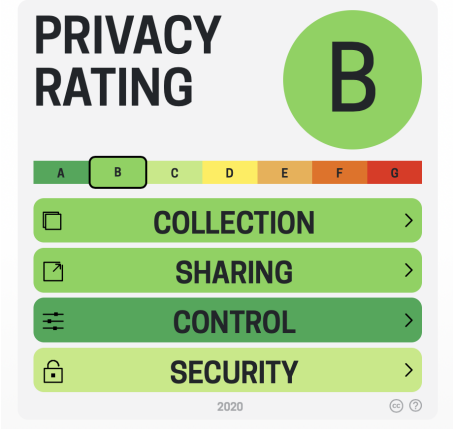

Figure 1: An example of the SERIOUS privacy label (generated with the interactive process of the SERIOUS tool).

2.3 SERIOUS privacy label

In this study we use the privacy label and the privacy labeling tool developed in the SERIOUS project, which take advantage of the features of existing privacy visualizations and the comprehensive features embedded in PbD guidelines [8]. The study in [8] and [9], describes the development process of the SERIOUS privacy label (system) which consist of (a) deriving a set of privacy attributes from existing privacy visualizations and PbD guidelines, (b) ranking these attributes by consumers and experts, and (c) visualizing these ranked and clustered attributes in a letter-color based label, and (d) evaluating the resulting privacy label via user studies (i.e., by consumers). Aiming at simplicity, clarity, recognizability, and attractiveness, the SERIOUS privacy visualization label, as indicated by an example in Figure 1, provides four classes – namely collection, sharing, control and security – to draw the attention of less-engaged consumers to make a quick overall judgment about the potential privacy threats of online services and apps.

Like familiar energy labels, as illustrated in Figure 1, these SERIOUS privacy classes are indicated by combinations of letters and

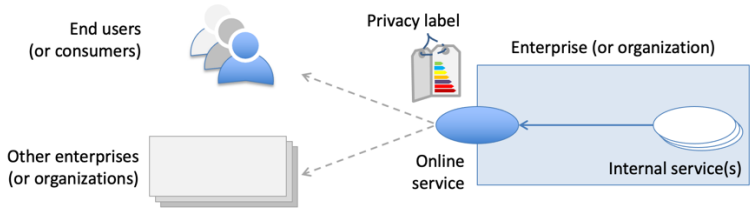

Figure 2: An illustration of the generic setting in which the SERIOUS privacy label is used.

colors, ranging from A plus green for the most positive online services, to G plus red for the most negative ones. The colors also resemble the conventional color scheme of traffic lights. For those highly engaged consumers the SERIOUS privacy rating system provides (a) the scores of the online service or app in the four privacy categories (namely collection, sharing, control, and security), and (b) specific information about every privacy attribute through hovering or clicking these privacy categories.

The generic setting for/in which the SERIOUS privacy label is created/used is illustrated in Figure 2. The label is created within an enterprise for the online service it offers; and used by consumers and the other enterprises to gain insight in the privacy practice of the enterprise.

2.4 SME characteristics

SMEs are defined based on their employment sizes, economic values, assets and sales volumes [1]. They typically employ less than a few hundred employees – like 500 or 200 employees [1, 19]. SMEs offer various advantages such as employment creation at low capital cost, flexibility, and innovation [1]. The role of SMEs is significant for economy due to their entrepreneurial spirit, adaptive capabilities, and competitiveness that act as drivers of economic growth and innovation [13]. SMEs account for 96% to 99% of the economic activities of most OCED nations and about 80% of their economic growth [1]. For North American and European countries, SMEs contribute to their Gross Domestic Product (GDPs) significantly (with 99% of all businesses) and to their job creation (around 70% job creation). Also in Australia, SMEs form the 95% of businesses, contribute to over 57% of the country's GDP, and are a key source of employment [15]. According to [14], in 2019 SMEs account for 65% of the added-value and for 71% of the employment in the business economy of The Netherlands.

A key enabler of innovation for organizations and businesses is the deployment and use of Information and Communication Technologies (ICTs). ICTs refer to a wide range of software, hardware, telecommunications and information management techniques, applications, and devices [20]. They are increasingly used to collect, store, process, and transmit data about every aspect of our personal and business lives. As such, ICTs impact the way that organizations and individuals work nowadays. ICTs enable SMEs to access new market opportunities and specialized information. Those SMEs that adopt ICTs can have increased productivity, increased efficiency of internal business operations, cheaper and easier connection to external contacts, increased business competitiveness, increased vertical integration with other related business, stakeholder and institutions, and improved networking with other parties [15, 20]. Via participating in e-marketplaces, SMEs can attain product differentiation and supply chain entry [15] and business growth may require SMEs to implement ICTs to effectively manage such growth [20].

ICT adoption within SMEs is lower than that in large enterprises. This adversely affects their economic development and weakens their access to global markets. Large organizations have more resources and greater economies of scale and, therefore, they can take greater risks associated with innovation adoption [15]. Often, the difficulty of adopting ICTs for SMEs can be attributed to resource constraints related to financial (ability to invest in ICTs), infrastructural (bandwidth and power) and organizational (lack of skilled staff, lack of coherent strategy, inability to adopt new ICT enabled processes) aspects [19, 20]. Moreover, like in any organization, SME employees often refuse to adopt an innovative technology due to fear of job loss if their working practices change [13]. Despite these constraints for SMEs, there are some advantages for SMEs compared to large enterprises. For example, compared to larger organizations, communication between employees and managers is more effective, and executing and implementing decisions are quicker in SMEs [15].

Given the importance of SMEs in economy, and their differences with large enterprises in adopting innovative technology (and ICT), it is essential to explore and study the issue of ICT adoption by SMEs. Therefore, it is worthwhile to investigate the adoption and acceptance of privacy labels and labeling tools within SMEs.

2.5 Study scope

Barth [8] investigated the similarities and differences between the four perspectives of (a) the principles of existing privacy visualizations, (b) the principles of existing PbD guidelines, (c) the requirements of privacy experts, and (d) the expectations of consumers to arrive at a privacy label that covers the raised privacy issues and to evaluate the resulting privacy label with those who use privacy labels (i.e., consumers). There are two issues, both of which are from the perspective of privacy label producing parties (i.e., the enterprises developing and providing online services and apps), not addressed in current studies. These two issues, which we are interested in here to study further in the context of SMEs, are:

- How the privacy label issuing SMEs perceive the privacy label and the process of the privacy label creation and
- How the created label and the labeling tool – which covers a wide range of PbD guidelines – help these SMEs to get

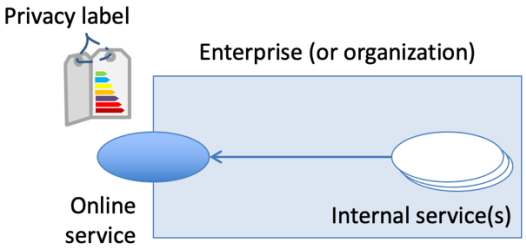

Figure 3: An illustration of the primary scope of this study.

insight into (and resolve) the privacy concerns of their online services and apps.

With respect to the generic setting depicted in Figure 2, the scope of our study is illustrated in Figure 3

2.6 Related work

One way to communicate the privacy risks to service consumers clearly and concisely is via visualizing how service providers handle personal data in their applications, mobile apps, websites, etc. Various privacy labels like nutrition labels have been developed for visualizing the privacy policies and practices of these service providers. For an overview of these labels, the interested reader is referred to (Chapter 6 of [8]), which investigates the most prominent privacy labels such as: the policy coding methodology of the KnowPrivacy project, the Carnegie Mellon's CyLab privacy nutrition label, Mozilla's privacy icons, the privacy icons of the PrimeLife project, the privacy icons of a draft version of the DGPR, to name a few.

The SERIOUS privacy label and labelling tool are developed based on the abovementioned existing privacy visualizations and also based on PbD guidelines (see Chapters 6 and 7 of [8]). To this end, a set of privacy attributes are chosen as basis, subsequently the chosen attributes are clustered based on user studies and expert interviews, and finally the attribute clusters are visualized in a privacy label. To facilitate deriving this label for a given context by the service provider, a web application is developed, see [16]. Finally, the developed privacy label and its tool are evaluated with user studies. Via these user studies, the usability of the privacy label, its perceived usefulness, and its effect on users' trust in an online service are evaluated.

Noting that the participants of the initial user study in [8] were recruited from a university's pool of research participants, from a commercial research participants pool and via social media, we have done a second round of user study within the scope of SMEs in this contribution. Our focus here is laid on how SMEs perceive this label, for which goal and how it may be used, and the issues they might face for creating and using the label in their enterprises. The study of [8], moreover, focuses on how service consumers (i.e., average persons) who receive the label perceive the label in a general business setting.

3 SEMI-STRUCTURED INTERVIEWS

In this section, we provide information about the way that the interviews were conducted, the theoretical principles used for structuring the interviews, and the outcomes of the interviews.

3.1 Guiding principles

The privacy label is issued by the enterprises that offer online services like websites and apps to individuals (e.g., citizens and consumers) in B2C settings and/or to other enterprises in B2B settings. In this study the term enterprise refers to those organizations that (a) use the privacy labeling tool and (b) publish their privacy labels. For these enterprises, there are two technical artifacts to *adopt*: the privacy label and the labeling tool. Therefore, a successful adoption of these two technical artifacts relies on those theories that explain technology adoption by consumers and by/within organizations. As our study focuses on technology adoption within organizations (more precisely, within SMEs), we organized our interviews and analyzed our results based on the corresponding technology adoption theories, as summarized below.

The Technology-Organization-Environmental (TOE) framework [21] is widely used for studying IT adoption in organizations, including SMEs. The TOE framework comprises three main contexts of Technology (T); Organization (O) and Environment (E), each of which contains a set of determinants that impact the adoption of innovation in organizations [2, 3].

- Technology context, which comprises technologies within an organization and those externally available,
- Organization context, which refers to the characteristics of the organization such as its size, communication processes and the amount of slack resource, and
- Environment context, which captures the structure of the industry, pressure from competitors and partners, and the regulatory environment.

The technology context can be characterized by five technology attributes in the Diffusion of Innovation
(DOI) theory [2, 18]. The DOI's technology attributes, which may influence the adoption or rejection of a given technology in organizations, are: Relative advantage (or perceived benefit), complexity (or perceived ease of use), compatibility (or perceived compatibility), trialability (via, e.g., offering the trial versions of the technology and providing information about it), and observability (referring to the visibility of an organization due to its adoption of the technology). The compatibility attribute is about whether the potential changes are compatible with the values, needs and practices as well as whether they are consistent with the existing technological infrastructure of the organization.

The organization context can be characterized by factors such as [2]: Enterprise size and scope (often, the larger organizations are, the better technology adoption is), top management support and CEOs' innovativeness (facilitating the adoption decision), and experience with and knowledge about previous technologies. The environment context encompasses several factors that affect an organization's decision to adopt new technologies such as [2]: Competitive pressure, customer pressure, industry type, the market scope encompassing an organization's operations, and external IS

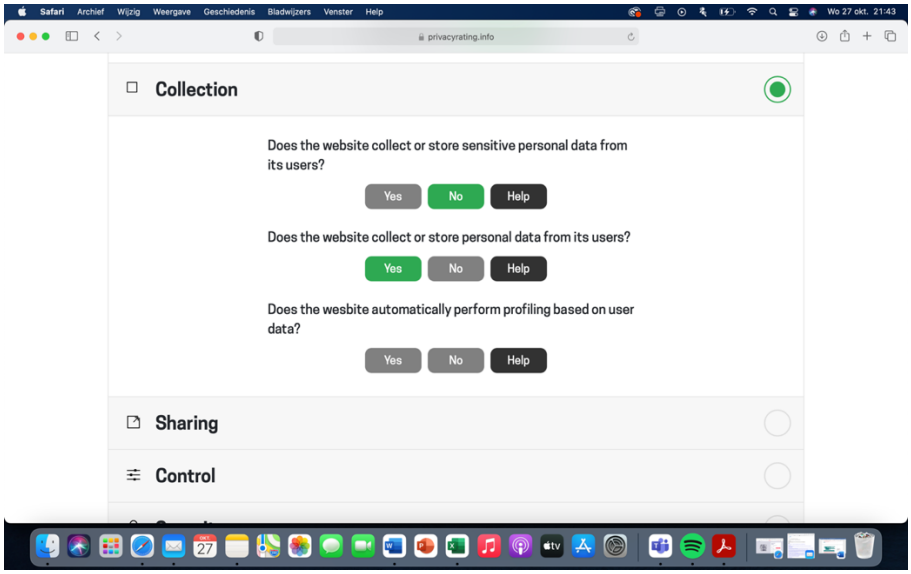

Figure 4: A screenshot of a section of the online tool designed in the SERIOUS project.

support. External IS support may affect adoption of a new technology especially for SME's as they often have limited resources and skills to deploy and use a new technology.

Most of the abovementioned factors are relevant for SMEs, as shown in many studies in recent years. For references to these studies, the interested reader is referred to [2], chapter 2.

Based on the technology adoption factors mentioned above, we prepared some questions to loosely shape our semi-structured interviews. Example questions were: What does privacy mean for your organization? How do you perceive the label and the labeling tool? What are the improvement aspects of the label and its tool? What do you see as the added value of the label and the labeling tool for your organization? How would you be willing to use them? What other facilitators (inside and outside your organization) are needed to use the label and the labeling tool in your organization?

3.2 Interview procedures

We conducted three qualitative studies with three SMEs from three different sectors of retail, culture and media. For each SME, two different sessions were organized. During the first session, the participants of each SME were introduced to the web-based online tool of the SERIOUS project for creating the SERIOUS privacy label. The second session consisted of an in-depth semi-structured interview about the web-based tool and the privacy label for the corresponding SME. Hence, in total, three SME interviews, each in two sessions, have been performed.

3.2.1 First sessions: Introduction round. During the first session, the three SMEs from the retail, media and culture domain, were introduced to the privacy label and accompanying online tool. In each of the first sessions, two researchers were present. The objective of the first session for each SME was to use the online SERIOUS tool and create a sensible SERIOUS privacy label for one online service of the SME. This tool is a web-based interactive questionnaire [16] developed in the SERIOUS project. As illustrated in Figure 4, the SME participants provided their answers, with either yes or no, to some questions posed by the tool in the categories of collection, sharing, control and security. The structure behind the tool is like a flowchart, so the questions that are presented to the user depend on their previous answers.

Due to the COVID-19 restrictions at the time, the sessions took place online via a Microsoft Teams call. Each session took around 30 minutes, where we started with a short introduction of the project, the researchers and the participants. The participants were asked to answer the questions posed in the labeling tool, keeping in mind a specific and relevant online service within their SME. For all three SMEs, this was their website. As stated in the instructions of the tool, the answers should be based on the worst-case scenario (i.e., most severe privacy risks) that can be imagined when operating their websites.

Next, the SMEs were guided through the online tool, interfering as little as possible to receive their genuine reaction to the tool and label as they observe on their own device. During this session, the participants were sharing their screen so it could be recorded by the researchers for later analysis. The result of the first session was a privacy label, as shown in Figure 1, for the website of the corresponding SME. The participants were able to use the resulting label code, which was provided by the tool, to implement the label into their website or download the visualization as a png or svg file. The participants were asked to save the label and share the file with the researchers.

3.2.2 Second sessions: Semi-structured interview. Following the first introduction sessions, a semi-structured interview session was conducted with each partner, so three interview sessions in total. Two researchers were present during each interview session. Again, due to the COVID-19 restrictions at the time, the interviews took place

online via a Microsoft Teams call. The interviews were about 1 hour long each.

The interviews were used to gain a more in-depth understanding of the experience of the participants with the labeling tool and their thoughts about the privacy label. During these interviews a semi-structured interview guide was followed. The topics and questions were constructed based on the guidelines in Section 3.1 and in the following categories:

- Reflection on the first session topics, like on the produced privacy label, the online tool used – the user interaction aspects, and the online tool used – the content of the questions posed by the tool,
- Use of the privacy label (in practice),
- Facilitation of the privacy label deployment (within the organization), and
- Reliability and risks of the privacy label.

3.2.3 Analysis. The analysis of the semi-structured interviews consisted of multiple steps, namely: collection, selection, categorization and validation. First, the recorded interviews were transcribed. This transcription allowed us to extract the relevant quotes and insights from the interviews. Subsequently, three researchers of this project held an online session, again due to the COVID-19 restrictions at the time, to cluster the quotes and insights from the interviews based on the discussed topics and using the online service Miro. The topic clusters were checked and labelled in 27 categories during this meeting, some more relevant and important than others.

Some example categories are: Complexity of the problem (i.e., privacy visualization) vs. the simplicity of the tool, service-specific label or organization-specific label, dependency on external partners and the network effect, and missing question categories. In Section 4.2, we shall group these categories in 5 clusters to structure our recommendations for future research directions.

4 DISCUSSION

In this section we present the preliminary results (derived before our data analysis) in Section 4.1 and provide our recommendations for future research in Section 4.2.

4.1 Preliminary results

From the discussions in the first sessions some preliminary insights were gained, namely:

- Some questions were difficult to understand, sometimes simply because of a language barrier, the help button proved to be useful in these situations,
- Answering questions for the worst-case scenario was applicable when, for example, there were multiple purposes for data collection due to having multiple (external) services linked to the SME websites. In these scenarios, the participant wanted to be able to give more nuanced answers than a hard yes or no, and
- All participants considered the label as a very useful tool, but the following question was mentioned by all SMEs: how will the privacy label be regulated? What is the credibility of the label?

From the interviews in the second sessions some preliminary insights were gained:

- Sometimes the questions could not be answered with a simple yes or no as the issue is complex. The tool asks to answer the questions according to the worst-case scenario, but this is not always right/satisfactory,
- The SMEs provide different online services – such as those for organizing online events, conducting ecommerce transactions, and providing informational – that entail having different and multiple outcomes for the privacy label (or multiple labels). Thus, the question that rises is: should SMEs use separate privacy labels for their different online activities?
- The SMEs use the online services of external parties because they do not have the capacity to provide them inhouse. Thus, the question that rises is: How should these service compositions be included in the privacy label?
- The SMEs do not have an allocated place and/or a responsible person/expert within the organization for handling privacy or possibly the privacy label, and
- As a result of the introduction sessions, the credibility and accountability of the privacy label is important to take into consideration for its implementation and deployment within and among organizations/SMEs.

The initial results and insights were presented during a session with two of the original developers of the SERIOUS privacy label and the SERIOUS labeling tool. The developers provided their feedback to the preliminary insights of this project, these were:

- The network effect was an aspect they did not find and realize during their research, probably due to their focus on the end users instead of on the organization providing the label. They understood the possible implications for the privacy label and endorsed further explorations on this topic.
- They confirmed the relevance of future research on how to implement and position the privacy label in SMEs.

4.2 Recommendations for future research

In this section we provide our recommendations for future research through clustering the 27 categories identified in our data analysis. Note that there are some dependencies among these clusters.

4.2.1 Trust in privacy label. The aim of using privacy labels is to provide transparency about the privacy practice of the organizations providing online services and apps. As such, consumers (e.g., the average users of privacy labels) should trust the labels in being, among others, reliable, truthful, and understandable. Considering the generic setting depicted in Figure 2, a relevant research question is: How can consumers (i.e., individuals and other organizations) trust the privacy label issued by/for an SME?

- Should a standard process be developed for issuing the privacy label? Should the label be issued by a trusted third party or do self-issued labels suffice?
- In the latter case of self-issued labels, is it necessary to introduce a trusted third party to supervise and monitor the process? What are the accountability and compliance issues

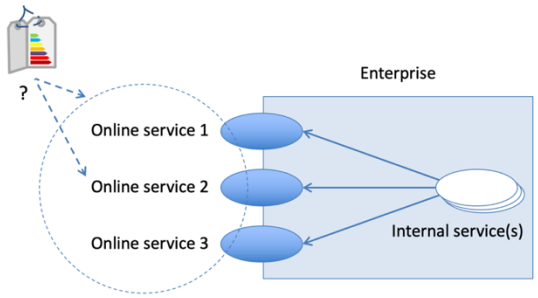

Figure 5: An enterprise offering multiple online services: a privacy label per service or for all services?

for an SME regarding own privacy label(s)? What are measures against these issues? And how can these measures be enforced?

Answering these questions asks for, among others, developing legislative and standardization measures.

4.2.2 Network aspects. An enterprise (or SME) may offer many online services as depicted in Figure 5. The current privacy label (i.e., that of the SERIOUS project) advocates issuing a privacy label for the worst-case online service (from a privacy protection perspective). However, it might be foreseeable or preferable to introduce separate labels for services of an SME. Therefore, a relevant research question is: How can we accommodate the differences in the services provided by SMEs in privacy labels? More specifically,

- Is it sufficient to introduce a privacy label per SME? Or
- Is it necessary (or preferred) to introduce a privacy label per SME online service?

Online services have different requirements about collecting and processing personal information, some require minimal personal information (like informative web-pages of SMEs for publicity purposes) and some require a considerable amount of personal information (like those used for customer relation management). Consequently, the privacy label of the former can be greenish while that of the latter can be more reddish if we follow the same scoring rules for both types of online services. In this case, the consumers should (be able to) interpret the resulting labels according to the context (i.e., the types of the services they represent). This approach might inflict burdens on laymen for the required context dependent interpretation of the labels. Alternatively, one may normalize privacy labels for all types of online services (i.e., a label normalized with respect to the needs of personal information of an online service) so that a semantically uniform label can be created for all services with varying needs of personal information. Hereby the interpretation of the label becomes straightforward for average humans. A relevant research question is: How can we accommodate the different degrees of personal information dependency of online services in such (normalized) privacy labels? More specifically,

- Do we need to define a privacy label per online service type? Or
- Should we define a normalized privacy label across all online services of an SME?

Provisioning the online service of an SME may depend on (online) services provisioned by other enterprises, as depicted in Figure 6. A key research question is: How should the privacy practices of the services of external partners (i.e., the providers of upstream services used by the SME's) be represented in the privacy label? More specifically,

- Should these upstream service providers also have their own privacy labels? If so, what would the SME do if the privacy practices of upstream service providers (negatively) affect the privacy label of the SME? How can these upstream labels be trusted by downstream SMEs?
- How should SMEs deal with the changes of the privacy practices of these upstream SMEs?

One research direction to remedy the need for having the privacy labels of upstream service providers is to develop automated systems, tools and architectures that help estimating the privacy practices/labels based on the operational behaviors of the corresponding services, for an example see [4].

4.2.3 Technology adoption aspects. The privacy label and the tools for creating privacy labels should be adopted by both label issuing enterprises and label consuming parties (individuals and organizations). While this study did not consider how consumers perceive the privacy label as it is, to some degree, done in [8], we observed that label issuing SMEs perceive the privacy labels and the labeling tool useful. Nevertheless, there is a need for further research about the ways for enhancing the label adoption by label issuing enterprises, who may act also as consumers of privacy labels in networked settings. The key research question is: How should the privacy label and labeling tools be implemented within SMEs? More specifically,

- How can the adoption of privacy labels be facilitated for SMEs?
- Should a central organization be set up to help SMEs to manage (i.e., create and maintain) their privacy labels?
- How often should the privacy label be updated? Who is responsible for these updates?
- Can SMEs use the privacy label (and the labelling tool) to get insight into their own privacy practice and how they can use the insight to improve their own privacy practice?

4.2.4 Using for audit purposes. When using the SERIOUS privacy tool to create the SERIOUS label, the provider of an online service must reflect on the key requirements of privacy protection regarding that service or app. Answering the questions of the tool and seeing the colors of the resulting label can lead to gaining insight into the aspects of the privacy protection which are done satisfactorily (i.e., those four classes of the label that are greenish) and unsatisfactorily (i.e., those four classes of the label that are reddish). The providers can compare the status of own labels with those of similar products (of other providers) or with those of the same online service and app in previous times. The former provides a cross-product insight and the latter provides a longitudinal insight into the privacy practice. These insights can be instrumental for SMEs to decide on which mitigations measures are necessary to adopt or whether to promote their services and apps based on the way that privacy protection is done (i.e., as the unique selling point).

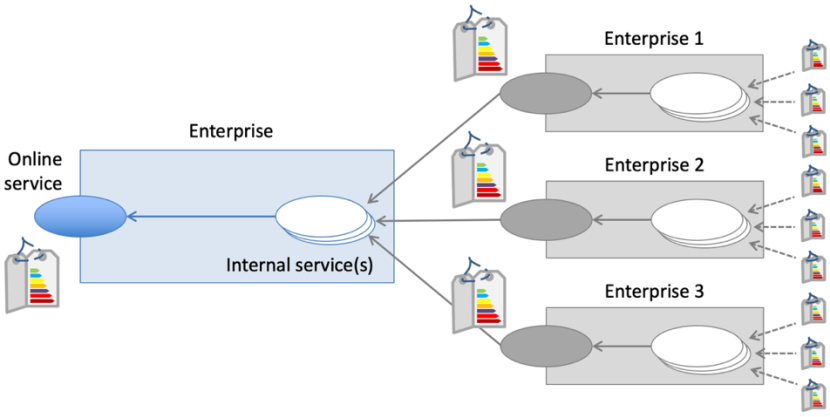

Figure 6: An illustration of the chain of trust issue, the need for trusting the upstream privacy labels.

The key research question is: How can SMEs use the label and tool to gain insight into their own privacy practice? More specifically,

- Do the privacy label and the labeling tool provide enough insight into the privacy practice of SMEs? Are they preferable to similar auditing products?
- How can SMEs use the gained insight to improve their own privacy practice?

4.2.5 Improvement aspects. The current privacy label and tool are a proof-of-concept realization that needs some developments in order to be used by SMEs with limited resources and in different settings (e.g., when offering various services, having composite and networked services, and acting in different business sectors). Therefore, an important research question is concerned with further development of the concept of the privacy label and the corresponding labelling tool. More specifically,

- How the privacy label can be improved for the heterogeneous and constrained SME settings?
- How the privacy labeling tool can be improved for such SME settings?
- Is it possible to automate some aspects of the labelling process, especially in networked service provisioning?

5 CONCLUSION

Privacy visualization via a label representation, like energy and food labels, is considered a promising solution direction to make privacy practices of online service and app providers transparent. In this feasibility study we interviewed three SMEs from retail, media and culture business domains to investigate the capabilities and limitations of the SERIOUS privacy label and its labeling tool for use by SMEs as well as to identify some future research and development directions.

As its outcome, the study identified several potentials and limitations of the SERIOUS label and its labeling tool. Based on these, the identified research and development directions are: Trusting the privacy label, dealing with network aspects, adopting technology within SMEs, using the label and tool for auditing and improving own privacy practice, and improving the current label and labeling tool. SMEs may operate multiple online services and every online service is often provided by multiple service providers. How these differences in services provided by SMEs and the networking characteristic of these services can be accommodated in (deploying) privacy labels are open issues for existing privacy labels. SMEs have limited resources and privacy labels are relatively new concepts. Therefore, one needs to seek for effective ways to promote the use and adoption of privacy label and tools within SMEs. From the interviewees we found that the current privacy label and labeling tool are insightful about own privacy practice (e.g., knowing which parts of the practice require applying mitigation measures). As the current SERIOUS label and tool are proof-of-concepts designed for single enterprise settings, addressing the abovementioned issues asks for their further development, for example, via automizing part of the label issuing process and its usage within networked settings.

ACKNOWLEDGMENTS

The authors would like to thank Ben van Lier and Peter Troxler for useful discussions and to thank Menno de Jong and Susanne Barth for providing their feedbacks on the early results of this study.

REFERENCES

[1] Salma Abed, 2018. A Critical Review of Empirical Research Examining SMEs Adoption from Selected Journals. The 17th Conference on e-Business, e-Services and e-Society (I3E), Oct. Kuwait City, Kuwait, 577- 587
[2] Hafedh S.A. AL Rahbi, 2017. Factors influencing social media adoption in Small and Medium Enterprises (SMEs), PhD Thesis, Brunel University London.
[3] Baker, 2012. The technology–organization–environment framework. In Information systems theory. Springer, 231-245.
[4] Masoud Barati and Omar Rana, 2021. Privacy-aware cloud ecosystems: Architecture and performance. In Concurrency and Computation: Practice and Experience (CCPE), Volume 33 (issue 23), e5852, Wiley.
[5] Mortaza S. Bargh and Sunil Choenni, 2019. Towards applying design-thinking for designing privacy-protecting information systems. In Proceedings of the 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS'19), Los Angeles, California, USA (Co-located with IEEE CIC 2019 & IEEE CogMI 2019), December 12-14.
[6] Mortaza S. Bargh, Sunil Choenni and Ronald Meijer, 2015. Privacy and information sharing in a judicial setting: A wicked problem. In Proceedings of the 16th Annual International Conference on Digital Government Research, May, 97-106.
[7] Susan B. Barnes, 2006. A privacy paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394.
[8] Susanne Barth, 2021. Data, data, and even more data: Empowering users to make well-informed decisions about online privacy, PhD dissertation, University of Twente, The Netherlands.

[9] Susanne Barth, Dan Ionita, Menno D.T. de Jong, Pieter H. Hartel and Marianne Junger, 2021. Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services. IEEE Transactions on Professional Communication, 64(4), 354-373.

[10] Sunil Choenni, Mortaza S. Bargh, Carmelita Roepan, and Ronald Meijer, 2016. Privacy and security in data collection by citizens. Book chapter in Smarter as the New Urban Agenda: a Comprehensive View of the 21st Century City, edited by J.R. Gil-Garcia, T.A. Pardo and T. Nam, Springer LNCS.

[11] Benjamin Edelman, 2011. Adverse selection in online "trust" certifications and search results. In Electronic Commerce Research and Applications, Volume 10, Issue 1, Pages 17-25, https://doi.org/10.1016/j.elerap.2010.06.001.

[12] GDPR, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[13] Erind Hoti, 2015. The technological, organizational and environmental framework of IS innovation adaption in small and medium enterprises. Evidence from research over the last 10 years. International Journal of Business and Management, 3(4), 1-14.

[14] Jaarbericht Staat van het mkb, 2020. Ondernemen is vooruitzien, Nederlands Comitevoor Ondernemerschap, https://cms.staatvanhetmkb.nl/wp-content/uploads/2020/12/Jaarbericht-staat-van-het-mkb-2020.pdf.

[15] Ruwan Nagahawatta, Mathew Warren, Sachithra Lokuge and Scott Salzman, 2021. Security and privacy factors influencing the adoption of cloud computing in Australian SMEs.

[16] Privacy Rating, 2021. The tool for deriving the privacy label of the SERIOUS project, available: www.privacyrating.info

[17] SERIOUS. 2021. Security Requirements for Serious Apps project, funded by Dutch Research Council (abbreviated as NWO in Dutch), https://www.utwente.nl/en/eemcs/scs/research/finished-projects/20200423-security-requirements-for-serious-apps/.

[18] Everett M. Rogers, 2010. Diffusion of innovations. Simon and Schuster.

[19] Paul Taylor, 2019. Information and Communication Technology (ICT) adoption by small and medium enterprises in developing countries: The effects of leader, organizational and market environment factors. International Journal of Economics, Commerce and Management United Kingdom, 7(5).

[20] Paul Taylor, 2015. The importance of information and communication technologies (ICTs): An integration of the extant literature on ICT adoption in small and medium enterprises. International journal of economics, commerce and management, 3(5).

[21] Louis G. Tornatzky, Mitchel Fleischer and Alok K. Chakrabarti, 1990. The Processes of Technological Innovation. Lexington, Mass: Lexington Books.