6-15-2020

Design Goals for Consent at Scale in Digital Service Ecosystems

Christian Kurtz
University of Hamburg, christian.kurtz@uni-hamburg.de

Florian Wittner
Leibniz Institute for Media Research | Hans Bredow Institute (HBI), f.wittner@hans-bredow-institut.de

Pascal Vogel
University of Hamburg, pascal.vogel@uni-hamburg.de

Martin Semmann
University of Hamburg, martin.semmann@uni-hamburg.de

Tilo Böhmann
Department of Informatics, University of Hamburg, tilo.boehmann@uni-hamburg.de

Recommended Citation

Kurtz, Christian; Wittner, Florian; Vogel, Pascal; Semmann, Martin; and Böhmann, Tilo, "Design Goals for Consent at Scale in Digital Service Ecosystems" (2020). *ECIS 2020 Research Papers*. 69.
https://aisel.aisnet.org/ecis2020_rp/69

DESIGN GOALS FOR CONSENT AT SCALE IN DIGITAL SERVICE ECOSYSTEMS

Research paper

Kurtz, Christian, University of Hamburg, Hamburg, Germany, Christian.Kurtz@uni-hamburg.de

Wittner, Florian, Leibniz Institute for Media Research | Hans Bredow Institute (HBI), Hamburg, Germany, F.Wittner@leibniz-hbi.de

Semmann, Martin, University of Hamburg, Hamburg, Germany, Martin.Semmann@uni-hamburg.de

Vogel, Pascal, University of Hamburg, Hamburg, Germany, Pascal.Vogel@uni-hamburg.de

Böhmann, Tilo, University of Hamburg, Hamburg, Germany, Tilo.Boehmann@uni-hamburg.de

Abstract

Digital services have undergone a shift to multi-actor constellations characterised by the utilisation of personal data. By involving external actors, service capability and variety increase but so does the number of actors that gain access to personal data. Here, privacy policies are legal documents that serve two primary functions: specifying the purpose and details of data processing in a binding manner and informing users about it. Privacy policies therefore have special importance in which the processing is based on user consent. In a case study of the platform eBay, we identified 18 problems that point out difficulties in achieving consent in a meaningful way in today's large-scale and massively interconnected digital service ecosystems. Based on these problems, the design goals are determined which help to find meaningful consent in digital service ecosystems. These goals include notifications for changed purposes of data processing in ecosystems or the reasonability of time needed for consent in relation to the usage time of the service. Thus far, no legal limits govern the reasonability of efforts for consent to privacy policies. This requires a fundamental rethinking of the concept of consent or far-reaching automation of privacy-related legal acts.

Keywords: Privacy Policy, Privacy Settings, Information Privacy, Digital Platform.

1 Introduction

The paradigm of a dyadic relationship between an individual and a single organisation is no longer valid in digital service interaction (Riedl et al., 2009, Vargo and Akaka, 2012). Digital interconnectivity manifests itself in individuals exposed to a broad range of actors when using a single digital service (Razaghpanah et al., 2018, Binns et al., 2018, Libert, 2018). These various actors are involved for different reasons, such as improving the service by providing analytics insights, adding functionality, or providing streams of income via, for example, advertisements (Kurtz et al., 2018b). In this context, personal data are shared with involved third parties. A common form for lawful processing of these personal data is to obtain the permission of an individual to receive consent (GDPR, 2016). In this relation, privacy policies are binding legal documents. They bind the data controller (the person responsible for the processing) to the purpose laid out in them and serve as the basis for ensuring that a service user is informed about data processing when providing consent. However, the importance of privacy policies far exceeds the attention that users paid to them, as individuals suffer from consent fatigue (Schraefel et al., 2017). Individuals have too frequently to determine whether and to what extent to grant consent in everyday life.

A New York Times article felicitously illustrates the existing problems of 150 privacy policies (Litman-Navarro, 2019). Most of the analysed policies exceed a level of comprehensibility, even for people with a higher education. Policies are written in such a complex manner that they are more difficult to access than Immanuel Kant's manuscripts (Litman-Navarro, 2019). A recent legal judgement indicates that Google's privacy policy does not conform to the General Data Protection Regulation (GDPR) due to its complexity and obscurity (Bahr, 2019). Already in 2016, 91% of questioned consumers believe that they have lost control of how their personal data is being used (Rainie and Duggan, 2016). Additionally, a study highlights the fear of data being transmitted to third parties as the most frequent issue preventing users from using an online service (Rohleder, 2015); these issues are in tension with the plethora of actors involved in contemporary digital services. A study of one million applications observed that a median of 10 third parties is included per application, and approximately 18% applications involve more than 20 third parties (Binns et al., 2018).

While digital services have undergone a shift towards multi-actor constellations, we question whether privacy policies can still pave the way for meaningful and informed consent. From a legal perspective, the limits governing the reasonability of the extent of privacy policies have hardly been tested. In addition, there is reason to believe that even when legal requirements are met, consent is still failing regarding the (regulatory) aims connected with it. We utilise a single case study of the platform eBay and derive design goals which cover the problems for consent which arise by digital service ecosystems. In our study, we address the gap originating from two directions. First, disseminating digital service ecosystems increasingly involve third parties. Existing studies address the occurrence of and statistics concerning third parties in privacy policies (Yu et al., 2016, Zimmeck et al., 2019, Libert, 2018). However, these studies do not address prescriptive design knowledge to overcome upcoming issues. Second, new solutions address existing problems of consent and policies (Tesfay et al., 2018, Wilson et al., 2016, Harkous et al., 2018). Nevertheless, these approaches do not address the effects of emerging digital service ecosystems. To this end, we present insights from an interdisciplinary study at the intersection of information systems research and law. Our findings indicate new dimensions of necessary effort in the act of determining whether and to what extent to grant consent for a digital service, located in a digital service ecosystem. Our results challenge the assumption that the form of privacy policies being used in digital service ecosystems is still manageable for an individual.

The following section begins by introducing the literature and background (Section 2). Afterwards, we describe the methodology used to determine design knowledge for consent in digital service ecosystems (Section 3). Based on the case study (Section 4), we determine prescriptive design goals (Section 5). We then discuss and legally assess our results (Section 6) before we draw a conclusion (Section 7).

2 Literature and Background

The form of services has shifted from single services to systems of services (Chandler and Lusch, 2015). In service systems, actors collaboratively create value in interactive configurations of mutual exchange (Vargo et al., 2008). Different technological and organisational networks are linked together for joint service provision. Within these networks, activities for integrating and exchanging resources are coordinated through institutional arrangements to achieve mutual value creation (Lusch and Vargo, 2014, Barrett et al., 2015). Service ecosystems encompass self-contained and self-adjusting service systems of resource-integrating actors (Lusch and Vargo, 2014). In digital service ecosystems, mediating platforms can establish the framework by connecting two or more interest groups (Van Alstyne et al., 2016, Bitner et al., 2008). Thereupon, platforms utilise network effects to capture, share and monetise various data sources within a service ecosystem (de Reuver et al., 2018, Hein et al., 2018).

From a user's point of view, personal data are consequently accessible by multiple actors in interaction with a digital service, as the focal element of a digital service ecosystem. We use the definition of 'personal data', declared in the GDPR as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (GDPR, 2016, Art. 4 (1)). The categories and nature of data being disseminated throughout a service ecosystem and its inhabitants can differ, as can the data's proximity to individual users. Depending on the purpose of a data recipient, data can be bundled, aggregated and even pseudonymised to differing degrees that may border on anonymisation. However, the GDPR's barrier for true anonymisation regarding data that was formerly personal is arguably high. Only when the data is so robust that no party can (e.g. through the combination of different data sets or inference of certain information) trace them back to individual users under any reasonable circumstance does the GDPR consider data to be no longer personally identifiable (European Commission, 2014). However, various de-anonymisation approaches exist and are continuously developed (Narayanan and Shmatikov, 2008, Ji et al., 2016, Paspatis et al., 2017, Di Luzio et al., 2016).

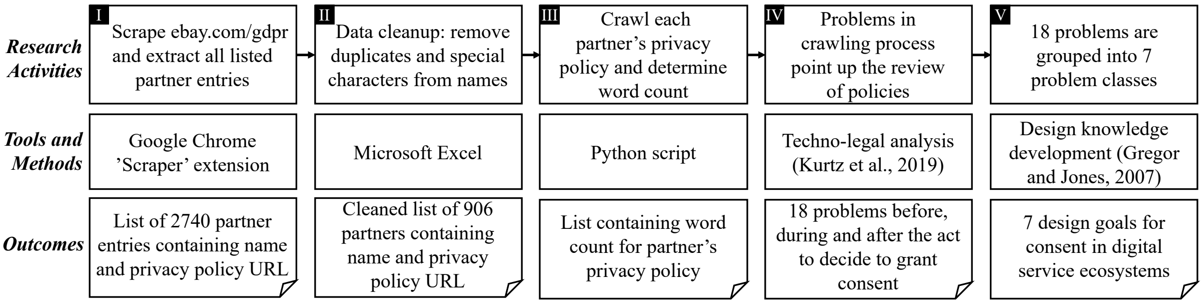
The goal of the GDPR, implemented in May 2018 after a two-year transitional phase, is to protect individuals regarding the processing of personal data pertaining to them (GDPR, 2016, Art. 1 (1)); thus, organisations are obliged to inform users when processing personal data pertaining to them (GDPR, 2016, Art. 13, 14). This typically occurs through organisations using privacy policies that are, most famously, linked to cookie or other prominent notices. Such policies inform a user about, for example, the types of data being processed, the purpose of the processing and possible recipients of further data transfers (GDPR, 2016, Art. 13 and 14). These obligations serve to making processing acts transparent and thereby enable users to exercise their informational privacy, as enshrined in the GDPR's data subject rights (GDPR, 2016, Art. 15-21). When the organisation in question wishes to base its acts of data processing on the consent of its users, its privacy policy serves another important purpose. Within the GDPR's framework for lawful data processing, consent is one – albeit arguably the most important and widely use – of six legal bases (GDPR, 2016, Art. 6 (1)). Processing can be lawful without a user's consent when inter alia, it is necessary for the performance of a contract or when its purpose serves the organisation's legitimate interests and the user's interests do not outweigh those interests. Consent as a legal basis is only accepted as such by the GDPR when it is expressed in the form of a 'freely given, specific, informed and unambiguous indication' (GDPR, 2016, Art. 4 (11)).

However, the assumption that the existing form of privacy policies achieves such imperatives is questionable. Findings identify that users as data subjects do not understand privacy policies and describe the practices therein (Reidenberg et al., 2015). This is driven, inter alia, by the difficulty of privacy policies (Ermakova et al., 2015). It follows that users cannot access the potential magnitude of harm, because users cannot build an expectation concerning when and how organisations are accessing and processing their personal data (Malandrino and Scarano, 2013). Moreover, some organisations exploit behavioural and psychological processes in privacy settings to promote data disclosure (Acquisti et al., 2015). This behaviour includes default settings with opt out rather than opt in to share data (Acquisti et al., 2015). In this relation, the phenomenon of individual's consent fatigue is increasing, which results in ineffective consent by accepting policies without informing oneself (Schraefel et al., 2017). Solution approaches introduce automatised methods of extracting user-relevant details from privacy policies by applying natural language processing and machine learning (Tesfay et al., 2018, Wilson et al., 2016). One example is the project pribot.org, which provides privacy policy summaries using deep learning (Harkous et al., 2018). Such approaches address the problem of the immense opportunity costs of users to read and understand privacy policies (McDonald and Cranor, 2008) and can be used for improved and easier content processing of privacy policies. Our design goals based on the case study (cf. Section 5) can be put into practice by combining such existing approaches to address the challenges posed by service ecosystems.

Digital service ecosystems with involved and emerging actors exacerbate the reservations and problems of privacy policies. An increasing number of third parties is involved in a single digital service (Razaghpanah et al., 2018, Binns et al., 2018, Libert, 2018, Kurtz et al., 2018a). In this context, the organisational view of how much service providers should share with third parties is investigated (Gopal et al., 2018). In addition, studies revealed the incongruous mismatch between the statements in organisations' privacy policies and the practices actually performed by involved third parties (Yu et al., 2016, Zimmeck et al., 2019). Based on a large-scale data set, an investigation identifies crucial findings regarding the massive third-party data collection, yet with fewer than 15% of attributed data flows disclosed in related privacy policies (Libert, 2018).

3 Research Methodology

The creation of design knowledge is fundamental for design science research (Legner and Löhe, 2012, Kuechler and Vaishnavi, 2008, Gregor and Jones, 2007). A design theory explains how an artefact should be constructed (Walls et al., 1992). However, no commonly accepted method exists for developing design knowledge and related theories (Baskerville and Pries-Heje, 2010, Fischer et al., 2010, Legner and Löhe, 2012). We utilise a case study to create design knowledge and have identified the platform eBay and its interconnected partner organisations as an exemplary manifestation of a digital service ecosystem. We conducted a case study appropriate for when the research focus is on contemporary events (Benbasat et al., 1987). A single case study approach is typically chosen to explore a significant phenomenon under rare or extreme circumstances which is representative of a situation (Yin, 2009). For our case study, eBay is particularly well suited, as it transparently provides an account of all involved third parties on a dedicated website. This is not the case for every platform or service provider involved in a digital service ecosystem. In some instances, the general term is utilised that third parties are involved but that actors and actions are not specified. Thus, the transparency of eBay's digital ecosystem allows for an in-depth investigation. The platform specifies a staggering number of third parties involved in data processing on www.ebay.com/gdpr (eBay, 2019a), which has access to eBay users' personal data.



	I	II	III	IV	V
Research Activities	Scrape ebay.com/gdpr and extract all listed partner entries	Data cleanup: remove duplicates and special characters from names	Crawl each partner's privacy policy and determine word count	Problems in crawling process point up the review of policies	18 problems are grouped into 7 problem classes
Tools and Methods	Google Chrome 'Scraper' extension	Microsoft Excel	Python script	Techno-legal analysis (Kurtz et al., 2019)	Design knowledge development (Gregor and Jones, 2007)
Outcomes	List of 2740 partner entries containing name and privacy policy URL	Cleaned list of 906 partners containing name and privacy policy URL	List containing word count for partner's privacy policy	18 problems before, during and after the act to decide to grant consent	7 design goals for consent in digital service ecosystems

Figure 1. Research approach

Our research approach is illustrated in Figure 1. For the data collection, conducted in August 2019, we utilised the Google Chrome extension 'Scraper' (chrome web store, 2019) as a first step and extracted a list containing the name of each eBay partner and the corresponding privacy policy URL in a .csv file. Some partners are listed in more than one purpose category of data processing. In the second step, we performed a data clean-up: we removed duplicates by reviewing the partner names and privacy policy URLs. Partners listed with several services and several corresponding policies were not removed as duplicates. After removing duplicates, a total of 906 unique partners resulted across all purpose categories. Once more, we extracted the list as a .csv file, which we fed into our Python crawler script. In step three, we parsed the .csv list in our Python script and utilised standard libraries to request the website containing the privacy policy for each contained URL. We used the Python library Beautiful Soup (Crummy, 2015) to parse the HTML content and remove unwanted elements such as styling information or scripts. To obtain an accurate word count, we fed the resulting raw text into the tokeniser package contained in the Python Natural Language Toolkit library (Natural Language Toolkit, 2019). We observed neglectable deviations between the precise, manually determined word count of a website and the word count determined by our script, as in some cases, words in a website's navigation bar or footer were included in the count. We subsequently stored the resulting word count for each URL in another .csv file for further analysis. Step four included the specification of different errors, and problems arose in the scraping and crawling process steps. These issues highlighted the need for a manual review of the user act of determining whether and to what extent to grant consent. By utilising a techno-legal analysis

(Kurtz et al., 2019), we considered a user's perspective to identify the hurdles and problems. We divided these problems chronologically: before (P_{before}), during (P_{during}) and after (P_{after}) the act of consent. In step five, we grouped these problems into problem classes, which set the basis to determine the differences between an envisaged state and the current state of an artifact (Cronholm and Göbel, 2019). Based on this, we created design knowledge and derived a set of design goals (DGs) (Gregor and Jones, 2007); design goals represent the design theory's purpose and scope (Gregor and Jones, 2007). Generalised design goals enable the application regardless of a specific setup (Horlach et al., 2019). Our universally applicable design goals can serve as the basis for consent in digital service ecosystems.

4 Case Study

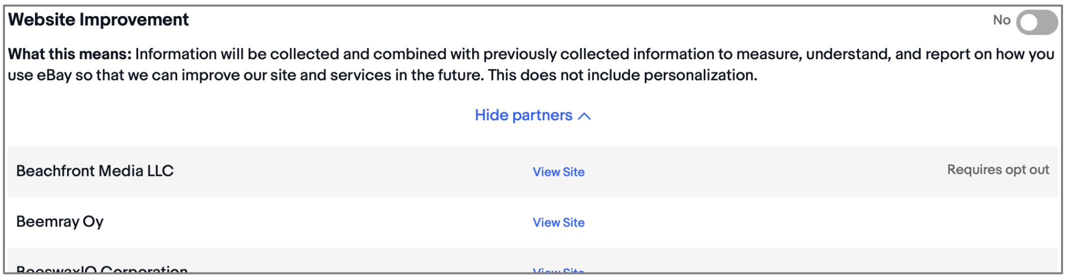
4.1 eBay and included partners

The platform eBay specifies the involvement of many partners for different purposes (eBay, 2019a). In the following, we detail eBay's specification. In addition, we illustrate the purpose categories and the number of included parties by eBay and related policies. The first time a user visits the eBay website or eBay application, the notice for the cookie and other technologies is displayed. In this notice, the aforementioned website is linked to the text 'Learn more, including how to manage your privacy settings'. Moreover, eBay's privacy policy specifies that this referenced website describes how eBay and related partners are processing users' personal data (eBay, 2019b). Users in the European Economic Area (EEA) have the choice to provide consent for related data processing.

Purpose category	**Count of partner entries**
'Content selection, delivery, and reporting'	315
'Website Improvement'	421
'Google Advertising'	645
'Storing and accessing information on your devices'	502
'Ad selection, delivery, and reporting'	460
'Personalizing advertising based on your behavior'	397
	2,740

Table 1. Count of partner entries per purpose category (August 2019)

In total, 2,740 partner entries are listed in the six purpose categories (Table 1) (research approach – step I). The name of each partner organisation and the URL to the related privacy policy are referenced in these categories. Users have the choice of deciding on partner's data processing and for each purpose category as a whole (Figure 2). On the website itself, the headline references 'Advertising and related preferences' for 'control the information eBay uses to show you ads'. This appears to conflict with two defined purpose categories. In particular, 'Content selection, delivery, and reporting' and 'Website Improvement' do not appear to fit the advertisement headline specified by eBay. The purpose categories described by eBay itself provide an indication that the majority of data in question is personally identifiable in nature. Apart from this, the fact that eBay itself lists these categories on a site about processing users' personal data clearly indicates that the data in question is personal data.



Website Improvement No

What this means: Information will be collected and combined with previously collected information to measure, understand, and report on how you use eBay so that we can improve our site and services in the future. This does not include personalization.

Hide partners ^

Beachfront Media LLC	View Site	Requires opt out
Beemray Oy	View Site	
BeeswaxIO Corporation	View Site	

Figure 2. Extract of purpose category 'Website Improvement' (eBay, 2019a)

A data clean-up of the 2,740 listed partner entries resulted in 906 unique partners (Table 2) (research approach – step II). A single partner can be listed in multiple purpose categories, thus leading to the 2,740 entries. However, several listings of one partner do not link to several privacy policies – only to one policy. Typically, no data clean-up, such as the removal of duplicates, is performed by a user. Nevertheless, we performed a data clean-up to obtain further results.

Partners	Count	Word count
Unique	906	-
Privacy policies not accessible	79	-
Privacy policies accessible	827	2,221,079
Privacy policies accessible, in English	735	1,984,823
Privacy policies accessible, in other languages (16 languages)	92	236,256

Table 2. eBay partners' privacy policies in numbers

Only 827 privacy policies of 906 partners could be accessed (research approach – step III), as 79 policies were not accessible due to two reasons. First, 'ERROR: HTTP Error 404: Not Found' was displayed – the URLs to the partner policies specified by eBay did not exist. Second, security issues existed when opening the policies; in detail, the browser indicated an insecure, unencrypted connection or certificate errors when accessing websites. Of the 827 accessible privacy policies, 735 are written in English. The other policies are written in 16 other languages, namely Bulgarian, Chinese, Czech, Danish, Dutch, German, Finnish, French, Italian, Japanese, Polish, Portuguese, Russian, Slovak, Spanish and South Korean. On the related websites of these partners, no option existed to change the language.

4.2 Legal classification

Pursuant to eBay's privacy policy, eBay bases its processing acts for the purpose of 'Personalization, measurement and improvement of [its] and third party advertisements in [its] online offerings, the online offerings of other eBay Inc. corporate family members or third parties' (eBay, 2019b, No. 5.5) on user consent as a legal basis for processing pursuant to the GDPR (GDPR, 2016, Art. 6 (1) (a)). Thus, eBay's aforementioned page (eBay, 2019a), offering further information on the various types of so-called 'eBay-Partners' that gain access to users' personal data under this purpose, is provided as a complementary document to the original privacy policy. This offers users more finely detailed information and allows them to change their consent preferences, either on a coarse level regarding different kinds of purposes or on a granulated level regarding every single partner. As the difficulties for determining and granting consent stem from the multitude of recipients to whom eBay transfers data, the focus shall be placed on the complimentary site that assesses the validity of consent granted by users.

When the personal data of eBay users is being transferred from eBay to a partner, two processing acts in need of a legal basis and other lawfulness requirements are actually occurring: the transfer itself, for which eBay evidently bases on user consent, and the saving and further processing of those data for which each individual recipient is a data controller with its own obligations, such as legal basis and user information. Thus, even if eBay were to act in a fully GDPR-compliant way regarding their transfer, unlawful processing acts might still occur within the digital service ecosystem, depending on each individual partner. Because of this, we shall evaluate the limits of user consent regarding both processing acts: Is the way eBay informs its users through its privacy policy sufficient to justify the initial processing and subsequent processing acts by partners? Only if this is the case, lawful types of processing acts are possible. This statement holds true for other, similar types of service ecosystems so long as they rely on consent as a legal basis and the service provider manages the way through which consent is being granted for the recipients in a service ecosystem.

The provided information by eBay must enable users to make an informed and free decision based on the specific purposes described to them. In addition, the mechanism through which consent is granted must be designed in such a way that the users can voice their wishes in an unambiguous manner (GDPR, 2016, Art. 4 No. 11). Differentiating here is important because the legal requirements for valid consent can differ based on the type of processing acts and data in question. For example, while it would suffice to inform about the 'recipients or categories of recipients of the personal data' (GDPR, 2016, Art. 13 (1) (e)) for consent encompassing only the processing and transfer of data by eBay itself, this would not suffice for consent that, as is the case here, aims to legitimise the subsequent processing acts by the recipients of the data, as well. Valid consent for these further processing acts would need to be granted based on the full range of information (GDPR, 2016, Art. 13). To consent to all such processing acts, users would need to know more information, such as the possible consequences. This would necessarily require access to the respective privacy policies of all the possible recipients at the times that consent is granted. However, consenting to so many (future) processing acts simultaneously also stretches the limits of the other aspects of valid consent, which is analysed in greater detail below.

4.3 Problems for users in deciding to grant consent

Hereafter, we specify the problems users have in determining whether and to what extent to grant consent in a digital service ecosystem (research approach – step IV). We have divided the categories into three chronological categories for a user: before, during and after the act. Eight problems exist *before the act* (Table 3). The first issue a user encounters is eBay's requirement for some partners 'to opt-out if [the user] do not wish [his/her] information to be shared […]. To opt-out, [the user has to] visit NAI, DAA or EDAA'. These acronyms belong to network advertising initiatives which bundle services – in this case, eBay partners. Partners included in these alliances receive personal data without consent by default (P_{before} 1). Second, neglecting the privacy settings banner linking to eBay's partner website in combination with any interaction, such as searching for an item or clicking on a bid, are followed by the automatised activation of every purpose category (P_{before} 2). Third, it is difficult to obtain an overview of which unique partners are involved by eBay (P_{before} 3). We scraped the partner entries and related privacy policy URLs and then removed the duplicates, resulting in 906 results of an initial 2,740. Such process steps cannot be expected from a user. However, if a user would complete these steps, the duration of reading the privacy policies could increase by up to a factor of three, as a user would not access all unique partners but all partner entries. Fourth and fifth, not all partner websites are accessible. In addition to websites not existing (P_{before} 4), security issues occur when attempting to open partner policies (P_{before} 5).

No	Problem description
P_{before} 1	Personal data are shared to partners by default
P_{before} 2	Automised activation of every purpose category when a user neglects the privacy settings banner
P_{before} 3	Difficult to obtain an overview of unique partners (research approach – step II)
P_{before} 4	Partner privacy policies are not accessible (ERROR: HTTP Error 404: Not Found)
P_{before} 5	Security issues (partner sites comprise a non-secure connection)
P_{before} 6	Requirement to accept data collection and processing on partner websites
P_{before} 7	Navigation on partner website to partner's privacy policies is not possible
P_{before} 8	Different policies offered by a single partner

Table 3. Problems before the act of determining whether and to what extent to grant consent

Sixth, before a user accesses partners' privacy policies, they must accept the different cookie and related personal data processing notices of partner websites (P_{before} 6). This issue leads to temporal expenditures. In addition, a partner can collect and process personal data based on the user visit and the user (necessary) acceptance of the cookie notice. These personal data can be processed by the partner independent of the processing formed by interactions with eBay. The consent is provided to the partner and related website itself, rather than eBay. This leads to the issue that, to gain more (necessary) information to understand the details of the consent that a user provides to eBay regarding data transfers to a partner, the user must consent to the processing of even more data on the partner's website simply to arrive at its privacy policy. Seventh, other partner sites, such as landing pages, are linked by eBay. Navigating to the privacy policy of the partners was not always possible (P_{before} 7). For cases in which the website has been displayed in a language not accessible to the user, the policy cannot be accessed. Moreover, some partners did not declare a privacy policy at all on their website. Eight, partners declared on the website a selection of policies to access (such as website and service privacy policies). The partner offered no clear indication of which policy is relevant to the user (P_{before} 8). For further analysis, we assume that the service privacy policy is relevant.

Five problems exist *during the act* of determining whether and to what extent to grant consent (Table 4). These problems occur when opening eBay's linked partner sites. First, rather than privacy policies, several other documents are linked (P_{during} 1). Cookie descriptions, data request sheets and opt-out descriptions represent a diverse collection of documents. Second, partners' privacy policies are not accessible for linguistic reasons. The policies are stated in 17 languages, and if written in a language other than English, they do not offer translated versions (P_{during} 2). Not every eBay user has the ability to understand policies not written in his or her native language. In addition, if capabilities in English exist, this competence might not cover complex sentences using legal terminology. Varying difficulty levels of readability are represented in the policies with, for example, in-depth technical descriptions or legal jargon (P_{during} 3). Fourth, diverse policy specification can be observed (P_{during} 4). The policies vary in word count, from 165 words up to 13,497 words. Fifth, the time required to read all partners' policies is extremely long (P_{during} 5) (cf. Section 4.4).

No	Problem description
P_{during} 1	Variety of linked documents (cookie descriptions, privacy policies and data request sheets)
P_{during} 2	Privacy policies are written in 17 languages (735 in English and 92 in 16 other languages)
P_{during} 3	Varying difficulty levels (legal and technical jargon)
P_{during} 4	Varying levels of detail (165 words up to 13,497 words)
P_{during} 5	Massive amount of time required to read partner policies (cf. Section 4.4)

Table 4. Problems during the act of determining whether and to what extent to grant consent

A user encounters five problems *after the act* of determining whether and to what extent to grant consent (Table 5). First, partners reference the involvement of third parties in their privacy policies (P_{after} 1). Thus, for the act, a user would also need to read the privacy policies of third parties involved by eBay's partners. Second, in its purpose category summary, eBay describes the purposes and related technologies used by partners; however, these descriptions do not match with the specifications made in the partners' policies (P_{after} 2). Declarations made by partners exceed those made on eBay's site. Third, no mechanism exists which notifies users of changes in the digital service ecosystem (P_{after} 3). This lack of notification mechanism pertains to changes of eBay's involved partners and in partners' privacy policies. Fourth, no indication is provided as to whether a partner is relevant for the user's transaction (P_{after} 4). Since these are international partners, such as Chinese or South Korean partners, the relevance for a user transaction from Europe is at least questionable. Unfortunately, an examination of the website for further information and a request to eBay did not yield any results. Fifth, partners are listed in multiple purpose categories. A user has the option to decide according to the purpose of the partner's data processing. However, only one privacy policy is linked to the partner independent from the purpose category (P_{after} 5). The question arises regarding the extent to what a user provides consent – the purpose listed on eBay's website or to all specifications made in the privacy policy by the partner.

No	Problem description
P_{after} 1	Integration of third parties by eBay partners
P_{after} 2	Different statements regarding used technologies or purposes
P_{after} 3	No mechanism notifies about changes regarding partner changes or partners' policy changes
P_{after} 4	Relevance of partner for user transactions
P_{after} 5	Choices for a partner's data processing to multiple purpose categories but to only one partner policy

Table 5. Problems after the act of determining whether and to what extent to grant consent

4.4 Average reading time for users of partners' privacy policies

In the following, we calculate the average reading time of the partners' privacy policies to serve as an example for the duration of providing consent in a digital service ecosystem (McDonald and Cranor, 2008). The privacy policies are written in 17 different languages; however, we utilise only the 735 privacy policies written in English. The 92 privacy policies not written in English (10.2% of partners) and 79 privacy policies not accessible (8.7% of partners) are not considered in the calculation. This restriction is driven by the assumption of Europeans being unable to understand languages such as Chinese or Japanese. The calculation represents an indicator but not the time for all partners. We use a scale of 250 words per minute as the basis for average reading time (McDonald and Cranor, 2008). The time depends on various factors, such as education level, difficulty level or language of a text. Moreover, different opinions exist, ranging between 200 and 300 words per minute (McDonald and Cranor, 2008, Carver, 1990). As a second variable, 1,984,823 words contained in 735 privacy policies is considered.

As result, a duration of 7,940 minutes is required to read the privacy policies in English for eBay's digital service ecosystem (Table 6). This time is equivalent to 132.3 hours, 16.5 working days (assuming 8 hours per day) and 5.5 days (assuming 24 hours a day). In addition, 171 partner policies are not considered in this result. Given the massive time amount of 5.5 days, this conflicts with eBay's listing duration options for articles of one, three or five days. In addition, our calculation relates to only the actual reading time, which might not necessarily correspond with the time required for the average user to fully understand the content and implications of the policies. The reading times for partners' policies range between 1 and 54 minutes, and the privacy policy with the longest reading time belongs to eBay itself. The platform is surprisingly mentioned in the purpose category of 'Google Advertising'.

Policies in English	Word count	Reading rate per minute	Minutes	Hours	Working days	Days
735	1,984,823	250	7,940	132.3	16.5	5.5

Table 6. Reading time for eBay partner privacy policies in English (rounded up)

5 Design Goals for Consent in Digital Service Ecosystems

Given that digital service has shifted from a single-actor encounter to a plethora of actors, this raises various problems identified in the case study. In the following, we use the identified problems to derive design goals (research approach – step V) as basis for enabling the act of consent to data processing in digital service ecosystems. In detail, we summarise the problems into multiple problem classes, which served as the basis for specifying the design goals (Table 7). Our design goals are generalised and independent from a specific ecosystem setup; therefore, the design goals for enabling consent can be applied in various digital ecosystems, and involved actors and actions can manifest in various ways (e.g. consent for mobile application service ecosystems or website ecosystems).

The first problem describes the circumstances that partners involved in network alliances encounter via default personal data – without consent (P_{before} 1). In addition, when a user neglects the settings banner, personal data may be shared and processed with not only those partners involved in the alliances but with all partners involved in the digital service ecosystem (P_{before} 2). This occurs without the act of providing consent. When accessing eBay partners' privacy policies, numerous personal data are already transmitted and processed on the partners' websites – request to confirm personal data processing to access the privacy policies (P_{before} 6). However, the concept of a policy is the specification of personal data usage and purposes prior to processing. Therefore, the problem class summarises the aspect that personal data is processed before the act of providing consent. Based on this issue, the first design goal is specified as **no personal data processing before providing consent (DG1)**.

In the case study, 79 partner privacy policies could not be accessed (P_{before} 4). In this context, also security issues arise in attempting to open privacy policies (P_{before} 5). The navigation to policies was sometimes impossible, due to policies not existing or for linguistic reasons (P_{before} 7). Another problem of accessibility is the determination of the relevant policies across the several offered by one partner (P_{before}

8). Moreover, not all privacy policies are written in English; thus, the 16 other languages serve as a potential problem for the user being unable to access the policy content (P_{during} 2). Due to the increasing involvement of actors across national borders, this aspect will be present in other digital service ecosystems. In addition, the partners also involve multiple third parties (P_{after} 1); however, these parties are not mentioned in eBay's policy and appear in eBay partners' policies, creating the problem of initial access. These problems can be summarised in the problem class of inaccessibility regarding information pertaining to data processing and purposes. This problem class can be addressed by the design goal which addresses the **accessibility of information concerning data processing and purposes** (**DG2**).

Various document types such as privacy policy, support policy, cookie policy or security policy are offered by eBay's partners (P_{during} 1). The policies differ in terms of difficulty level, such as being highly legal or containing technical terminology (P_{during} 3). In addition, the information in linked documents is presented in varying detail levels (P_{during} 4). These issues result in the problems class in which the information and its representation vary massively. No uniform act of consent is possible whereby the user is confronted with new circumstances across policies. The third design goal seeks the **uniformity of information concerning data processing and purposes** (**DG3)**.

Partner statements in privacy policies exceed the information of personal data, used technologies and purposes described in eBay's privacy policy and purpose summary (P_{after} 2). Neither the statements of eBay lack in completeness nor are the partners' policies too extensive in describing the data processing and purposes. In addition, the various categories allow a user to decide about the data processing of one partner. Since a partner appears in multiple categories, different choices can be made (P_{after} 5); however, dissociated of the choice, the same partner policy is placed for all purposes. It is not comprehensible how partners operate in the case of deselecting one purpose yet still gain access to personal data via another category. It remains hidden to the user as to whether the purpose leads to distinct processes and data processing at eBay partners. Thereupon, the fourth design goal addresses the non-corresponding statements and seeks **consistency in information concerning data processing and purposes (DG4)**.

The partners involved by eBay include users' personal data in their services and parties processing (P_{after} 1). In this context, no mechanism exists which notifies about changes in a dynamic digital ecosystem (P_{after} 3). The involvement of multiple actors and related dynamics are summarised in the problem class of dynamic service ecosystems. The partners therein, the applied personal data and purposes for processing these data change over time. Thus, the fifth design goal addresses the need for **notifications about changed information of data processing, purposes or involved actors (DG5)**, as consent must be renewed. When consent is provided in a digital service ecosystem regarding processing acts performed by multiple actors, the correctness and accuracy of the information regarding such processing acts must be assured. If this is not possible, modifications in digital service ecosystems are difficult, as the user has provided consent to only the initial state of the ecosystem at the time of his or her granting consent.

The case includes the noteworthy aspect that no information is given if all 906 partners are involved in each user transaction (P_{after} 4). The platform eBay potentially requires all mentioned partners to monetise, improve or monitor their platform. Another interpretation is that eBay refers to only partners that sellers use without utilising them on their own. One could argue that eBay's management of partners is professional and detailed compared with other service providers, as it offers an overview to a large set of actors grouped in categories. However, 79 privacy policies of partners cannot be accessed at all. Users must assume that all listed partners can gain access to their personal data. As every partner specifies its used data and related purposes for data processing – and in this case, 906 partners are involved – consent is provided for an in-total extensive data processing. In addition, personal data may be shared to actors (P_{before} 1) which are not necessarily relevant for a user at all. We grouped these problems in the problem class of extensive consent; therefore, we develop the sixth design goal, which addresses **transaction-specific consent to data processing** (**DG6**).

Of the 2,740 specified partner entries, 906 unique partners are involved in six purpose categories, which creates the problem of acquiring an overview of unique partners (P_{before} 3). In addition, eBay's partners involve other third parties and these parties in turn, which results in a large-scale digital service ecosystem (P_{after} 1). Privacy policies consequently tend to be recursive in digital service ecosystems. The user is exposed to a massive amount of reading time (P_{during} 5), which was calculated for only a fraction of the total digital ecosystem. A median shopping duration of five minutes (Salesforce Commerce Cloud, 2019) has no relation to at least 7,940 minutes of reading time for 'only' partners' privacy policies. The time amount of 5.5 days conflicts with eBay's listing duration options of one, three or five days. A bidding would not be possible if partners' policies were read. The sixth design goal seeks **reasonability of the time required to provide consent in relation to usage time of the service (DG7)**.

No	Problem	Problem Class	Design Goal
P_{before} 1	Personal data are shared with partners by default	Personal data is collected and processed before the user provides consent	DG1: No personal data processing before providing consent
P_{before} 2	Automised activation of every purpose category when a user neglects the privacy settings banner		
P_{before} 6	Requirement to accept data collection and processing on partner websites		
P_{before} 4	Partner privacy policy is not accessible	Inaccessibility of information concerning data processing and purposes	DG2: Accessibility of information concerning data processing and purposes
P_{before} 5	Security issues		
P_{before} 7	Navigation on partner website to partner's privacy policies is not possible		
P_{before} 8	Different policies offered by a single partner		
P_{during} 2	Privacy policies are written in 17 languages		
P_{after} 1	Integration of third parties by eBay partners		
P_{during} 1	Variety of linked documents	Variety of information concerning data processing and purposes in form, terminology and representation	DG3: Uniformity of information concerning data processing and purposes
P_{during} 3	Varying difficulty levels		
P_{during} 4	Varying levels of detail		
P_{after} 2	Different statements regarding used technologies or purposes	Non-corresponding statements concerning personal data processing and purposes in statements of service providers and involved partners	DG4: Consistency in information concerning data processing and purposes
P_{after} 5	Choices for a partner's data processing to multiple purpose categories, but to only one partner policy		
P_{after} 1	Integration of third parties by eBay partners	Dynamic ecosystems include changing and emergent actor involvements, related personal data processing and purposes	DG5: Notifications about changed information of data processing, purposes or involved actors
P_{after} 3	No mechanism notifies about changes regarding partner changes or partners' policy changes		
P_{before} 1	Personal data are shared with partners by default	Consent to an extensive number of actors processing personal data	DG6: Transaction-specific consent to data processing
P_{after} 4	Relevance of partner for user transactions		
P_{before} 3	Difficult to obtain an overview of unique partners	Massive amount of time required for the process of providing consent to use a single digital service	DG7: Reasonability of the time required to provide consent in relation to the usage time of the service
P_{during} 5	Massive amount of time required to read partner policies		
P_{after} 1	Integration of third parties by eBay partners		

Table 7. Design goals for consent in digital service ecosystems

6 Discussion

Our design goals can be applied to enable consent in other contemporary and rising digital service ecosystems. Plausible reasons exist for involving partners in digital service ecosystems (i.e. users expect at least solid performance of digital services, and thus, application performance management is a typical area in which third parties apply). Additionally, personalisation is a common driver for the inclusion of third parties. Nevertheless, the case of eBay demonstrates how large a digital service ecosystem can become and that the existing act of acquiring the user's consent becomes questionable. Even more, digital service ecosystems bear the challenge that privacy policies must consider third parties which include other parties, as well. Recursive digital service ecosystems cannot be covered by the existing form of policies. With numerous partners involved, obtaining access to diverse personal data, increasing points for potential data breaches and negative practices occur. Subsequently, the implications of service usage and associated data provision become incalculable for users. In practice, another method is for digital service providers to mention an involvement of different actor groups for specific purposes. This approach does not specify the involved actors, as categories of recipients may be sufficient (GDPR, 2016, Art. 13 (1) (e)). However, this approach cannot address the problem that oftentimes, these actors process personal data for purposes that are not covered by the digital service provider's policy and the purposes specified therein. This might explain why eBay and other websites link third-party policies.

In the following, we compare the determined design goals and the requirements for effective consent, according to the GDPR (GDPR, 2016, Art. 4 (11)). The aspect of freely given and unambiguous consent is covered by the first design goal pre-privacy protection (DG1). The design goals accessibility (DG2), uniformity (DG3), consistency (DG4) and notifications about changed information (DG5) can be mapped to the characteristic of informed consent. In addition, the design goal transaction-specific consent (DG6) addresses the characteristic of specific consent. However, the design goal reasonability (DG7) does not exactly match one of the requirements of consent as specified by the GDPR. While realising the identified design goals can mean fulfilling the GDPR's requirements for consent, neither the design goals nor the GDPR requirements has a fixed scale with a concrete endpoint. Realising the design goals in a more efficient and better manner could also raise the bar for what is expected by the GDPR. We wish to identify a new aspect of consideration that might be missing from the legal interpretation of what makes consent valid; as our case study demonstrates, the (dis)proportion between the time spent using a service and the time needed to read (let alone understand) its privacy policies are key elements for consent in digital service ecosystems and the plurality of involved actors and therefore privacy policies. Subsequently, two approaches appear suitable for overcoming the issue of reasonability. On one hand, law can attempt to restrict and limit digital service ecosystems and the involvement of numerous service partners. This approach may be successful in limiting personal data sharing in ecosystems. However, specifying the limits of ecosystems and involvement would be challenging and would need to be balanced with the legitimate interests and fundamental rights of the service provider and third parties. On the other hand, the uniformity and machine-readable data processing information would allow for a new form of consent, considering mandatory conditions. Employing a method of automatisation appears plausible in achieving the design goals. The Platform for Privacy Preferences Project (P3P) is no longer supported yet possibly relevant (Cranor and Wenning, 2019). The idea behind this technical platform was the exchange of data processing information as a standard, and it was recommended by the WWW Consortium (W3C) (Cranor and Wenning, 2019). The reactivation of this project would allow for standardising personal data processing information and would have the potential to establish a standard.

With our article, we call for research on the challenging issue of enabling consent to personal data processing in digital service ecosystems. Empirical studies already present manifold problems of single privacy policies (Acquisti and Gross, 2006, Sunyaev et al., 2014, Ermakova et al., 2016). However, as the analysis within this paper reveals, reading, understanding and consenting to a single privacy policy in a meaningful manner is not common practice in digital service ecosystems. The GDPR declares that consent is valid when it is freely given and unambiguously voiced for a specific purpose or specific set of purposes and based on an informed decision. In the absence of precedent court rulings, no definite lines of interpretation for these requirements exist. Practices consequently arise which may understate specifications made in the GDPR. Still, the existing understanding by both legal scholars and the few court decisions that exist are sufficient for casting serious doubts about the validity of consent provided in scenarios such as the one assessed in this paper. Given that privacy policies are a legal instrument necessary for ensuring consent to data processing in the lied-out manner, it is highly important that these policies are usable from a user's perspective. A broader dialogue with legal scholars in consideration of the existing laws is necessary for redesigning consent. In addition, the perspective of IS scholars can be highly beneficial in filling the GDPR's abstract provisions with life and developing their scope.

This study introduces interdisciplinary avenues for further research. In particular, this study reveals that enabling consent can be acquired only through a dialogue between stakeholders from both professions: the legal and information systems disciplines. In doing so, further research can contribute to this area by addressing the limitations of this study. Furthermore, how dynamic privacy policies in service ecosystems are is mirrored in a recent change made by eBay: The names of purpose categories changed. In addition, the platform began to include additional detail regarding what information is shared with third parties. However, this information is not yet available for all partners. Thus, we decided to not include this additional material, as the design goals are not affected by this change. An analysis of these changes can be beneficial for further results. By utilising other digital service ecosystems, the design goals can be expanded and refined for specific solutions towards design principles. However, this was not the aim of this manuscript and would have gone beyond the scope of this study.

7 Conclusion

This manuscript's primary contribution is seven design goals that guide organisations and researchers in addressing consent in digital service ecosystems. We demonstrated a new dimension of effort for the act in this context. With the benchmark of 906 involved partners and 132.3 hours needed for reading the policies, our selected case achieves a magnitude for which nobody can claim a well-balanced ratio of time to become informed before providing consent. The existing form leads to incomprehensibility of personal data processing. Users consequently possess consent fatigue (Schraefel et al., 2017) and may not be equipped to act in their own self-interests. It would be wrong to cling to forms which even today do not fulfil their function in ensuring effective consent and cannot keep up with service ecosystems.

Promising approaches through creating summaries based on artificial intelligence are already in use (Harkous et al., 2018) and could be combined with our design goals to address characteristics of emerging digital service ecosystems. As demonstrated in the comparison with the GDPR, the determined design goals can support service providers positioned in ecosystems to implement the legal requirements. Additionally, the balancing act of implementation and in turn the generative improvement of all design goals has the potential to shape the GDPR requirements in a way that raises the bar and gradually closes the gap between what the GDPR deems adequate regarding, for example, when a user is sufficiently informed about processing circumstances and the user's de facto understanding. As the scope of (most) GDPR provisions is dynamic rather than static, it evolves alongside the 'state of the art' (GDPR, 2016, Art. 24 (1), 25 (1)). The increasing complexity of connected actors involved in service provision lead to insufficient operability of consent and therefore necessitate a redesign. We pave the way for research and practice for consent in consideration of emerging digital service ecosystems.

Acknowledgements

This research was sponsored by the Hamburg Ministry of Science, Research and Equality in the project Information Governance Technologies under the reference LFF-FV 34.

References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). 'Privacy and human behavior in the age of information', *Science,* 347(6221), 509-514.

Acquisti, A. and Gross, R. (2006). 'Imagined communities: Awareness, information sharing, and privacy on the Facebook', *International workshop on privacy enhancing technologies*, 36-58.

Bahr, K. D. (2019). 'KG Berlin: Umfangreiche DSGVO-Verstöße bei Google-Datenschutzerklärung'. https://www.dr-bahr.com/news/umfangreiche-dsgvo-verstoesse-bei-google-datenschutzerklaerung.html (visited on 01.08. 2019).

Barrett, M., Davidson, E., Prabhu, J. and Vargo, S. L. (2015). 'Service innovation in the digital age: key contributions and future directions', *MIS Quarterly,* 39(1), 135-154.

Baskerville, R. and Pries-Heje, J. (2010). 'Explanatory design theory', *Business & Information Systems Engineering,* 2(5), 271-282.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987). 'The Case Research Strategy in Studies of Information Systems', *MIS Quarterly,* 11(3), 369-386.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N. (2018). 'Third Party Tracking in the Mobile Ecosystem', *Proceedings of the 10th ACM Conference on Web Science.*

Bitner, M. J., Ostrom, A. L. and Morgan, F. N. (2008). 'Service blueprinting: A practical technique for service innovation', *California Management Review,* 50(3), 66.

Carver, R. P. (1990) *Reading rate: A review of research and theory,* Academic Press.

Chandler, J. D. and Lusch, R. F. (2015). 'Service Systems: A Broadened Framework and Research Agenda on Value Propositions, Engagement, and Service Experience', *Journal of Service Research.*

chrome web store (2019). 'Scraper'. https://chrome.google.com/webstore/detail/scraper/mbigbapnjcgaffohmbkdlecaccepngjd (visited on 20.07. 2019).

Cranor, L. and Wenning, R. (2019). 'Platform for Privacy Preferences (P3P) Project'. https://www.w3.org/P3P/ (visited on 12.11. 2020).

Cronholm, S. and Göbel, H. (2019). 'Design Science Research Constructs: a Conceptual Model', in *Pacific Asia Conference on Information Systems 2019*,

Crummy (2015). 'Beautiful Soup Documentation'. https://www.crummy.com/software/BeautifulSoup/bs4/doc/ (visited on 28.07. 2019).

de Reuver, M., Sørensen, C. and Basole, R. C. (2018). 'The digital platform: a research agenda', *Journal of Information Technology,* 33(2), 124-135.

Di Luzio, A., Mei, A. and Stefa, J. (2016). 'Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests', in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, IEEE, 1-9.

eBay (2019a). 'Advertising and related preferences'. www.ebay.com/gdpr (visited on 09.08. 2019).

eBay (2019b). 'User Privacy Notice'. https://www.ebay.com/help/policies/member-behaviour-policies/user-privacy-notice-privacy-policy?id=4260 (visited on 27.07. 2019).

Ermakova, T., Fabian, B. and Babina, E. (2015). 'Readability of Privacy Policies of Healthcare Websites', *Wirtschaftsinformatik*, 1085-1099.

Ermakova, T., Krasnova, H. and Fabian, B. (2016). 'Exploring the impact of readability of privacy policies on users' trust', *European Conference on Information Systems (ECIS).*

EuropeanCommission (2014). 'Article 29 Data Protection Working Party - Opinion 05/2014 on Anonymisation Techniques'.

Fischer, C., Winter, R. and Wortmann, F. (2010). 'Design theory', *Business & Information Systems Engineering,* 2(6), 387-390.

GDPR (2016). 'General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Directive 95/46)', 59, 1-88.

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E. and Zhdanov, D. (2018). 'How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas', *MIS Quarterly,* 42(1), 143-164.

Gregor, S. and Jones, D. (2007). 'The anatomy of a design theory', *Journal of the Association for Information Systems,* 8(5), 312.

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G. and Aberer, K. (2018). 'Polisis: Automated analysis and presentation of privacy policies using deep learning', *27th {USENIX} Security 18*, 531-548.

Hein, A., Scheiber, M., Böhm, M., Weking, J. and Krcmar, H. (2018). 'Towards a Design Framework for Service Platform Ecosystems', in *The European Conference on Information Systems*.

Horlach, B., Schirmer, I. and Drews, P. (2019). 'Agile Portfolio Management: Design Goals and Principles', *Proceedings of the European Conference on Information Systems, Stockholm-Uppsala, Sweden (ECIS 2019)*.

Ji, S., Mittal, P. and Beyah, R. (2016). 'Graph data anonymization, de-anonymization attacks, and de-anonymizability quantification: A survey', *IEEE Communications Surveys & Tutorials,* 19(2), 1305-1326.

Kuechler, B. and Vaishnavi, V. (2008). 'On theory development in design science research: anatomy of a research project', *European Journal of Information Systems,* 17(5), 489-504.

Kurtz, C., Semmann, M. and Böhmann, T. (2018a) 'Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors', in *Americas Conference on Information Systems*, New Orleans,

Kurtz, C., Semmann, M. and Schulz, W. (2018b) 'Towards a Framework for Information Privacy in Complex Service Ecosystems', in *International Conference on Information Systems (ICIS)*, San Fransisco,

Kurtz, C., Wittner, F., Semmann, M., Schulz, W. and Böhmann, T. (2019) 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems', in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Hawaii,

Legner, C. and Löhe, J. (2012). 'Improving the realization of IT demands: A design theory for end-to-end demand management'.

Libert, T. (2018). 'An automated approach to auditing disclosure of third-party data collection in website privacy policies', in *Proceedings of the 2018 World Wide Web Conference*, International World Wide Web Conferences Steering Committee, 207-216.

Litman-Navarro, K. (2019). 'We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.'. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (visited on 30.07. 2019).

Lusch, R. F. and Vargo, S. L. (2014) *Service-dominant logic: Premises, perspectives, possibilities,* Cambridge University Press.

Malaga, R. A. (2014). 'Do web privacy policies still matter?', *Journal of Management Information Systems,* 17(1), 95.

Malandrino, D. and Scarano, V. (2013). 'Privacy leakage on the Web: Diffusion and countermeasures', *Computer Networks,* 57(14), 2833-2855.

McDonald, A. M. and Cranor, L. F. (2008). 'The cost of reading privacy policies', *I/S: A Journal of Law and Policy for the Information Society,* 4, 543.

Narayanan, A. and Shmatikov, V. (2008). 'Robust de-anonymization of large sparse datasets', in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, IEEE, 111-125.

Natural Language Toolkit (2019). 'NLTK 3.4.5'. https://www.nltk.org/# (visited on 28.07. 2019).

Paspatis, I., Paspatis, I., Tsohou, A., Tsohou, A., Kokolakis, S. and Kokolakis, S. (2017). 'Mobile application privacy risks: Viber users' de-anonymization using public data', in *Mediterranean Conference on Information Systems (MCIS)*, Association For Information Systems,

Rainie, L. and Duggan, M. (2016). 'Privacy and information sharing', *Pew Research Center,* 16.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C. and Gill, P. (2018). 'Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem', *Network and Distributed Systems Security (NDSS) Symposium 2018*.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Liu, F., McDonald, A., Norton, T. B. and Ramanath, R. J. B. T. L. (2015). 'Disagreeable privacy policies: Mismatches between meaning and users' understanding', *Berkeley Tech. LJ,* 30, 39.

Riedl, C., Boehmann, T., Leimeister, J. M. and Krcmar, H. (2009). 'A framework for analysing service ecosystem capabilities to innovate', *17th European Conference on Information Systems*.

Rohleder, B. (2015). 'Datenschutz in der digitalen Welt', *bitkom*.

Schraefel, M., Gomer, R., Alan, A., Gerding, E. and Maple, C. (2017). 'The internet of things: interaction challenges to meaningful consent at scale', *interactions,* 24(6), 26-33.

Sunyaev, A., Dehling, T., Taylor, P. L. and Mandl, K. D. (2014). 'Availability and quality of mobile health app privacy policies', *Journal of the American Medical Informatics Association,* 22(e1).

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S. and Serna, J. (2018). 'I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR', in *Companion Proceedings of the The Web Conference 2018*, International World Wide Web Conferences Steering Committee, 163-166.

Van Alstyne, M. W., Parker, G. G. and Choudary, S. P. (2016). 'Pipelines, platforms, and the new rules of strategy', *Harvard Business Review,* 94(4), 54-62.

Vargo, S. L. and Akaka, M. A. (2012). 'Value cocreation and service systems (re) formation: A service ecosystems view', *Service Science,* 4(3), 207-217.

Vargo, S. L., Maglio, P. P. and Akaka, M. A. (2008). 'On value and value co-creation: A service systems and service logic perspective', *European management journal,* 26(3), 145-152.

Walls, J. G., Widmeyer, G. R. and El Sawy, O. A. (1992). 'Building an information system design theory for vigilant EIS', *Information Systems Research,* 3(1), 36-59.

Wilson, S., Schaub, F., Dara, A. A., Liu, F., Cherivirala, S., Leon, P. G., Andersen, M. S., Zimmeck, S., Sathyendra, K. M. and Russell, N. C. (2016). 'The creation and analysis of a website privacy policy corpus', *Meeting of the Association for Computational Linguistics*, 1330-1340.

Yin, R. K. (2009) *Case Study Research: Design and Methods* SAGE.

Yu, L., Luo, X., Liu, X. and Zhang, T. (2016). 'Can we trust the privacy policies of android apps?', in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, IEEE, 538-549.

Zimmeck, S., Story, P., Smullen, D., Ravichander, A., Wang, Z., Reidenberg, J., Russell, N. C. and Sadeh, N. (2019). 'MAPS: Scaling privacy compliance analysis to a million apps', *Proceedings on Privacy Enhancing Technologies,* 2019(3), 66-86.