A case study on the implementation of the right of access in privacy dashboards*

Jan Tolsdorf[1] [0000−0002−1961−100X], Michael Fischer, and Luigi Lo Iacono[1] [0000−0002−7863−0622]

H-BRS University of Applied Sciences, Germany
[1] Data and Application Security Group
https://das.h-brs.de/
{jan.tolsdorf, luigi.lo_iacono}@h-brs.de, michaelfischer5@web.de

Abstract. The right of access under Art. 15 of the General Data Protection Regulation (GDPR) grants data subjects the right to obtain comprehensive information about the processing of personal data from a controller, including a copy of the data. Privacy dashboards have been discussed as possible tools for implementing this right, and are increasingly found in practice. However, investigations of real world implementations are sparse. We therefore qualitatively examined the extent to which privacy dashboards of ten online services complied with the essential requirements of Art. 15 GDPR. For this, we compared the information provided in dashboards with the information provided in privacy statements and data exports. We found that most privacy dashboards provided a decent initial overview, but lacked important information about purposes, recipients, sources, and categories of data that online users consider to be sensitive. In addition, both the privacy dashboards and the data exports lacked copies of personal data that were processed according to the online services' own privacy statements. We discuss the strengths and weaknesses of current implementations in terms of their ability to fulfill the objective of Art. 15 GDPR, namely to create awareness about data processing. We conclude by providing an outlook on what steps would be necessary for privacy dashboards to facilitate the exercise of the right of access and to provide real added value for online users.

Keywords: GDPR · right of access · privacy dashboards.

1 Introduction

The GDPR [11] provides users of online services operating in the European Union (EU) with many rights to maintain control over their personal data. A

* Supported by the German Federal Ministry of Education and Research (BMBF) under the research project "TrUSD - Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen" (transparent and self-determined design of data use in organizations) (16KIS0899).
The final authenticated publication is available online at https://doi.org/10.1007/978-3-030-76663-4_2

prerequisite for the GDPR to be effective, however, is the requirement that controllers comply with their obligations by implementing adequate processes as well as providing their users with tools to exercise their rights. Much of recent work has revealed weaknesses in the implementation of such tools such as intrusive consent forms [45] and incomprehensible privacy statements [15,46]. Certainly, research has merely focused on problems and solutions with regards to ex-ante control and therefore on rights that apply prior to processing. However, the GDPR, and in particular the right of access under Art. 15, aim to ensure that data subjects are aware of the extent of processing at all times: before, during, and after processing. The right of access is special in the sense that it requires data subjects to exercise this right regularly and independently in order to become truly aware of the processing of their personal data. Research suggests, however, that people are either unaware of their rights or reluctant to make the effort to exercise them [2,34]. To address this problem, the use of prominently placed tools for ex-post control in the form of privacy dashboards is gaining traction, since such tools provide users both with transparency and intervention mechanisms. Research suggests that the use of privacy dashboards both facilitates data controllers' obligation to provide transparency and intervention options to their users and ease data subjects' exercise of their rights [5,33,35]. In practice, online services also already refer data subjects to use these tools for exercising their rights in privacy statements or FAQs, in particular with regards to the right of access.[1] Different to ex-ante control, however, there is currently a lack of research about real world implementations of tools for ex-post control.

This paper constitutes a first step towards closing this gap, by providing an overview of privacy dashboards found in practice, with a particular focus on the right of access. More precisely, our contributions are guided by the overall research question *"to what extent are privacy dashboards found in practice used to implement the right of access under Art. 15 GDPR?"*. For this purpose, we evaluated the information provided by privacy dashboards, data exports, formal requests for access, and privacy statements with ten popular online services operating in different business domains in the EU. The key insights are:

- We found that none of the examined privacy dashboards complied with the requirements of the right of access, and that the information provided was incomplete with respect to purposes, external recipients, external sources, and categories of data listed in the respective privacy statements. Overall, privacy dashboards contained rich information about personal data directly related to individuals or their interactions with a service, but lacked most of the information about personal data that are technical in nature and considered as highly sensitive by online users.
- Furthermore we found that all but one online service provided incomplete personal data in their data exports. For 6/10 online services, the data also differed between privacy dashboards and data exports, and the union of

[1] https://privacy.microsoft.com/en-us/privacystatement
https://support.google.com/accounts/answer/162744?hl=en

both increased the overall amount of information. For another 6/10 online services, privacy dashboards provided less information compared to exports.
- We conclude that the privacy dashboards found in practice have the potential to become a good compromise between the time and effort required for exercising the right of access compared to the extent of information provided. However, they leave lay people in an uninformed state due to a lack of important information.

We consider our results a valuable contribution to previous research on the monitoring and examination of the implementation of the right of access by online services, and complement towards a holistic picture of the GDPR in practice [2,4,8,26,44,47]. To the best of our knowledge, we are the first to investigate the use of privacy dashboards found in practice with regards to their compliance with Art. 15 GDPR by conducting a target/actual comparison of the information provided with respect to online services' privacy statements. Researchers, practitioners, and policy makers may use our results as means to become aware of possible pitfalls when using or implementing privacy dashboards, and as a basis for further research and regulation.

The rest of this paper is structured as follows: first, we present related work on the right of access and privacy dashboards. We then provide details on our procedure and methods for investigating the current implementation of the right of access in privacy dashboards for a sample of ten online services. We then present the results of our study for each online service as well as a summary of findings. We finally discuss our findings and give an outlook for future work.

2 Related work

We discuss related work with a focus on the right of access and the use of privacy dashboards to accommodate the fundamental objectives of the GDPR with regards to transparency and intervention.

2.1 Right of access

The right of access under Art. 15 GDPR consists of three key paragraphs:

(Art. 15 para. 1 GDPR) – The obligation for controllers to inform data subjects whether personal data are processed, including but not limited to details about the categories of data concerned, the purposes of the processing, and the (categories of) recipients to whom the data are disclosed;

(Art. 15 para. 2 GDPR) – The obligation for controllers to inform data subjects about the safeguards taken when transferring personal data to third countries or international organizations;

(Art. 15 para. 3 GDPR) – And the right of data subjects to obtain a copy of the personal data processed by a controller. If the request is made digitally, the copy must also be provided in a "commonly used electronic form".

The rights described in Art. 15 para. 1 GDPR have been available to EU citizens since 1995, yet they have regained visibility since the GDPR came into force in 2018. Back then, the right of access made headlines with an NGO filing strategic complaints against large online services who did not comply with the new regulation.[2] Lately, academia has also started to explore the implementation of the different rights available to data subjects in more depth, finding that 20% of the most popular online services did not comply with their basic obligations on informing data subjects one year after the GDPR came into force [8].

Moreover, Art. 15 para. 3 GDPR and the novel right of data portability under Art. 20 GDPR drew researchers' attention too. These articles differ in that the former only obliges controllers to supply a copy of the data, whereas the latter also demands the use of structured data formats to allow data subjects reusing their personal data for their own purposes and also in other services. However, previous studies found that controllers provide the same data formats (e.g. JSON, PDF) for both the right of access and the right of data portability [8,47]. Thereby, the data formats are very heterogeneous [8,44,47] and the number of GDPR compliant file formats can be as low as 40% [47]. Research demonstrated that the usability and perceived usefulness of structured data formats are rather low [5]. Also, a recent qualitative survey on consumer expectations of the right of access for a loyalty program in Germany found that data subjects are more interested in what controllers infer from their personal data, rather than simply knowing what personal data are processed [2]. These findings are also supported by work on transparency conducted prior to the GDPR [21].

The right of access is further governed by the provisions of Art. 12 GDPR, which obliges controllers to verify the identity of the person making the request for access. However, there does not exist a uniform process. Instead, data protection authorities provide different recommendations and controllers' authentication procedures were found to be unsafe in practice [6]. Also, previous studies demonstrated that the right of access can be abused to access personal data of foreigners due to flaws in the authentication process of controllers [10,31,26].

Moreover, Art. 12 para. 3 GDPR provides that controllers must respond to requests for access within one month, but may extend this time span by two months if they can demonstrate the high efforts involved. Previous studies revealed a mixed picture in this respect. In [44], 55% out of 38 online tracking companies responded in time, whereas in [8] 89% out of 212 controllers responded in time. Similarly, the authors of [47] examined the right of data portability and found that 70% out of 230 controllers responded in time.

To the best of our knowledge, there is a lack of studies verifying whether the information provided under the right of access is complete with respect to the personal data processed by controllers, and to what extent the provided information differs between different sources. We provide first insights on this matter by systematically comparing the information retrieved when exercising the right of access with the information provided in controllers' privacy statements. Also,

[2] https://noyb.eu/en/netflix-spotify-youtube-eight-strategic-complaints-filed-right-access

we provide insights on the type and amount of information provided to data subjects in privacy dashboards, data exports, and formal requests for access.

2.2 Privacy dashboards

Privacy dashboards are transparency tools specially adapted to the context of information privacy, and have repeatedly been identified as helpful in the context of the GDPR for implementing legal obligations, including the right of access [5,35]. Privacy dashboards have been established in the area of (social) online services and are intended to provide their users with an overview and control (through appropriate settings) of their personal data processed by a controller [35,48]. They are classified as transparency-enhancing tools (TETs) and constitute proven patterns for the implementation of privacy-friendly systems, so-called privacy transparency patterns (PTPs) [39]. Privacy dashboards are special in the sense that they comprise multiple different PTPs appropriate to the context and in order to provide functions to promote transparency. They may provide the following essential privacy controls [5,39,48]:

1. *Overview* – All personal data available to a controller about a data subject together with the associated information (e.g., recipients, purposes) and data flow are presented in a clearly understandable and structured manner. This makes it possible to sensitize users to the extent of their data disclosures and potential consequences for privacy [7].
2. *Verifiability* – Data subjects may understand the current and future processing (e.g., collection, use) of their personal data. This enables data subjects to check the lawfulness of processing and to hold data processors liable in the event of violations [20].
3. *Intervention* – Data subjects may actively influence the processing of their personal data. In particular, they are provided with control over the data stored, and may also initiate corrections or deletions on their own [3,5,35].

Academia has recognized and discussed the value of tools similar to privacy dashboards to support online users in their information privacy a long time before the GDPR came into force (e.g. [3,7,22,38]). However, their implementation as a means to accommodate the legal requirements of the GDPR has gained popularity in recent years, including contexts other than online services [5,24,27,33,35,43]. As a result, research has defined several requirements for privacy dashboards that provide guidance on (1) how to accommodate legal requirements [5,35], (2) the architecture and technical prerequisites [5,27,32], and (3) the constraints for usability and stakeholder requirements [5,32,35,43]. In conclusion, Raschke et al. [35] postulated that privacy dashboards must implement four tasks to support data subjects in their rights: **(T1)** Execute the right of access; **(T2)** Obtain information about involved processors; **(T3)** Request rectification or erasure of data; **(T4)** Consent review and withdrawal.

In terms of benefits to controllers, research suggests that providing privacy dashboards increase user trust in online services [9,18]. This increase is attributed to the tools' transparency properties in particular. A case study on the Google dashboard demonstrated that privacy dashboards may also increase users' willingness to disclose personal data [9]. However, limited intervention options or information known to be lacking may have adverse effects [18].

A look at real world data controllers reveals that the majority of online services only recently started implementing different forms of privacy dashboards themselves. However, investigations on these tools are strongly limited to the Google dashboard so far and focused on user attitudes [9] and theoretical concepts [29,48]. To the best of our knowledge, we are the first to systematically examine the scope of information and functions provided by multiple different privacy dashboard implementations found in practice, and with special regards to their compliance with the right of access Art. 15 GDPR. We highlight existing problems and discuss possible solutions to increase the value of privacy dashboards for both data subjects and controllers.

3 Methodology

We conducted a qualitative study to examine the extent to which privacy dashboards found in practice already accommodate the right of access with ten popular online services during the period October and December 2020. For this purpose, we created accounts with these online services and simulated their use with different devices and recorded all activities in a logbook. We then analyzed the information provided by dashboards with controllers' privacy statements and information obtained from data exports. In the following, we provide details on the applied methodology and evaluation of the data. An overview of our methodology is shown in Fig. 1.

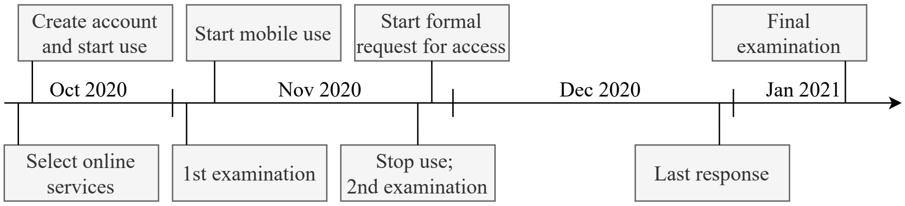

Fig. 1. Chronology of online service use and examination of provided information.

3.1 Selection of online services

For our case study, we aimed to gain an overview of the use of privacy dashboards by online services operating in different fields and contexts that online users in the EU frequently interact with. According to the Digital Economy and Society Index [41] and the annual survey on Information and Communication

Technologies [40], the top six categories of online services used by European internet users are music, videos and games (81%), email and communication (75%), news (72%), shopping (71%), banking (66%), and online social networks (65%). For further investigation, we excluded news and banking services because the former often does not require the creation of accounts nor the provision of personal data, whereas the latter requires high efforts for the creation of accounts. We therefore focused on providers of music streaming, video streaming, email, shopping, and social online networks.

We used the Tranco list[3] [23] created on 14 October 2020 to screen the top 100 online services for possible candidates for our investigation. First, we excluded services that are unavailable in German, and then extracted possible candidates for each of the five categories. Next, we reviewed the different services in order of appearance in the Tranco list and examined whether a service offered a privacy dashboard or at least similar functionalities with regards to Art. 15 GDPR. For this purpose, we inspected a provider's website and privacy statement, and signed up for an account if we were unsure about the provided functionality. If a service did not conform with our requirements, we continued with the next service in the list. After we successfully identified a candidate for each category, we stopped our screening. We then repeated the previously described steps for online services that were less popular, but offered similar services compared to the five selected online services. To do this, we conducted a partial online search to find suitable candidates. Based on our screening, we have ultimately picked the following online services:

- Audio streaming: Spotify (Tranco: 80), Deezer (Tranco: 1461)
- Video streaming: Netflix (Tranco: 8), Rakuten TV (Tranco: 43297)
- Shopping: Amazon (Tranco: 18), Zalando (Tranco: 7439)
- Email and search engine: Google (Tranco: 1), Yahoo (Tranco: 17)
- Social network: Facebook (Tranco: 2), LinkedIn (Tranco: 9)

3.2 Sign-up and use of online services

We created accounts for each online service and provided information about basic demographics (e.g., age, sex), contact data (e.g., name, address), and financial information (e.g., credit card) if applicable. When possible, we used the web version of a service as well as the mobile app (Android) in order to allow the processing of additional meta data (e.g., device ID). We interacted with each service at multiple different points in time in order to generate data about community and service interactions (e.g., creating playlists, streaming media, sending emails, liking groups). We monitored our interactions with a service for the upcoming examination step. More precisely, we recorded the details of the personal data we disclosed along with information about our technical devices in a logbook.

[3] https://tranco-list.eu/list/W3W9

3.3 Examination of the right of access

After we successfully set up all the accounts, we aimed for examining which information and functionality are provided by privacy dashboards. First, we extracted required information from privacy statements of online services and then exercised the right of access using (1) privacy dashboards, a user generated (2) data export, as well as a (3) formal request for access. Our investigation consisted of the various steps described below.

Preparation phase – We started our investigation by inspecting each providers' privacy statement with particular attention to the different recipients, data sources other than the data subject, purposes for processing, and categories of data claimed to be processed. We extracted this information for each provider and double checked our findings with the information provided by Pribot[4], a tool that analyzes privacy statements based on deep learning [17]. Next, we consolidated our findings and identified commonalities between the different privacy statements of all online services. For this, we built a union list of all purposes, recipients, sources, and data categories.

In order to allow drawing conclusions about the expected user perceived sensitivity of the different data, we classified the data into six different groups, following the identified clusters by Milne et al. [28]: Basic demographics (low sensitivity), personal preferences (low to medium sensitivity), community and service interaction (medium sensitivity), financial information (medium to high sensitivity), contact information (medium to high sensitivity), and technical identifiers or data (high sensitivity). While Milne et al. focused on online users in Brazil and the U.S., there is evidence that data sensitivity does not differ significantly for European online users [25,36].

Examination of dashboards – For each online service, we examined the information and functions provided in the respective dashboards with a particular focus on the tasks T1–T4 defined by Raschke et al. [35] (cf. Sec. 2.2). We examined whether and which information about purposes, recipients, data sources, and personal data was displayed or referenced in the privacy settings and additional info texts. We documented our findings using the lists created during the preparation phase. Furthermore, we examined whether the dashboards provided functions for (1) downloading a copy of the data, (2) restricting or at least limiting data processing, and (3) editing and deleting personal data. Here, we only checked whether the function was present or not, but did not quantify our findings for the different categories of data.

Examination of data exports – When possible, we downloaded a copy of personal data using the dashboard at the beginning of our study and again after two weeks to compare the different data exports (cf. Fig. 1). We manually examined each export and extracted the different categories of data. Again, we documented whether and which data were present or missing based on our logbook and the

[4] https://pribot.org/polisis

list of categories of data created during the preparation phase. We also recorded the response formats and response time.

Formal request for access – After we finished examining the data exports and identified missing information or personal data, we started a formal request for access by contacting each provider via email or online-forms. We specifically asked for the categories of data that were missing from the exports with respect to their privacy statements and our logbook. Once we received the final response to our request, we repeated the steps taken for analyzing exports described above.

4 Results

In the following section, we present the results of our investigation. First, we report our findings on the information provided in privacy statements, followed by the results of our investigation of the different dashboards for each online service. We then summarize our findings and report on the overall completeness of information found in privacy dashboards.

4.1 Information in privacy statements

Recipients and sources – In total, we identified 13 categories of recipients, and six categories of external data sources. Half the privacy statements listed at least six recipients ($min = 4,\ max = 9$) and two sources ($min = 0,\ max = 4$). All online services stated their *corporate group* and *public authorities* as recipients. Seven online services each also mentioned *advertisers*, *owners*, or *service providers*, and five online services mentioned *third-party providers.* Three of the examined online services even provided the exact (company) name of the recipients. With regards to external sources, five online services each referred to *third-party providers* and *service providers*, four online services mentioned *advertisers*, and three online services stated that they also process *publicly accessible information.*

Purposes – We extracted 22 different purposes for processing from the privacy statements provided by the online services. Half the online services listed at least 11 purposes ($min = 9,\ max = 17$). The five purposes included in all privacy statements comprised *providing the service*, *troubleshooting and improving the service*, *customizing the service experience*, *advertising*, and *preventing fraud.* Moreover, only two providers, namely Spotify and Deezer, clearly stated which personal data were processed for each purpose.

Categories of data – Looking at the individual online services, we found that each privacy statement listed 32 different categories of data on average ($min = 21,\ max = 48,\ sd = 7$). Yet, only eight categories of data were processed by all service providers, from which five categories belonged to technical data. In total, we extracted 77 different categories of data from all privacy statements.

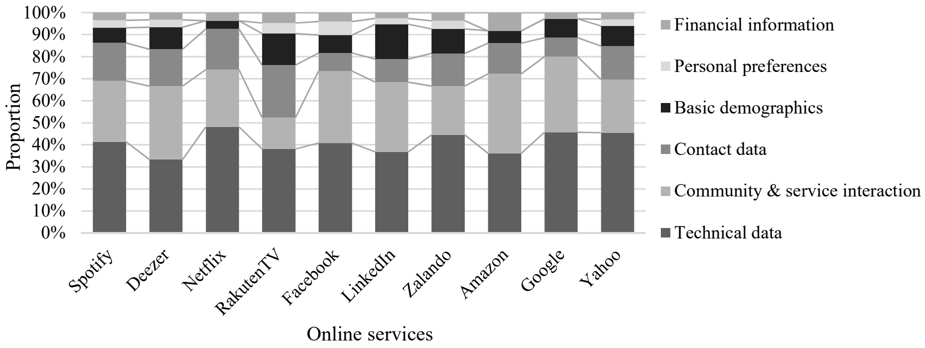

Fig. 2. Proportion of categories of data processed by each online service as defined in privacy statements. Categories of data were classified into groups according to [28].

The proportion according to the applied classification (cf. Sec. 3.3) is as follows: 37.6% technical data, 35.1% community and service interaction, 9.1% basic demographics, 9.1% contact information, 5.2% personal preferences, and 3.9% financial information. Consequently, technical data together with information about community and service interaction already accounted for two thirds of all data processed by online services, whereas personal data with a clear and direct personal reference accounted for only one third of the data.

Based on this classification, 59.5% of the data belonged to the high–medium sensitivity segment, 31.2% belonged to the medium–low sensitivity segment, and 9.3% belonged to the low sensitivity segment. Based on previous research [25,36], we conclude that online users would perceive the processed data to be of medium to high sensitivity if they were aware of its extent. An overview of the distribution of the different groups of data for each online service is provided in Fig. 2.

4.2 Information in privacy dashboards and exports

In the following, we summarize the functions and information provided by the privacy dashboards for each provider, together with details on the information obtained in data exports.

Spotify – For one thing, the dashboard provided comprehensive overview and control over contact data, basic demographics, and financial information. On the other hand, however, information about technical data and personal preferences were lacking completely. The dashboard made aware of advertisers and third-party services as recipients. Spotify was also one of two providers who made visible the processing of data from linked online social network accounts. The data export was requested via the dashboard and consisted of two parts. The first part became available after three days and the second part after 16 days. The information was provided in JSON format. Whereas the first part lacked technical data and service interaction data with respect to the items mentioned by the privacy statement, the second export was complete. We therefore refrained from sending a formal request.

Deezer – The dashboard provided an overview and control over most groups of personal data, but lacked information about service interaction and all technical data. Furthermore, it made aware of advertisers as recipients. According to their privacy statement, they did not process data from external sources. Also, it was not possible to request an export via the dashboard, but only by email. We received a response after one day containing a TXT-file that included less information than the dashboard for three groups of data, and still lacked technical data. Upon request, we were provided with login credentials for a FTP-server to download an extended data export, however, we were unable to access the server due to technical issues. The problem persisted despite support request.

Netflix – The dashboard provided an overview and control over all groups of personal data, but lacked some technical data and information about service interaction. Furthermore, the dashboard made aware of third-party services as possible recipients as well as a source for personal data. A data export was requested via the dashboard and became available after eight hours. Again, the CSV-files lacked technical data (e.g., advertising IDs). Upon request, we received a response after 29 days, in which we were, again, referred to the data export.

Rakuten TV – The dashboard provided very limited overview and control over personal data, and also lacked all technical data, personal preferences, and some information about community interaction. Nevertheless, the dashboard made aware of advertisers as recipients. According to their privacy statement, they did not process data from external sources. As with Deezer, a data export had to be requested via email. After two days, we received several PDF-files, which, however, did not include any information about personal preferences and also lacked some information about technical data and community interaction.

Facebook – The dashboard provided an overview and control over the different data processed, but lacked mostly technical data. The various data categories were divided into groups and could be inspected individually. A privacy wizard guided us through the different privacy settings. The dashboard made aware of advertisers, third-party services, as well as internal and external users as recipients, but lacked information about external sources. The data export was requested via the dashboard and became available after 30 minutes. We could choose between HTML and JSON format. Yet again, technical data were incomplete. We obtained a response to our formal request after two days. However, we were again referred to the dashboard and data export only.

LinkedIn – Similar to Facebook, the dashboard provided overview and control over different data by dividing them into different groups. Privacy settings provided control over the processing. The dashboard made aware of third-party services and other users as recipients, but lacked information about external sources. The export was requested via the dashboard and became available on the next day. The provided CSV-files also lacked technical data (e.g. cookie IDs). Upon request for access, we received the same export again.

Zalando – The dashboard provided an overview and control over most groups of data, but lacked some information about service interaction and all technical data. Furthermore, no information was provided about recipients and sources. The export was downloaded via the dashboard and became available after three days. Data subjects may choose between a single PDF-file or multiple CSV-files. The export contained less information compared with the dashboard. Upon a formal request for access, we received a second export on the next day that still lacked technical data, contact data, and information about service interaction.

Amazon – The official web form for requests for access informed data subjects about the possibility to access personal data via the user account dashboard. The dashboard summarized the different services for which personal data are processed, however, largely lacked technical data. Also, it only made aware of third-party services as recipients, but completely lacked information about external sources. The export was available after four days and consisted of CSV-files. Again, technical data were incomplete (e.g., ISP, URL clickstream). We received a response to our formal request after eight days, but no additional data were made available and we were referred to the web form again.

Google – The dashboard provided an overview of the different services and personal data used in connection with the Google account (e.g. browsing history), as well as control over the processing of some personal data (e.g. location tracking, YouTube history). A "privacy checkup"-wizard guided us through the different privacy settings. The dashboard made aware of third-party services and external entities as recipients, but completely lacked information about external sources. The data export was requested via the dashboard and became available after 30 minutes. While most of the data were provided as JSON-format, some data were provided using common file formats for specific data (e.g. calendar, contacts). We found that technical data (e.g., cookie IDs) as well as basic demographics (e.g., date of birth) were incomplete. In response to our formal request for access, Google referred us to the dashboard. After we pointed out the missing data, we received an archive after 16 days, but no further data were made available.

Yahoo – The dashboard was similarly structured to that of Google and provided an overview and control over the different services and personal data used in connection with the Yahoo account. Furthermore, the dashboard only made aware of advertisers as recipients, but completely lacked information about external sources. The export was requested via the dashboard and became available after eight days. The JSON-files lacked technical data (e.g., cookie IDs), but also contact data and service interactions, which both were available in the dashboard.

Table 1. Summary of findings for privacy dashboards of ten online services: completeness of information with regards to Art. 15 GDPR (left hand side) and available ex-post controls (right hand side).

	Recipients (all)	Recipients (ext.)	Ext. sources	Cat. of data	Period	Profiling	Safeguards	Download data	Restrict use	Delete data	Edit data
Spotify	◔	◑	◔	◑	✗	✓	✗	✓	✓	✗	✓
Deezer	◔	◔	n.a.	◑	✗	✓	✗	✗	✓	✓	✓
Netflix	◔	◔	◔	◕	✗	✓	✗	✓	✓	✗	✓
Rakuten TV	◔	◑	n.a.	◔	✗	✓	✗	✗	✓	✓	✓
Facebook	◑	◕	○	◑	✗	✓	✗	✓	✗	✓	✓
LinkedIn	◔	◕	○	◕	✗	✓	✗	✓	✓	✓	✓
Zalando	○	○	○	◑	✗	✓	✗	✓	✗	✓	✓
Amazon	◔	◔	○	◑	✗	✓	✗	✓	✓	✓	✓
Google	◔	◔	○	◕	✗	✓	✗	✓	✓	✓	✓
Yahoo	◑	◑	○	◕	✗	✓	✗	✓	✓	✓	✓

◑ $= \frac{PDB \cap (PRI \cup LOG)}{(PRI \cup LOG)}$

✗: missing; ✓: present; n.a.: not in privacy statement
PDB: privacy dashboard; PRI: privacy statement; LOG: logbook

4.3 Summary of findings

Privacy dashboards – Overall, we found that all examined privacy dashboards implemented the tasks T1 – T4 defined by Raschke et al. [35] to at least some extent (cf. Tab. 1). With regards to intervention mechanisms (T3 & T4) we found that all dashboards allowed the editing of personal data that were disclosed directly or were related to community interactions. Also, eight dashboards each supported deleting data, restricting the processing of data, and downloading a copy of the personal data. With regards to Art. 15 para. 1 GDPR (T1 & T2), however, we found that none of the privacy dashboards provided complete information. In fact, no dashboard informed about the period of storing personal data as well as the safeguards taken for transferring personal data to servers outside the EU. Also, no dashboard explicitly presented the purposes of the processing other than targeted advertising. A number of other purposes may also be indirectly identifiable, but we were unable to perform unambiguous comparisons with our previously compiled lists. In order to prevent conflicting interpretations, we refrained from a detailed analysis of the purposes in the further evaluation.

On a positive side, however, all dashboards informed about some form of profiling or automated decision-making taking place, in particular with regards to targeted advertisements. With regards to recipients, we found that no dashboard informed about personal data becoming available to public authorities and the corporate group, and only one dashboard made visible that data may be shared between services of the same company. However, we found that information about external recipients tended to be more complete (cf. Tab. 1). Five dashboards each made visible that data were shared with third-party ap-

Table 2. Completeness of personal data provided in privacy dashboards and data exports compared to the information provided in privacy statements and our logbook.

	Source	Technical data	Community & service interaction	Contact data	Basic demographics	Personal preferences	Financial information
Spotify	PDB	○	◕	●	●	○	●
	Exp	◔	◕	●	●	●	●
	Exp*	●	●	●	●	●	●
Deezer	PDB	○	◕	●	●	●	●
	Exp	◔	◕	●	◑	○	◑
Netflix	PDB	◑	◕	●	n.a.	n.a.	●
	Exp	◕	●	●	n.a.	n.a.	●
Rakuten TV	PDB	○	◔	●	n.a.	○	●
	Exp	◕	◕	●	n.a.	○	●
Facebook	PDB	◔	◕	●	●	n.a.	●
	Exp	◕	●	●	●	n.a.	●
LinkedIn	PDB	◔	●	●	◕	○	●
	Exp	◑	●	●	◕	●	●
Zalando	PDB	○	◕	●	●	●	●
	Exp	○	◔	◑	●	●	●
	Exp*	◑	◕	◑	●	●	●
Amazon	PDB	◔	◕	●	●	n.a.	●
	Exp	◕	●	●	●	n.a.	●
Google	PDB	◕	●	●	●	n.a.	●
	Exp	◕	●	●	◕	n.a.	●
Yahoo	PDB	◑	●	●	●	●	●
	Exp	◕	◑	◕	●	●	●
Avg. Information $\Delta = PDB - EXP$		-19%	+7%	+9%	+3%	-1%	0%

◑ $= \frac{SRC \cap (PRI \cup LOG)}{(PRI \cup LOG)}$, $SRC \in \{PDB,\ EXP,\ EXP^*\}$

PDB: privacy dashboard; EXP: standard data export; EXP*: extended data export;
PRI: privacy statement; LOG: logbook

plications or advertisers, and two dashboards each made visible that other users (including users outside the service) and external service providers (e.g., payment service) may have access to personal data. With respect to external data sources, only two dashboards made visible that the online service consumed data from third party services (e.g., access profile information from Facebook).

We further found that, on average, 53% (*min* = 27%, *max* = 81%, *sd* = 17%) of personal data listed in the respective privacy statements were accessible through dashboards. Yet we observed distinct differences between different groups of personal data (cf. Tab. 2). First, financial and contact data were complete for all providers, and basic demographic data were likewise complete apart from one exception. With regards to information about community and service interaction, seven dashboards were missing one or two categories of data, whereas

Table 3. Summary of the completeness of personal data provided in privacy dashboards, data exports, and upon request for ten online services.

Online Service	Completeness of personal data by source											
	PDB			EXP			EXP*			Total		
Spotify	8/21	38%	◔	11/21	52%	◑	21/21	100%	●	21/21	100%	●
Deezer	8/19	42%	◔	8/19	42%	◔	same as EXP			10/19	52%	◑
Netflix	15/23	65%	◑	20/23	87%	◕	same as EXP			20/23	87%	◕
Rakuten TV	4/15	27%	◔	11/15	73%	◕	same as EXP			11/15	73%	◕
Facebook	22/37	59%	◑	30/37	81%	◕	same as EXP			30/37	81%	◕
LinkedIn	16/27	59%	◑	19/27	70%	◕	same as EXP			21/27	78%	◕
Zalando	7/18	39%	◔	5/18	28%	◔	11/18	61%	◑	12/18	67%	◕
Amazon	9/23	39%	◔	20/23	87%	◕	same as EXP			20/23	87%	◕
Google	22/27	81%	◕	22/27	81%	◕	same as EXP			23/27	85%	◕
Yahoo	19/27	70%	◕	19/27	70%	◕	same as EXP			23/27	85%	◕

◑ $= \frac{SRC \cap (PRI \cup LOG)}{(PRI \cup LOG)}$, $SRC \in \{PDB,\ EXP,\ EXP^*\}$

PDB: privacy dashboard; EXP: standard data export; EXP*: extended data export;
PRI: privacy statement; LOG: logbook

three dashboards provided complete information. Interestingly, the former seven dashboards belonged to online services that processed less data about community and service interaction compared with the latter three online services. In terms of technical data, we found that no dashboard provided complete information and four dashboards even lacked this information altogether. In fact, on average, 96% ($min = 82\%,\ max = 100\%,\ sd = 6\%$) of all missing data belonged to the group of technical data.

Data exports – Seven online services provided the data exports in a structured data format (JSON, CSV), whereas the remaining services responded with HTML, TXT, or PDF files. With regards to the response time, exports provided through download facilities in dashboards became available within a few hours or at the same day in four cases, whereas the other exports only became available after three to eight days. In case the export consisted of multiple parts, the second part became available between five and 16 days. Concerning formal requests for access, six online services responded within two days, whereas the others responded within 8 to 29 days.

We found that, on average, the default data exports contained 67% ($min = 27\%,\ max = 87\%,\ sd = 19\%$) of the categories of data mentioned by the respective privacy statement. The extended data exports, as provided by some online services, further increased the amount of data to 75% ($min = 42\%,\ max = 100\%,\ sd = 15\%$). However, responses to formal requests for access were more complete than standard exports in two cases only. With regards to the different groups of data, we found the following: Two exports each lacked data on personal preferences and contact data. Three exports also missed out on information about basic demographics, and four exports lacked data on community and service interaction. All but one export also lacked technical data. Concluding, only one controller, namely Spotify, provided complete information with respect to the categories of data listed in their privacy statement and our logbook.

Comparison of exports and dashboards – Overall, data exports contained 14% to 22% more personal data compared to privacy dashboards. Only in one case, the dashboard provided more data (cf. Tab. 3). Moreover, the data obtained via the separate sources differed. Exports containing the same amount or more data compared to dashboards did not necessarily contain all data provided by dashboards, and vice versa. In six cases, the union set of exports and dashboards yielded more data than the individual sources. In the remaining four cases, exports included all data available in dashboards. On average, exports contained 19% more technical data than dashboards. Nevertheless, dashboards contained more or the same amount of data for all other data categories (cf. Tab. 2).

5 Discussion

For as long as dashboards have existed, their purpose has been to make all the information required for a decision accessible to laypersons, preferably at a glance [12]. Certainly, this requires the careful selection of content in order to find the right amount of information required. The problem, however, is that the filtering of information is always done by experts, or as with privacy dashboards, by controllers. In order to ensure the objective of awareness of the right of access, it is therefore crucial that the information presented actually addresses the decision-making process of data subjects in a holistic manner. The numerous theories on decision-making about the privacy of online users under the research stream on the privacy paradox show that this may be difficult to achieve in practice [14]. Yet, with regards to the right of access, the well-known framework contextual integrity can act as a foundation [30]. Contextual integrity emphasizes on the appropriate flow of information based on a tuple comprising sender, data subject, recipient, data, and context. Taking into account social norms for a particular context, different transmission principles apply to a tuple. Consequently, people's privacy decision making process heavily rely on implicit rules. Applying this framework to our results, we find that the balancing of information is fair for some information provided by privacy dashboards, but also has some flaws for other information. Both aspects are discussed in the following sections.

5.1 Information about purposes, recipients, and sources

Regarding recipients, it is probably fair to assume that users of online services are generally aware of public authorities and the corporate group to possibly become recipients of their personal data. Therefore, while their omission from privacy dashboards conflicts with legal requirements to disclose such information, it still seems plausible as to not overload dashboards with information. However, the omission of external recipients are grave enough to conclude that the examined tools undermine most online users' decision making processes. That is, ordinary online users have poor understanding of the online world [19] and simplified mental models let people overlook entities involved in the background of data processing routines, even if they are well aware of the processing in general [1,42]. For example, consumers may overlook service providers such as payment services who get hold of their personal data [1]. Moreover, while online users may be aware of their data being shared with the corporate group, they may be unaware of the different rules that apply to personal data processed outside the EU. Other information deficits relate to the lack of explicit purposes in privacy dashboards and the lack of details in privacy statements. This likely increases the sharing of sensitive data by consumers for purposes for which they do not want their data processed [34]. In contrast, a clear mapping between personal data and purposes, as implemented by Spotify and Deezer, would allow consumers to make informed choices that meet their protection goals. Furthermore, omitting data sources and technical data, but, at the same time, providing almost complete overview and access to user supplied data, pretends a false sender according to contextual integrity. The lack of use of simple but proven privacy patterns, such as personal data tables, which are well known to be very effective for such purposes and have been studied for years [39], constitutes a serious gap. Regarding the extensive functions that some online services made available to their users in the dashboards, it is therefore surprising to find that none of the providers simply displayed all the information in a clear manner in accordance with Art. 15 GDPR.

5.2 Information about categories of data

With regards to the information provided about categories of data, our findings are somewhat ambivalent. On the positive side, categories of data that users consciously disclosed themselves (e.g., contact information) or that relate to the main purpose of an online service were almost in all cases completely mapped in the dashboard. On the other hand, however, technical data were generally missing. This is problematic in that online users perceive many technical data such as IP addresses, device IDs, cookie data, and location data to be highly sensitive [25,36]. Also, online users are very concerned if such information is passed on to third-party providers, such as online advertisers [28]. For one thing, current privacy dashboards simply do not take into account much of the data classified as sensitive. On the other hand, it is of course questionable to what extent such information influences users in their data protection decisions. Nevertheless, this decision must not be made by online services. Awareness always requires complete information and therefore requires at least the visibility of the processing of numerous technical data. Thus, while making self-reported data accessible appears reasonable, this could be a false prioritization in terms of the actual perceived sensitivity of data. In this context, online providers can already rely on a plethora of TETs for making sensitive technical data transparent [29]. Here, of course, the effort required on the part of the controller must be weighed against the added value for data protection of providing real time copies of technical data. Clearly, complying with the GDPR must not jeopardize the availability of the actual services. The somewhat long response times of several days for data exports with technical data let us assume that the providing of such data cannot be achieved in real time. Yet this may not even be necessary for the purpose of awareness, since already visualizing the different amount of personal data supports online users in drawing conclusions about the processing [37]. Since technical data accounted for almost 40% of all personal data across all services examined, the current state represents a clear imbalance in information content.

Also, another problem constitutes the lack of self-reported data in privacy dashboards (e.g. community and service interaction) or data assumed to be present (e.g. personal preferences). In such cases, online services risk losing a considerable amount of trust among their customers [9,18]. Online services would be well advised to correct these deficiencies in order to counteract a loss of trust and at the same time provide users with more complete information.

5.3 Copy of personal data

Studies have shown that the usability of JSON documents is very poor, and, for lay users in particular, the use cases for the right of access are strictly limited to simple text searches [5]. Instead, visualizations of the data using graph views have been shown to facilitate understanding of recipients, sources, and data flow [3,5,13]. While some of these tools are available to the public[5], they are unlikely to be widely used in practice, since some users are ignorant about their rights [2], or may even refrain from downloading a copy of their personal data due to security concerns [21]. Either way, users expect tools for inspecting data to be provided by online services themselves [21]. It follows that providing structured documents without further ado and without any means to inspect the information offers little value to data subjects. Consequently, current practice reduces the principles of Art. 15 to absurdity, in particular with regards to Recital 63 GDPR claiming that exercising the right must be easy and should enable data subjects "to be aware of, and verify, the lawfulness of the processing." While data exports undoubtedly constitute an important instrument for self-determined privacy, the right to a copy of the data seems to offer little added value in its current form and interpretation. We argue that providing a copy of the data under Art. 15 should be distinct from exports under Art. 20, as they address fundamentally different concerns. To add value to the right to a copy of personal data for awareness, we argue, in line with other work [2,16], that online services should explain the information provided to strengthen the trust relationship with online users. We believe that privacy dashboards as knowledge conversion tools could serve as powerful tools in this regard too.

[5] https://transparency-vis.vx.igd.fraunhofer.de/

6 Ethical considerations

In the scope of this work we never tried to get hold of any personal data of any natural person other than the authors of this work. However, since our formal request for access involved interaction with people working for the different online services, we identified possible ethical issues. We did not collect nor analyze any of our respondents' personal data. Furthermore, we were only interested in receiving a copy of the personal data processed. If we found discrepancies between data exports and data protection statements, we disclosed this in mail correspondence. We therefore see no need to explicitly report our investigations to the providers again.

7 Limitations and outlook

Our case study of privacy dashboards from ten online services certainly represents only a small subset of all online services frequently used in practice. However, when selecting these services we found that extensive privacy tools are not yet widely available, which limits the number of possible candidates. Our investigation also already included some of the most popular online services for the most common online activities in the EU. Since we also found the same discrepancies for missing information between privacy dashboards, data exports, and privacy statements from market leaders as well as from less popular providers, we believe that our results offer a solid basis for future quantitative analysis. Yet, privacy dashboard analyses can likely only be conducted qualitatively in the foreseeable future, since it requires manual inspection of UI elements. Different though, automatized verification checks based on privacy statements and data exports would already be possible using the tools available. For example, existing inspection tools for data exports may make users aware of missing categories of data, utilizing deep learning capabilities to automatically extract and compare information from privacy statements and data exports [17].

Furthermore, we did not verify whether personal data were missing from the privacy statements, that is, whether a provider processed more categories of personal data than specified in the statement. Nevertheless, our results indicate that already now controllers have difficulties providing complete information.

Last but not least, our evaluation of privacy dashboards was conducted by experts. Real online users may actually perceive the information provided differently, and future studies should examine in how far privacy dashboards actually make users aware of purposes, recipient, sources, and categories of data.

8 Conclusion

Privacy dashboards are promising tools to meet legal obligations for providing transparency and intervention mechanisms to data subjects, and to ease the exercise of their rights [5,33,35]. However, our review of ten online services indicates that the extent to which real-world implementations already address the right of access is insufficient at present. Despite our small sample, we found rather clear and systematic differences for the amount and completeness of information provided concerning different subjects covered by Art. 15 GDPR. In particular, we found that information about storage period and safeguards were generally missing, while information about data sources, recipients, and technical data were at least incomplete. In contrast, however, information about personal data entered by data subjects themselves were mostly complete, accessible, and editable. Aside from the limited information provided in privacy dashboards, our findings also suggest that the current implementation of the right of access itself is flawed, since only one of ten online services provided a complete copy of personal data with respect to their own privacy statement. Also, for users to become aware of the extent to which their data are processed, they would need to combine the information from privacy dashboards and data exports in most cases. Nevertheless, the objective of Art. 15 to increase awareness would not be achieved because both sources lack some information that is considered highly sensitive by users. Online services should address this issue in order not to lose the trust of their customers. Furthermore, it seems unreasonable to provide incomplete information via several different channels. We therefore advocate – in context of Art. 15 – replacing or at least supplementing the provision of less user-friendly JSON and CSV file downloads with better and complete preparation of the data in the privacy dashboards themselves. Here, it is the developers' task to integrate the tools provided and evaluated by the scientific community. In doing so, they should consider the extent to which all legally required information can be provided and be considerably more cautious in deciding to omit information. Moreover, while the provision of structured data formats is essential for the right to data portability, the usefulness of such copies in the context of Art. 15 is questionable, as they do not effectively facilitate the understanding of personal data processing without appropriate tools. Therefore, in order to facilitate the exercise of the right of access, policymakers should consider clearly separating the concerns of Art. 15 and Art. 20 and emphasize the need to provide copies under Art. 15 in an intelligible manner.

References

1. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security and Privacy **3**(1), 26–33 (2005). https://doi.org/10.1109/MSP.2005.22
2. Alizadeh, F., Jakobi, T., Boden, A., Stevens, G., Boldt, J.: GDPR Reality Check - Claiming and Investigating Personally Identifiable Data from Companies. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW). pp. 120–129. IEEE (2020). https://doi.org/10.1109/EuroSPW51379.2020.00025
3. Angulo, J., Fischer-Hübner, S., Pulls, T., Wästlund, E.: Usable transparency with the data track: A tool for visualizing data disclosures. In: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems. p. 1803–1808. Association for Computing Machinery (2015). https://doi.org/10.1145/2702613.2732701

4. Arfelt, E., Basin, D., Debois, S.: Monitoring the GDPR. In: 24th European Symposium on Research in Computer Security (ESORICS). pp. 681–699. Lecture Notes in Computer Science, Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-29959-0_33
5. Bier, C., Kühne, K., Beyerer, J.: PrivacyInsight: The Next Generation Privacy Dashboard. In: Privacy Technologies and Policy. pp. 135–152. Lecture Notes in Computer Science, Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-44760-5_9
6. Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., Santos, C.: Security Analysis of Subject Access Request Procedures. In: Privacy Technologies and Policy. pp. 182–209. Lecture Notes in Computer Science, Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-21752-5_12
7. Buchmann, J., Nebel, M., Roßnagel, A., Shirazi, F., Simo, H., Waidner, M.: Personal Information Dashboard: Putting the Individual Back in Control. In: Digital Enlightenment Yearbook 2013, pp. 139–164. IOS Press (2013)
8. Bufalieri, L., Morgia, M.L., Mei, A., Stefa, J.: GDPR: When the Right to Access Personal Data Becomes a Threat. In: 2020 IEEE International Conference on Web Services (ICWS). pp. 75–83 (2020). https://doi.org/10.1109/ICWS49710.2020.00017
9. Cabinakova, J., Zimmermann, C., Mueller, G.: An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case. In: Proceeding of the 24th European Conference on Information Systems (ECIS). Research Papers, vol. 114, pp. 1–18. AIS Electronic Library (AISeL) (2016)
10. Cagnazzo, M., Holz, T., Pohlmann, N.: GDPiRated – Stealing Personal Information On- and Offline. In: 24th European Symposium on Research in Computer Security (ESORICS). pp. 367–386. Lecture Notes in Computer Science, Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-29962-0_18
11. European Parliament and Council of European Union: Regulation (EU) 2016/679 (2016),
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
12. Few, S.: Information Dashboard Design: The Effective Visual Communication of Data. O'Reilly Media, Inc. (2006)
13. Fischer-Hübner, S., Angulo, J., Pulls, T.: How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used? In: Privacy and Identity Management for Emerging Services and Technologies. pp. 77–92. IFIP Advances in Information and Communication Technology, Springer (2014). https://doi.org/10.1007/978-3-642-55137-6_6
14. Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security **77**, 226–261 (2018). https://doi.org/10.1016/j.cose.2018.04.002
15. Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L.F., Agarwal, Y.: How short is too short? implications of length and framing on the effectiveness of privacy notices. In: 12th Symposium on Usable Privacy and Security (SOUPS). pp. 321–340. USENIX Association (2016)
16. Goodman, B., Flaxman, S.: European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". AI Magazine **38**(3), 50–57 (2017). https://doi.org/10.1609/aimag.v38i3.2741
17. Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K.G., Aberer, K.: Polisis: Automated analysis and presentation of privacy policies using deep learning. In:

27th USENIX Security Symposium (USENIX Security). pp. 531–548. USENIX Association (2018)

18. Herder, E., van Maaren, O.: Privacy Dashboards: The Impact of the Type of Personal Data and User Control on Trust and Perceived Risk. In: Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization (UMAP). pp. 169–174. Association for Computing Machinery (2020). https://doi.org/10.1145/3386392.3399557
19. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In: 11th Symposium On Usable Privacy and Security (SOUPS). pp. 39–52. USENIX Association (2015)
20. Kani-Zabihi, E., Helmhout, M.: Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features. In: Information Security Technology for Applications (NordSec). Lecture Notes in Computer Science, vol. 7161, pp. 131–148. Springer Berlin Heidelberg (2012). https://doi.org/10.1007/978-3-642-29615-4_10
21. Karegar, F., Pulls, T., Fischer-Hübner, S.: Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This? In: Privacy and Identity Management. Facing up to Next Steps, vol. 498, pp. 164–181. Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-55783-0_12
22. Kolter, J., Netter, M., Pernul, G.: Visualizing Past Personal Data Disclosures. In: 2010 International Conference on Availability, Reliability and Security (ARES). pp. 131–139. IEEE (2010). https://doi.org/10.1109/ARES.2010.51
23. Le Pochat, V., Van Goethem, T., Tajalizadehkhoob, S., Korczyński, M., Joosen, W.: Tranco: A research-oriented top sites ranking hardened against manipulation. In: Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS). The internet society (2019)
24. Mannhardt, F., Oliveira, M., Petersen, S.A.: Designing a Privacy Dashboard for a Smart Manufacturing Environment. In: Digital Transformation for a Sustainable Society in the 21st Century. pp. 79–85. IFIP Advances in Information and Communication Technology, Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-39634-3_8
25. Markos, E., Milne, G.R., Peltier, J.W.: Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. Journal of Public Policy & Marketing **36**(1), 79–96 (2017). https://doi.org/10.1509/jppm.15.159
26. Martino, M.D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., Andries, K.: Personal Information Leakage by Abusing the GDPR 'Right of Access'. In: 15th USENIX Symposium on Usable Privacy and Security (SOUPS). USENIX Association (2019)
27. Matzutt, R., Müllmann, D., Zeissig, E.M., Horst, C., Kasugai, K., Lidynia, S., Wieninger, S., Ziegeldorf, J.H., Gudergan, G., genannt Döhmann, I.S., Wehrle, K., Ziefle, M.: myneData: Towards a Trusted and User-controlled Ecosystem for Sharing Personal Data. In: 47. Jahrestagung Der Gesellschaft Für Informatik. pp. 1073–1084 (2017). https://doi.org/10.18420/in2017_109
28. Milne, G.R., Pettinico, G., Hajjat, F.M., Markos, E.: Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. Journal of Consumer Affairs **51**(1), 133–161 (2017). https://doi.org/10.1111/joca.12111

29. Murmann, P., Fischer-Hübner, S.: Tools for Achieving Usable Ex Post Transparency: A Survey. IEEE Access **5**, 22965–22991 (2017). https://doi.org/10.1109/ACCESS.2017.2765539
30. Nissenbaum, H.: Privacy as Contextual Integrity. Washington Law Review **79**(1), 1119–157 (2004)
31. Pavur, J., Knerr, C.: GDPArrrrr: Using Privacy Laws to Steal Identities. arXiv:1912.00731 [cs] (2019), https://arxiv.org/abs/1912.00731
32. Polst, S., Kelbert, P., Feth, D.: Company Privacy Dashboards: Employee Needs and Requirements. In: 1st International Conference on Human-Computer Interaction for Cybersecurity, Privacy and Trust (HCI-CPT). pp. 429–440 (2019). https://doi.org/10.1007/978-3-030-22351-9_29
33. Popescu, A., Hildebrandt, M., Breuer, J., Claeys, L., Papadopoulos, S., Petkos, G., Michalareas, T., Lund, D., Heyman, R., van der Graaf, S., Gadeski, E., Le Borgne, H., deVries, K., Kastrinogiannis, T., Kousaridas, A., Padyab, A.: Increasing Transparency and Privacy for Online Social Network Users – USEMP Value Model, Scoring Framework and Legal. In: Privacy Technologies and Policy. pp. 38–59. Lecture Notes in Computer Science, Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-31456-3_3
34. Presthus, W., Sørum, H.: Consumer perspectives on information privacy following the implementation of the GDPR. International Journal of Information Systems and Project Management (IJISPM) **7**(3), 19–34 (2019)
35. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a GDPR-Compliant and Usable Privacy Dashboard. In: Privacy and Identity Management. The Smart Revolution - 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers. IFIP Advances in Information and Communication Technology, vol. 526, pp. 221–236. Springer (2017). https://doi.org/10.1007/978-3-319-92925-5_14
36. Schomakers, E.M., Lidynia, C., Müllmann, D., Ziefle, M.: Internet users' perceptions of information sensitivity – insights from Germany. International Journal of Information Management **46**, 142–150 (2019). https://doi.org/10.1016/j.ijinfomgt.2018.11.018
37. Schufrin, M., Reynolds, S.L., Kuijper, A., Kohlhammer, J.: A Visualization Interface to Improve the Transparency of Collected Personal Data on the Internet. IEEE Transactions on Visualization and Computer Graphics **27**(2), 1840–1849 (2021). https://doi.org/10.1109/TVCG.2020.3028946
38. Scudder, J., Jøsang, A.: Personal Federation Control with the Identity Dashboard. In: Policies and Research in Identity Management. pp. 85–99. IFIP Advances in Information and Communication Technology, Springer (2010). https://doi.org/10.1007/978-3-642-17303-5_7
39. Siljee, J.: Privacy Transparency Patterns. In: Proceedings of the 20th ACM European Conference on Pattern Languages of Programs (EuroPLoP). pp. 1–11. ACM (2015). https://doi.org/10.1145/2855321.2855374
40. The European Comission: ICT usage in households and by individuals. Tech. rep., The European Union (2019), https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm
41. The European Comission: Digital Economy and Society Index (DESI) 2020 - Use of internet services. Tech. Rep. DESI 2020, The European Union (2020), https://ec.europa.eu/digital-single-market/en/use-internet-and-online-activities
42. Tolsdorf, J., Dehling, F.: In Our Employer We Trust: Mental Models of Office Workers' Privacy Perceptions. In: Financial Cryptography and Data Security Workshops

(FC Workshops). pp. 122–136. Lecture Notes in Computer Science, Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-54455-3_9

43. Tolsdorf, J., Dehling, F., Lo Iacono, L.: Take Back Control! The Use of Mental Models to Develop Privacy Dashboards. ITG News **8**(3), 15–20 (2020)
44. Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N.: A Study on Subject Data Access in Online Advertising After the GDPR. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology. pp. 61–79. Lecture Notes in Computer Science, Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-31500-9_5
45. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (un)informed consent: Studying gdpr consent notices in the field. In: Proceedings of the 26th ACM SIGSAC Conference on Computer and Communications Security (CCS). p. 973–990. Association for Computing Machinery (2019). https://doi.org/10.1145/3319535.3354212
46. Wilson, S., Schaub, F., Ramanath, R., Sadeh, N., Liu, F., Smith, N.A., Liu, F.: Crowdsourcing annotations for websites' privacy policies: Can it really work? In: Proceedings of the 25th International Conference on World Wide Web (WWW). p. 133–143. International World Wide Web Conferences Steering Committee (2016). https://doi.org/10.1145/2872427.2883035
47. Wong, J., Henderson, T.: How Portable is Portable? Exercising the GDPR's Right to Data Portability. In: Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers (UbiComp). pp. 911–920. Association for Computing Machinery (2018)
48. Zimmermann, C., Accorsi, R., Müller, G.: Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy. In: Proceedings of the 9th International Conference on Availability, Reliability and Security (ARES). pp. 152–157. IEEE Computer Society (2014). https://doi.org/10.1109/ARES.2014.27