IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 23, 2017, accepted October 1, 2017, date of publication October 23, 2017, date of current version November 14, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2765539

Tools for Achieving Usable Ex Post Transparency: A Survey

PATRICK MURMANN AND SIMONE FISCHER-HÜBNER, (Member, IEEE)
Department of Mathematics and Computer Science, Karlstad University, 651 88 Karlstad, Sweden

Corresponding author: Simone Fischer-Hübner (simone.fischer-huebner@kau.se)

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant 675730.

ABSTRACT Transparency of personal data processing is a basic privacy principle and a right that is well acknowledged by data protection legislation, such as the EU general data protection regulation (GDPR). The objective of ex post transparency enhancing tools (TETs) is to provide users with insight about what data have been processed about them and what possible consequences might arise after their data have been revealed, that is, ex post. This survey assesses the state of the art in scientific literature of the usability of ex post TETs enhancing privacy and discusses them in terms of their common features and unique characteristics. The article first defines the scope of usable transparency in terms of relevant privacy principles for providing transparency by taking the GDPR as a point of reference, and usability principles that are important for achieving transparency. These principles for usable transparency serve as a reference for classifying and assessing the surveyed TETs. The retrieval and screening process of the publications is then described, as is the process for deriving the subsequent classification of the characteristics of the TETs. The survey not only looks into what is made transparent by the TETs but also how transparency is actually achieved. A main contribution of this survey is a proposed classification that assesses the TETs based on their functionality, implementation and evaluation as described in the literature. It concludes by discussing the trends and limitations of the surveyed TETs in regard to the defined scope of usable TETs and shows possible directions of future research for addressing these gaps. This survey provides researchers and developers of privacy enhancing technologies an overview of the characteristics of state of the art ex post TETs, on which they can base their work.

INDEX TERMS GDPR, HCI, privacy, transparency, usability, visualization.

I. INTRODUCTION

Transparency of personal data processing can play an important factor for establishing user trust in applications. As previous studies show, trust in an application can be enhanced if procedures are clear, transparent and reversible, so that users feel in control [1], [2].

Transparency is also an important privacy principle, and a means for meeting with information asymmetry, which, according to Calo [3], arises due to different, unbalanced perspectives of multiple parties as a potential privacy harm.

It is a prerequisite for the data subjects[1] to control their personal spheres, and thus to exercise their rights of informational self-determination. In particular, it is a precondition for 'intervenability' as specified by ENISA [4]. Intervenability allows data subjects to 'intervene' with ongoing or planned processing of their personal data, for example by requests to correct, block or erase the data.

As the German constitutional court declared in its Census Decision, transparency is not only crucial as an individual basic right but also for democracy: "A society in which individuals can no longer ascertain who knows what about them and when and a legal order that makes this possible would not be compatible with the right to informational self-determination." Self-determination is in turn "an elementary prerequisite for the functioning of a free democratic society predicated on the freedom of action and participation of its members" [5].

Throughout this survey, the term 'transparency'[2] refers to the property of 'visibility' as specified by Turilli *et al.* [7].

[1] A data subject is a natural person about whom personal data is processed.

[2] Transparent (adjective): "(2.a) free from pretense or deceit: frank, (2.b) easily detected or seen through: obvious, (2.c) readily understood, (2.d) characterized by visibility or accessibility of information especially concerning business practices." [6]

In this context, transparency is described as a state in which any obstacles that may impede the visibility of the underlying data are being mitigated. In a transparent environment, data that have been disclosed previously by a data subject are accessible later for information and for enabling future decisions. Processes that aim at being transparent depend on factors such as the availability and accessibility of respective transparency-enhancing mechanisms. Such processes depend on ethical, business and legal factors, all of which may impose constraints on the stakeholders involved in storing and processing the underlying data. In that regard, the meaning of the term transparency differs from the alternative meaning often implied in computer science and computing,[3] which denotes the property of 'invisibility,' such as hiding the implementation details of a process or component from the user of the system [7].

Most Western privacy and data protection laws or guidelines grant data subjects with extensive information, access and control rights for enforcing transparency and intervenability. For instance, the OECD Privacy Guidelines [9] aim at enforcing transparency and intervenability by their 'Openness' and 'Individual Participation' principles. The EU General Data Protection Regulation (GDPR) [10], which came into force in May 2016 and will apply in EU member states from May 25th, 2018, provides data subjects with extensive rights for transparency, intervenability and control. In contrast to the high level statement of transparency principles of the OECD Guidelines, it defines in much detail what transparency should comprise. For this reason, this survey is based on the legal stipulations by the GDPR.

The concept of transparency comprises both 'ex ante transparency' and 'ex post transparency' [11]. Ex ante transparency informs about the intended data collection, processing and disclosure, and thus enables the anticipation of consequences before data are actually disclosed, for example with the help of privacy policy statements. Ex post transparency provides insight about what data were collected, processed or disclosed by whom and to whom, and whether the data processing has been in conformance with negotiated or stated policies and should particularly inform about consequences if data already have been revealed.

Transparency Enhancing Tools (TETs) can help individuals to exercise their right for transparency, and subsequently for intervenability, by technological means. TETs can be defined as tools providing insight into how the users' data are being collected and processed, and visualise related consequences in an accurate and comprehensible way [12].

Even though research has been conducted on ex ante and ex post TETs, as well as on the usability of both types of TETs, technical standards for how such tools should be implemented are still missing. Existing implementations often focus on a handpicked selection of features, but it is not always clear how the respective feature sets relate to the underlying legal principles and societal needs. As far as the authors are aware, no classification of ex post TETs exists that explicitly focuses on usability and that is based on a systematic review of such artifacts in the scientific body of knowledge.

This paper presents a survey for assessing the state of the art of ex post TETs for enhancing privacy and their usability aspects in the scientific literature. It aims to discuss and classify them in terms of their common features, unique characteristics and overarching concepts. The authors' focus has especially been on surveying ex post TETs and their usability features, which support users to achieve ex post transparency and which may also enable them to subsequently exercise their intervenability rights, for the following reasons: The GDPR has specifically extended the data subject rights to ex post transparency[4] and to intervenability.[5] Besides, the GDPR emphasises that transparency should be provided in a concise, intelligible and easily accessible, that is usable, form. Usable ex post TETs that enable end users to exercise these data subject rights of access and to intervenability online will therefore play an even more important role for the users' privacy self-protection in the future, which has motivated this survey on usable ex post TETs. Moreover, the authors' decision to focus on ex post TETs was also motivated by the fact that in comparison to ex ante TETs, which comprise a broad range of technical tools and concepts, the area of ex post TETs is less researched and the scope is more limited.

Existing literature surveys on TETs [12], [13] have neither focused in depth on ex post TETs nor on recent TETs and their usability. In that regard, this survey analyses the means employed by the reviewed ex post TETs to provide their respective functionality, and seeks to find patterns in the attempt to make the tools usable by the target audience. In the specific context of ex post TETs, this survey aims to make a contribution to science by answering the following questions:

1) What are the characteristics of usable ex post TETs for enhancing privacy published in scientific literature?
2) How can these TETs be classified?
3) How does the proposed classification relate to and differ from the findings of previous surveys on TETs and PETs?
4) What aspects of usable ex post TETs are not covered by the TETs in the reviewed literature?

The remainder of this paper is organised as follows: Section II derives legal privacy and Human Computer Interaction (HCI) principles for usable transparency that will be used as a basis for the classification and assessment. Section III discusses previous work related to the subject matter. Section IV elaborates on the method that led to the selection of the reviewed literature, and consequently the basic set of TETs that are discussed throughout the rest of

[3]Transparent (adjective): "(of a process or interface) functioning without the user being aware of its presence." [8]

[4]For example by extending the right of data access with the right to receive also an electronic copy of their data undergoing processing, and by allowing the data subjects to receive the information in a commonly used electronic form for request done by electronic means.

[5]For example by extending the right to data erasure, that is, the 'right to be forgotten,' and introducing the right to data portability.

the paper. Section V proposes a classification scheme based on the characteristics detected in the reviewed TETs. Section VI summarises and assesses the major findings obtained by classifying the TETs of the reviewed literature, and discusses limitations of the reviewed state of the art literature in terms of the derived principles for usable transparency. Thereby, it also shows aspects of TETs areas that are worthwhile to research and develop further. Section VII finally concludes the paper with major conclusions with regard to the research questions.

II. PRINCIPLES FOR USABLE TRANSPARENCY

As mentioned earlier, in this paper, the term 'transparency' refers to forms of information visibility, as specified by Turilli *et al.* [7]. To explore transparency in the privacy context, two different aspects should be taken into consideration: (1) what information should be made visible, and (2) what usable forms of presentation of this information can be used to achieve visibility.

Section II-A discusses the legal privacy principles for promoting transparency pursuant to the EU GDPR, which specifies what information should be made visible and how, while section II-B will then more generally discuss principles for usable presentation of transparency information from an HCI-perspective.

A. LEGAL PRINCIPLES FOR TRANSPARENCY

For deriving principles with regard to what information should be made transparent for promoting privacy and how, the authors refer to the GDPR, which defines in its recitals and articles detailed legal principles for providing ex ante and ex post transparency that data controllers[6] need to fulfill. Even though TETs are not necessarily tools provided by data controllers but are in most cases developed as 'privacy self-protection' tools for users, for the purpose of the study at hand, the principles by the GDPR provide a useful description of what the privacy principle of transparency should practically offer to data subjects. For this reason, legal principles that are elicited in this section will also be used for the classification and assessment of TETs in this article.

Although this survey is restricted to ex post TETs, the authors decided to also explore the legal principles of ex ante transparency in addition to principles for transparency in general and for ex post transparency, as they can provide additional criteria as to what transparency in general should offer and comprise.

1) TRANSPARENCY IN GENERAL

As regards transparency, the GDPR requires pursuant to its Art. 12, and explains in Recitals 39 and 59, that any transparency information relating to data processing should be provided to the data subject in a 'concise, easily accessible form.' It should be 'intelligible' and 'easy to understand,' and should be provided 'using clear and plain language.' Where appropriate, visualisation should be used. According to Recital 39, data subjects should be "made aware of risks, rules, safeguards and data subject rights" (of access and to intervene) and be informed 'how to exercise their rights' in relation to the processing of their personal data.

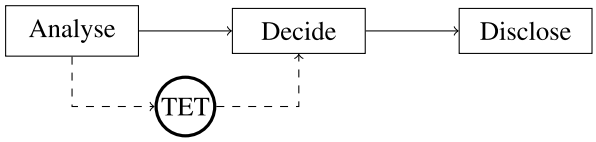


FIGURE 1. Sequential steps involved in an ex ante decision-making process. Solid lines show transitions between states. Dashed lines signify transitions supported by a TET.

2) EX ANTE TRANSPARENCY

Ex ante transparency is a condition that enables data subjects be in control and to render a consent. Pursuant to its definition in Art. 4 (11) GDPR, rendered consent has to be informed consent in order to be valid. Pursuant to Art. 13 GDPR, the data controller must ensure that when personal data are collected from a data subject, the data subject is provided with relevant privacy policy information, including at least information about the identity of the data controller, the data processing purposes (Figure 1). To ensure fair and transparent processing also information is needed such as about recipients or categories of recipients, data subject rights including the right to withdraw consent at any time, the right to lodge complaint with a supervisory authority, the legal basis of whether the data subject is obliged to provide the data, consequences of not providing the data, as well as the existence of automated decision-making including profiling, the logic involved, significance and envisaged consequences. Art. 14 GDPR requires that similar information needs to be provided in the case that the personal data have not been obtained from the data subject. Pursuant to Art. 12 (7), ex ante transparency information may be provided in combination with standardised icons for improving the usability of privacy policy information, which should be machine-readable to support electronic policy statements.

3) EX POST TRANSPARENCY AND INTERVENABILITY

The GDPR provides data subjects with the right of access to their data pursuant to Art 15, which comprises the right to obtain information about the data being processed, data processing purposes, data recipients or categories of recipients ('downstream data processors', Figure 2), as well as information about the logic involved with regard to any automatic processing including profiling. In the latter case, data subjects should also be informed about the significance and envisaged consequences of such processing. The controller shall provide to the data subject a copy of the personal data undergoing processing, and in the case that the data subject

[6] A data controller denotes a natural or legal person, which, alone or jointly with others, determines the purposes or means of personal data processing (c.f. Art. 4 (7) GDPR).

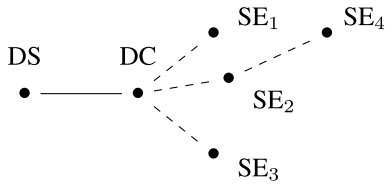


FIGURE 2. Relationship between a data subject (DS), a data controller (DC), and potentially several secondary entities (SE) in the form of downstream data processors. Dashed lines signify the retransmission of personal data to downstream processors.

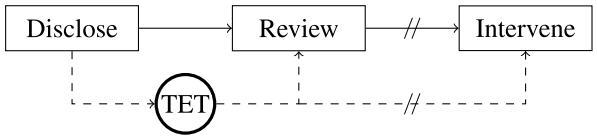


FIGURE 3. Sequential steps involved in an ex post review process. Solid lines show transitions between states. Dashed lines signify transitions supported by a TET. Intervention as an optional function supported by some TETs is delimited via '//'.

makes the request in electronic form, the information should be provided in ''an electronic form, which is commonly used.'' Moreover, the right to Data Portability (Art. 18), that is, the right to receive data in a structured and commonly used, machine-readable format, and the right to transmit data to another controller, or to have it transmitted directly from controller to controller, could also be used as a means for enhancing transparency. Its main objective, however, is to prevent data subjects from being 'locked' into privacy-unfriendly services by allowing them to easily change providers along with their data. Nevertheless, in contrast to the electronic copy of the data under processing that the data subject has the right to receive pursuant to Art. 15, exported data will usually only contain the data that the data subject has explicitly or implicitly disclosed, but not necessarily the data that the service provider derived from that data. Such derived data, for example in the form of user profiles, may represent a business value for a company, which may thus not support a transfer of such derived data to a competing service provider.

Ex post transparency is also a prerequisite for exercising 'intervenability' rights of the data subjects. Even though intervenability goes beyond transparency, data subjects should be provided ex post transparency about their intervenability rights and , as mentioned in Recital 39, should be made aware of how to exercise them. These intervenability rights include the right to withdraw consent at any time, which should be made as easy as to give it (Art. 5), to request correction or deletion, the right to restrict the processing, as well as the newly introduced 'right to be forgotten' in a timely manner (Art. 16, 17, 17a) (Figure 3).

Furthermore, the requirement of data breach notification pursuant to Art. 34 by a data controller to an affected data subject shall provide transparency of a personal data breach that is likely to result in a high risk to the data subject's rights and freedom. Transparency, especially thorough Data Breach Notification, is also a prerequisite for enforcing the principle of accountability of data controllers, which is named as an explicit principle of the OECD privacy guidelines and also part of the GDPR (Art. 5 2.).

B. GENERAL USABILITY PRINCIPLES FOR TRANSPARENCY

As pointed out by Patrick *et al.* [14], legal privacy principles, such as the transparency principle, have HCI implications as ''they describe mental processes and behaviour that the data subjects must experience in order for a service to adhere to these principles.'' In particular, the transparency principle requires that data subjects comprehend the transparency and control options, are aware of when they can be used, and are able to use them. In other words, transparency can only be achieved if transparency information is presented in a 'usable' manner; therefore, another important design criterion for TETs is usability.

As discussed above, the GDPR for this reason requires in its Art. 12 (1) that any transparency information needs to be provided to the data subject in an intelligible, easy-to-understand, and thus usable manner. In this section, usability principles will be presented in more detail. These principles have been accepted as relevant for assessing the usability of systems, and which, for this reason, will be referred to in the survey for the classification and assessment of usable TETs.

In the context of this survey, the usability of a TET refers to the superimposition of multiple principles specified independently in different recommendations, guidelines and standards.

ISO 9241-11 [15] defines (1) Effectiveness, (2) Efficiency and (3) User satisfaction as usability principles for completing a task.

ISO 9241-110 [16] defines seven dialogue principles for human-machine interaction: (1) Suitability for the task, (2) Self-descriptiveness, (3) Conformity with user expectations, (4) Suitability for learning, (5) Controllability, (6) Error tolerance, and (7) Suitability for individualisation.

Nielsen [17] stipulates ten usability heuristics necessary to successfully implement user interfaces (UIs) of task-oriented interaction systems: (1) Visibility of the system status, (2) Match between system and the real world, (3) User control and freedom, (4) Consistency and standards, (5) Error prevention, (6) Recognition rather than recall, (7) Flexibility and efficiency of use, (8) Aesthetic and minimalist design, (9) Help users recognize, diagnose, and recover from errors, and (10) Help and documentation.

Patrick *et al.* [14] define (1) Comprehension, (2) Consciousness, (3) Control, and (4) Consent as four basic requirements for the design of user interfaces for privacy-enhancing technologies (PETs).

The specifications provided by ISO and Nielsen are generic principles meant to be applicable to task-oriented interaction systems in general. Their purpose is to allow for the assessment of completing a task in a well-defined usage context. Conversely, in the context of TETs, these principles are considered benchmarks in terms of individual characteristics of

a TET. Individual principles may apply to a varying degree, or may not be applicable to certain aspects of TETs at all. The applicability of the principles is discussed in section V, following the descriptions of the characteristics throughout the classification.

Whereas some of the principles are congruent or bear similar meanings across multiple sources, such as 'error tolerance' [16] and 'help users recognize, diagnose, and recover from errors' [17], the semantics of the employed terminology may differ. For example, while 'controllability' described by ISO [16] refers to users literally being in control over an interaction process at all times, Patrick *et al.* [14] discuss 'control' in the specific scope of data subjects exercising control over the flow of their personal data. In the context of this survey, all usability principles are scrutinised through the lens of ex post TETs that aim to fulfill the legal requirements of transparency as stipulated in section II-A. By doing so, their specificity is raised from an abstract level to the respective usage context of individual TETs.

III. RELATED WORK

Work related to this survey comprises two surveys on PETs and TETs, respectively.

Hedbom's [13] survey on PETs names the legal stipulations of the European Union as the core principle underlying the necessity of PETs. The classification used in the survey is built on conceptional, socio-structural and technical aspects. The scope is specifically restricted to practical implementations, which includes remote services, stand-alone applications, and browser plug-ins that were available at the time of publishing, but disregards enabler technologies and protocols.

Janic *et al.*'s [12] survey on TETs focuses on the aspect of trust. The authors discuss the connection between trust, privacy concern, and transparency. They reflect on how a user's privacy concerns influence her trust in the service she uses, and whether an increase of transparency implies an increased amount of trust. The authors discuss the available publications, and then continue to analyse selected TETs according to the factors previously ascertained in the gathered body of evidence.

Hedbom defines transparency in the context of TETs as information about the actual or intended collection, storage, or processing of personal data. Janic et al. define transparency as ''insight in how user's data is being collected, stored, processed and disclosed'' [12]. Conversely, this survey considers the term 'transparency' beyond mere conceptional reflection. It aims to answer the question of how exactly individual implementations actually manage to make transparent the processes they were designed for. The design decisions made for the TETs depend on but are not limited to factors such as the stakeholders involved, the environment in which they interact with each other, and the type of device or platform respective TETs operate on.

Hedbom as well as Janic et al. briefly discuss the aspect of comprehensibility and usability. Hedbom [13] classifies the 'ease of access' as an aspect related to the security requirements of a tool, arguing that tools that are easier to access provide better usability. He attributes comprehensibility in the sense of being easy to understand to a specific type of audience targeted by TETs, namely data subjects in their role as non-professionals. In that regard, that target group's preference for comprehensible information is contrasted by the demands of domain experts whose demands are oriented towards detailed information, which, according to Hedbom, comes at the cost of immediate approachability. Janic et al. [12] discuss the aspect of usability explicitly in the context of the comprehensibility of TETs. They hold that comprehensible tools are more likely to support a user's awareness, and are thus more suitable to act as enablers of transparency.

However, neither of the two surveys goes into detail about the means by which usability of the reviewed PETs and TETs is achieved, nor whether and how user studies were conducted to test the usability of the respective implementation by the respective target audience. This survey, on the other hand, specifically analyses the means that the reviewed TETs have chosen to achieve usability. The literature research described in Section IV is based on documented methodology, and specifies usability as a key criterion for the screening of the papers.

Moreover, the classification scheme presented in this survey in Section V is more detailed and more fine-grained than the ones used in previous surveys and emphasises the connection of its characteristics to the legal and usability principles pointed out in Section II. It comprehends visualisation techniques and usability as a major category of how to meaningfully convey information about disclosed personal data. As such, this survey builds upon and significantly extends and updates the two existing surveys, reviewing contemporary ex post TETs that were discussed in the scientific literature after the aforementioned surveys were published. The contextual scope of this survey is narrower with a fine-grained classification and assessment of ex post TETs compared to the previous surveys, which consider the broader spectrum of PETs and TETs, including ex ante TETs.

IV. LITERATURE RESEARCH

The methodology used for the literature research was based on the procedure described by Webster *et al.* [18]. However, instead of relying on a carefully selected, hand-picked set of articles that serves as a starting point for the subsequent search, the initial approach suggested by Kitchenham *et al.* [19] was chosen. The latter approach relies on an initial database search that yields a set of publications on which, in turn, all further selection is based.

The initial search was based on database queries performed on the databases provided by Inspec [20] and DBLP [21], as well as the publication databases of the two publishers ACM [22] and IEEE [23]. These databases were chosen because of the high quality of the publications available in or referenced by them. This choice biased the research

conducted throughout the retrieved publications towards the disciplines of computer science, information systems and engineering. The thematic restriction was considered as much a limitation for the breadth of the review as it was considered a deliberate choice regarding the feasibility of the systematic approach.

Each database was queried using the semantic equivalent of the same set of well-defined search terms. The terms were derived from the intersection of the three thematic areas of *privacy, transparency* and *usability.* The logical combination of a set of respective search terms defined the scope in which relevant publications were assumed to reside. The query of the literature databases resulted in over 800 unique papers. After the first review of these papers, it was obvious that the number of publications dealing with ex ante TETs by far exceeded the ones that covered ex post TETs. It was at this point that the contextual scope of the literature review was further narrowed down to implementations of ex post TETs and disregarded papers that exclusively dealt with ex ante scenarios.

During the subsequent screening phase, all publications were checked for content-related relevance, as well as for a set of selection criteria that warranted the scientific relevance of the papers. The rigorous screening of the retrieved publications ensured that only publications were selected that represented original implementations that existed in the form of usable prototypes. It was considered a plus if a paper elaborated on the user study conducted to verify the usability of the TET, but such studies were not a criterion for inclusion in the result set. The screening process resulted in 12 publications that met the specified prerequisites.

The subsequent snowballing phase traced the references of the publications backwards and forwards, and was carried out according to the recommendations of Webster *et al.* [18]. Scopus was used to generate a set of references based on the original result set retrieved during the initial search phase, and yielded more than 300 additional publications. The screening of these articles was conducted by applying the exact same criteria that had been used during the screening of the initial result set. The screening of the references yielded nine additional publications, resulting in 21 publications that met the specified criteria.

A comprehensive description of the information retrieval and screening process is being provided as a technical report [24]. That report also provides brief summaries of the individual functionality of each of the reviewed papers. After finalising the report, two additional papers, [25] and [26], were included that meet the selection criteria. Moreover, the implementations of the TETs presented by Fischer-Hübner *et al.* [27] were broken down into two distinctive TETs, [28] and [29], increasing the total number of papers to 24. A concise overview of the reviewed papers is provided in Table 1.

Each of the final set of 24 publications describes an implementation that thematically qualifies as an ex post TET, and that meets the criteria specified for the screening process.

TABLE 1. List of reviewed publications on ex post TETs.

Year	Authors	Title (abbreviated)
2007	Hsieh, Tang, Low, et al. [30]	Field deployment...
2008	Abdullah, Conti, Beyah [31]	A Visualization...
2008	Kelley, Drielsma, et al. [32]	User-controllable Learning...
2009	Kolter, Kernchen, Pernul [33]	Collaborative Privacy...
2009	Sadeh, Hong, Cranor, et al. [34]	Understanding...
2009	Tsai, Kelley, Drielsma, et al. [35]	The impact of feedback...
2010	Kolter, Netter, Pernul [36]	Visualizing Past Personal...
2010	Toch, Cranshaw, et al. [37]	Empirical models of...
2011	Schlegel, Kapadia, Lee [38]	Eying Your Exposure...
2012	Trabelsi, Sendor [39]	Sticky policies for data...
2012	Kani-Zabihi, Helmhout [25]	Increasing Service Users'...
2013	Balebako, Jung, Lu, et al. [40]	Little Brothers Watching...
2013	Bilogrevic, Huguenin, et al. [41]	Adaptive Information...
2013	Louw, von Solms [42]	Personally Identifiable...
2013	Biswas, Aad, Perrucci [43]	Privacy Panel...
2013	Zavou, Pappas, Kemerlis [44]	Cloudopsy: An autopsy...
2014	Mun, Kim, Shilton, et al. [45]	PDVLoc...
2015	Xu, Zhu [46]	SemaDroid...
2015	Pistoia, Tripp, Centonze, et al. [47]	Labyrinth...
2015	Angulo, Fischer-Hübner et al. [28]	Usable Transparency...
2016	Bier, Kühne, Beyerer [48]	PrivacyInsight...
2016	Popescu, Hildebrandt, et al. [26]	Increasing Transparency...
2016	Riederer, Echickson, et al. [49]	FindYou...
2017	Karegar, Pulls, Fischer-Hübner [29]	Visualising Exports...

According to the descriptions provided in the publications, the implementations vary in terms of maturity. They range from prototypical implementations in the testing stage to software tools that have been tested repeatedly, and that appear to be ready to be used by the target audience they were designed for. Similarly, the usage contexts of the reviewed TETs differ in such a way that their variety in terms of functionality impedes a systematic comparison in absolute terms. However, it is possible to compare them in terms of abstract characteristics, which are represented in the form of the taxonomy introduced in Section V.

V. CLASSIFICATION OF USABLE TETs

The term 'classification' as employed throughout this survey,[7] acts as "a representational tool used to organise a collection of information resources" [50]. According to Bradley *et al.* [51], a classification or taxonomy is a "formal system for classifying multifaceted, complex phenomena according to a set of common conceptual domains and dimensions." It serves the purpose of "increas(ing) clarity in defining and comparing complex phenomena" [51].

In the context of this survey, the classification provides a well-defined scheme against which all reviewed publications were systematically classified. The scheme discussed in this section was specifically chosen against the backdrop of patterns and themes detected in the TETs of the reviewed publications. The elicitation of these themes and the superordinate model are the result of an 'integrated approach' of systematically analysing the contents of the reviewed literature as discussed by Cruzes *et al.* [52]. Starting with an initial set of a priori dimensions retrieved from related work reviewing the literature, followed an inductive approach that iteratively

[7]Classification (noun): "Systematic arrangement in groups or categories according to established criteria." [6]

TABLE 2. Characteristics of the reviewed TETs.

Year	Publication	Stakeholders					Locality					Hosting platform				Predication					Visualisation							Intervenability		User study		
		User group		Environment		Target entity	Logging			Review						Kind of data				Specificity	Representation			Guidance		Perspective			Rectification		Pre study		
		Data subject	Auditor	Solitary	Shared	Primary	Client	Service	3rd party	Client	Service	3rd party	Handheld	Computer	Web-based	Social network	Explicit	Implicit	Derived	Predicted	Generic	Textual	Graphical	Iconified	Judgmental	Recommended	Multilayered	Multi-angled	Data flow	Erasure	Usability 1	Usability 2+
2007	Hsieh et al. [30]	●			●	○	●	●		●	●			●	●		●				●	●	●	●			●				●	●
2008	Abdullah et al. [31]	●	○	●		●	●			●								●			●		●				●				●	●
2008	Kelley et al. [32]	●			●	○	●	●			●		●	●	●		●	○			●	●		●	●							
2009	Kolter et al. [33]	●	●	○	●	●	●					●		●	●		●	●			●	○										
2009	Sadeh et al. [34]	●	○		●	○	●	●			●		●	●	●		●	○			●	●			●		●	●			●	●	●
2009	Tsai et al. [35]	●	○		●	○	●	●			●			●		●	●	○			●	●					●					●	●
2010	Kolter et al. [36]	●	○	●		●	●			●				●			●	●	●		●	●	●				●	●				●	
2010	Toch et al. [37]	●	○		●	○	●	●			●		●			●	●	○			●	●						●			●	●	●
2011	Schlegel et al. [38]	●		●		○	●			●			●				●				●	●	●	●			●					●	●
2012	Trabelsi et al. [39]	●	●	●		●	●		●		●	*	●	●			●				●	●	●					●					
2012	Kani-Zabihi et al. [25]	●		●		●	●		●		●				●		●	○			●	●	●					●	●	○	○		●	
2013	Balebako et al. [40]	●		●		●		●		●			●					●			●	●	●	●							●	●	
2013	Bilogrevic et al. [41]	●			●	○	●			●			●			●	●	○			●	●	●	●	●			●			●		
2013	Louw et al. [42]	●	○		●	●	●		●		●					●	●	●	●	○	●	●	●										
2013	Biswas et al. [43]	●		●		○		●			●		●				○	●			●	●	●	●			●	●					
2013	Zavou et al. [44]	●	●	●		●	○			●		●			●		●	●			●		●					●	●				
2014	Mun et al. [45]	●	○		●	○	●		●		●		●		●		●	○		○	●	●			●		●					●	
2015	Xu et al. [46]	●		●		●	●			●			●				○	●			●												
2015	Pistoia et al. [47]	●	○	●		●	●			●			●				●	●			●												
2015	Angulo et al. [28]	●		●	○	●	●	●		●	●			●	●		●	●	●		●	●	●				●	●	●	●	●	●	●
2016	Bier et al. [48]	●	●	●		●	●			●					●		●	●	●		●	●	●				●	●	●	●		●	
2016	Popescu et al. [26]	●	○	●		●	●		●			●		●	●	●	○	●	●		●	●					○	●		○	○	●	●
2016	Riederer et al. [49]	●	○	●		●		●				●			●		●	●	●	●	●	●		○				●					
2017	Karegar et al. [29]	●	●	●		●	●			●				●	●		●	●	●		●	●	●				●	●	●	●	●	○	●	●

revised the taxonomy to accommodate individual aspects found in the papers. Each iteration worked towards inferring increasingly generic themes that reflected the characteristics of all reviewed TETs.

The classification scheme satisfies the combined characteristics of a 'faceted analysis' and a 'paradigm' as specified by Kwasnik [53]. It suffices the principles of a faceted analysis in that it captures knowledge about a set of artifacts, i.e. the TETs, by means of independent, multi-faceted properties without requiring complete knowledge regarding the extent of the examined entities or the exact relationship of their facets. It fulfils the principles of a paradigm in that individual aspects may be unspecified or only partially applicable. However, individual aspects are not specified by the intersection of two or more attributes represented by the dimensions of a matrix, but by the attributes of a single dimension that all considered artifacts are classified against. As a result, the classification scheme serves as a model for a body of knowledge in which queries by either artifact or attribute are equally possible.

Table 2 displays the classification scheme in the form of a matrix. The horizontal axis is structured hierarchically. On the topmost level, this hierarchy consists of the high-level themes represented by the subsections of Section V. More concrete concepts are classified on the second level of the hierarchy. In some instances, the two upper levels concur conceptually, for example, for *Hosting platform* (Section V-C). In those cases, Table 2 indicates only the combined concept that spans both levels. The third level of the hierarchy constitutes concrete facets of the superordinate concepts. Each of these facets, and thus each table column, describes a conceptual property that each reviewed publication was scrutinised against. Unlike strict hierarchies and tree-like classifications, as specified by Kwasnik [53], the categories of this scheme are contextually interrelated, overlapping, and not necessarily mutually exclusive. *Judgmental statements,* for example, are classified as *Guidance* (Section V-E.2), but could also be considered a means of *Predication* (Section V-D).

The facets indicated as table entries in Table 2 specify whether and to what extent a particular property applies. An entry marked as '●' means that the respective facet applies fully, while '○' means that it applies in part. '∗' denotes that the respective publication did not provide sufficient information to be able to make a justified statement about the nature of the property. However, it is assumed from the overall context that the property applies either fully or in part. Conversely, the absence of any of the aforementioned marks signifies that the reviewers found no evidence that the property in question

applies to the respective TET. The rows in Table 2 are sorted in ascending order by the date of publication as specified in the bibliography records of the reviewed papers.

Most of the elicited characteristics that are presented below relate to the principles of usable transparency that were derived in Section II, except for those that relate to implementation details or type of evaluation of TETs. The relation of the principles of usable transparency to the facets and concepts of the classification will be discussed in more detail in the following subsections.

A. STAKEHOLDERS

This section discusses the characteristics of the various stakeholders involved in processing and reviewing a data subject's personal data.[8] It categorises the parties involved in processing that data, the environments these parties originate from, and the nature of their respective relationships that are made transparent. These characteristics relate to the legal transparency principle of providing information about data recipients or categories of recipients, as well as consequences of data processing.

1) USER GROUP

The first group of stakeholders considered in this survey is the *target user group* of a TET, that is, the kind of users that will actually use it. As this survey targets TETs for enhancing privacy, all TETs surveyed consider at least the data subjects themselves as one of its user groups. Like Hedbom [13], this survey considers data subjects and auditors as possible target groups. Likewise, this survey also draws the line between both groups on a conceptual and functional level, meaning that data subjects are likely to be non-professional users, while auditors are domain experts explicitly chosen for the task of analysing the former's data with professional scrutiny. Unlike Hedbom, this survey does not differentiate both groups on the level of 'user friendliness.' Instead, this survey seconds the design principles of interactive systems by ISO according to which any kind of software should be targeted towards the experiences and abilities of the respective target audience, and should satisfy the expectations of that group [16].

While Hedbom defines 'proxies' as entities contextually related to auditors, this group could, in theory, be treated as a separate intermediate group. Proxies could be guardians or legal representatives without technical or domain knowledge, and would therefore not qualify as members of either of the aforementioned groups. No TET could be identified that specifically targets proxies.

The TET presented by Zavou *et al.* [44] differentiates between visualisation modes for service users on the one hand and online service providers on the other. While the former can review only their own personal data, the latter receive detailed information about all service users that use their service. In that regard, the TET offers multiple perspectives (Section V-E.3) for different audiences and usage contexts, respectively. The TET presented by Pistoia *et al.* [47] depends on an intermediate proxy server whose operator might be an independent authority that concurrently acts as an auditor. The TETs presented by Bier *et al.* [48], Angulo *et al.* [28], and Riederer *et al.* [49] allow users to review their data without referring to transaction logs. Once data subjects have retrieved their personal data from the data processors, the review process could theoretically be outsourced to an independent auditor. The majority of the TETs that might be used by an auditor were generic in nature (see Section V-D.2), the complexity of the broader usage context lending itself to the in-depth knowledge of a domain expert.

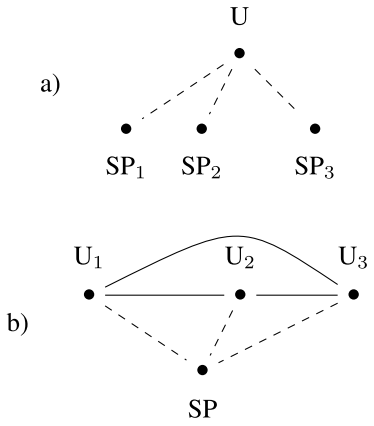


FIGURE 4. Data flows between users (U) and service providers (SP) in a) a solitary usage context and in b) a participatory network with data being shared among multiple users. Solid lines denote information shared between users, whereas dashed lines denote data traffic between users and service providers.

2) ENVIRONMENT

The second categorisation of stakeholders considered in this survey is a differentiation based on the *environment* the TETs are designed for.[9] The environmental context largely defines prerequisites and constraints for the technological and functional choices made by the designers. In a *solitary* environment, the functionality of the TET focuses on reviewing the data subject's personal data independently of other users of the same service. In such an environment, individual users do not entertain mutual relationships other than the ones to the service providers (Figure 4a). Conversely, the principal idea of online social networks and participatory communities is that participants *share* personal data in the form of certain facets of their lives among each other. In this type of social context, shared information, such as the participant's location data or her availability for appointments, is exchanged with certain other participants of the same social circle (Figure 4b). In the case of centralised services, users

[8] Stakeholder (noun): "One who is involved in or affected by a course of action." [6]

[9] Environment (noun): "(1.1) The setting or conditions in which a particular activity is carried on. (1.2) The overall structure within which a user, computer, or program operates." [8]

providing and requesting data still channel their respective queries through a central service provider in order to convey information from one user to the other.

TETs that visualise data that are disclosed with the explicit purpose of being shared among groups of people have to take into account the relationship of the members of these groups. The respective user's preferences for disclosing her data apply not only to a single service provider, but to several entities of the social context. The user of the TET may entertain different relationships to each of these entities, and might therefore maintain different privacy preferences as regards sharing her data with them.

Most TETs distinctively qualify as either personal or shared environments. In one case, the TET presented by Kolter *et al.* [33], a fraction of the functionality of the TET resides in the domain of a solitary environment, in which users maintain their relationships with various service providers. However, the primary goal of the TET presented by the researchers is to publish and distribute the insight gained from analysing the data disclosed to these providers, including reviewing target-actual discrepancy disclosed data based on privacy policies. Once published, other users are encouraged to comment on and add their personal experiences to the insight gained about the service providers, thereby creating a participatory knowledge base for the community as a whole.

3) TARGET ENTITY

The stakeholder referred to as *target entity* signifies the entity about which a TET provides information as a result of personal data being disclosed to it. In the case of a *primary* entity, that entity deals with a data controller with whom the data subject has a legal contract as regards the processing of her data. Conversely, a *secondary* entity denotes a downstream entity (see Figure 2) to whom the data controller has forwarded personal data for a specific purpose. The secondary entity might be a subsidiary or third party service provider responsible for storing and processing personal data for the data controller. In shared environments, it might also be another user of the system, that is, another data subject with whom the originator shares her data. Regardless of the identity of the recipient of the data, TETs inform users about the details regarding their personal data being disclosed to the respective entity.

Whereas Hedbom [13] distinguishes between 'organisational' and 'conglomerate' scopes of processing entities, the survey at hand does not distinguish between stakeholders based on their administrative or technical affiliation. It focuses instead on the conceptual and topological differentiation between primary entities on the one hand and secondary downstream entities on the other.

In many cases, shared environments and information about secondary entities correlate. Almost all TETs employed in usage contexts that rely on personal data being shared between multiple users and that provide information about the entity that queried that data fall into the category of providing insight into said secondary entities. The only notable exception is the TET by Kolter *et al.* [33], whose distinctive purpose aims at sharing disclosed data publicly regardless of the ultimate recipient. The TETs presented by Bier *et al.* [48], Angulo et al. [28], Kolter *et al.* [36], and Louw *et al.* [42] provide modes of visualisation specifically dedicated to displaying information about the chain of downstream processors. Such views are either hierarchical or sequential in nature, and they visualise semantic interrelations between the entities involved in processing the personal data disclosed to them.

B. LOCALITY

All ex post TETs presented in the reviewed literature were analysed as regards their operational and administrative locality,[10] and can be subdivided into three distinctive categories: (1) Local client-applications that reside in the user's immediate vicinity, (2) remote server-applications that provide a primary service through a standardised upstream protocol and (3) third parties that provide supplementary services in addition to the primary service provided by the server. In that regard, the taxonomy as regards the locality of a TET relates to Hedbom's [13] classification of trust requirements that specifies servers, clients, and third parties as distinctive sources of trust on whom users rely when they employ privacy-enhancing tools. By transposing this classification to a scenario that relies on ex post TETs, this taxonomy takes two specific sub processes into consideration, both of which can be classified independently with regard to the locality of their respective process logic.

1) LOGGING

The transaction *logging*[11] locality refers to the process that scans and collects a data subject's personal data while she is interacting with a data processor. Once disclosed personal data are being detected, the incident is logged in the form of a transaction record for later review. TETs that make use of transaction logging offer the advantage of collecting additional factual data about the circumstances under which the user's personal data are being disclosed. Such information can be used later during the review process to verify the completeness of data retrieved from a data processor. However, transaction logging comes at the price of complicating the TET by monitoring local data processing. Detecting disclosed personal data in data streams requires a significant amount of control over the respective hosting platform, and may require supervisor privileges or extended permissions in order to scrutinise outbound data traffic [30], [33], [43], [45], [47].

a: LOGGING LOCALITY

In the context of the logging locality, *client* refers to a client-side application installed on a computer or mobile device that operates in the user's immediate vicinity. Such devices

[10]Locality (noun): "The position or site of something." [8]

[11]Log (noun): "A record of performance, events, or day-to-day activities." [6]

may or may not be under the legal and technical jurisdiction of that user. Even though users may not be able to fully control or manipulate the software installed on a device, they have physical access to the hardware and may, for example, switch off the device or disconnect it from the upstream network.

Conversely, *service* denotes a remote, network-based service maintained by an online service provider. Users of such services interact with the service only by means of a well-defined UI, such as a website, or by an interface that implements remote procedure calls.

In the case that a TET is not implemented on the primary infrastructure controlled by the service provider, but is instead controlled by a *third party,* all processing of personal data is channeled through that party, while the primary service provider is responsible for the business logic of the actual service. The third party functions as an independent mediator that both the user and the primary service provider rely upon for transaction logging. The primary service provider relies on it by encapsulating the processing and storing all personal data, while data subjects rely on it to audit and review the transactions that have been conducted on their behalf.

As will be discussed in section VI-D, the logging locality may influence the user's trust in the TET.

b: DISTRIBUTED SERVICES

The logging locality of a considerable amount of TETs is distributed among more than a single stakeholder. Many client-sided TETs rely on a remote counterpart to complement local sensing or processing, or to aggregate collected information for further use in a larger context. For example, most of the location sharing TETs fall into this category. While sensing the user's environment and querying the locations of other users is handled by the local client of such TETs, all aggregation and distribution of the collected data to querying parties is taken care of by a central server.

The 'Data Track' ('GenomSynlig'), implemented for the A4Cloud EU project [28], logs all data disclosures locally. In addition, it allows users to retrieve transparency logs from remote servers that received and processed their data, and could thus also make transparent data processing along a cloud chain. However, the authors state that the visualisation of remotely logged information has so far not been fully implemented, and is only presented in form of mockups [54].

TETs that rely on third-party services are typically designed for large-scale infrastructures that satisfy the demands of a large number of stakeholders. 'PDVLoc' by Mun *et al.* [45] aims at providing a central infrastructure that allows multiple content service providers to query personal data managed by individual data subjects. Conversely, 'Cloudopsy' by Zavou *et al.* [44] implements a basic infrastructure that logs transactions of services offered by providers of value-added services. The collected 'audit trails' can be reviewed later by both the providers and the users of these services.

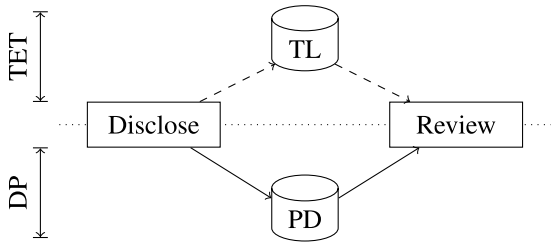


FIGURE 5. Personal data (PD) disclosed by the data subject to a data processor (DP). Personal data stored with that data processor can be retrieved in order to be reviewed. Transaction logs (TL) maintained by the TET allow for a target-actual analysis.

c: NOTIFICATION

Ex post TETs operate on personal data once they have been disclosed, that is, retrospectively. They differ conceptually in whether they detect and log disclosures themselves or rely entirely on retrieving personal data from a data controller to which they have previously been disclosed. However, some TETs of the former category also provide live feedback about the disclosure. For example, 'Labyrinth' by Pistoia *et al.* [47] displays visual overlays as soon as a possible impact on the user's privacy is detected. 'Privacy Leaks' by Balebako *et al.* [40] issues just-in-time notifications when the disclosure is detected. The textual notification is accompanied by auditory feedback and a vibration of the mobile device. The TETs presented by Schlegel *et al.* [38], Hsieh *et al.* [30], and Sadeh *et al.* [34] use customised notifiers in response to external queries to a user's current location. Trabelsi *et al.* [39] discuss email and SMS as suitable modalities to notify originators about the disclosure of their personal data.

2) REVIEW PROCESS

In the context of this survey, the *review process*[12] refers to the process of inspecting a data subject's personal data that have been disclosed to a data controller or data processor. The review locality refers to the locality of the system that hosts or enables the inspection process. Reviewing data is temporally, technically, and administratively decoupled from the preceding transaction logging process. The review process of a TET may therefore either be hosted on the same system that writes the transaction logs or on a system that differs in terms of its physical vicinity, its administrative domain, or its legal authority. If the localities of the two processes differ, the personal data disclosed earlier would have to be transferred from the logging locality to the review locality to be inspected there. Consequently, reviewing disclosed personal data is possible without transaction logs being written by a TET, in which case the review process solely relies on the data that are retrieved back from the data processor to which they were originally disclosed.

The solid lines in Figure 5 signify two subsequent, decoupled processes that (1) detect personal data that are being

[12]Review (noun): "A formal assessment of something with the intention of instituting change if necessary." [8]

disclosed to a data controller and that (2) enable data subjects to review that data. The upper half of the figure above the dotted horizontal line signifies the sphere of influence of the TET, whereas the lower half signifies the sphere of influence of the data processor. TETs that maintain transaction logs (TL) themselves can use such supplementary information to compare nominally (PD) and actually disclosed data (TL).

The platform selected to host the review process likewise falls in one of the three categories of client, server or third party, each signifying the exact same administrative domains as for the logging locality. A *client-sided* host operates in the immediate vicinity of the user and, as such, allows for direct interaction during the review process. In order to review disclosed personal data, the data must either already reside on the client system or first be downloaded from the remote host of the logging locality, e. g. by exercising the right of data portability. Intervenability regarding rectification or erasure of individual data items requires exercising the data subject's rights in the administrative domain of the data controller. Similarly, a review process hosted by a *third party* requires first transferring the collected transaction records from the logging locality host, and subsequently resubmitting any changes made to the personal data back to the entities that act as data controllers. Pre- and post-update transmissions can be omitted if the review process is provided by the primary service provider itself. Regardless of the locality of the entities involved, trust in the respective stakeholders is required, as pointed out by Hedbom [13]. In a scenario that builds its trust on ex post TETs, trust may or may not be required for more than one stakeholder, if logging locality and review process are distributed among multiple entities.

The review locality was mostly found to be limited to a single entity. Either the disclosed personal data collected by the logging locality were available on the review process because both units coincided to begin with, or the reviewing user triggers a process that transfers the necessary data from one entity to the other. Either way, the visualisation of the data then lies with a single party.

C. HOSTING PLATFORM

The *hosting platform* denotes the hardware architecture, operating system or type of service TETs are implemented for. Each category of hosting platform has specific capabilities, advantages and disadvantages. As a result, designers and developers select the platforms of their TETs according to the functional requirements of their respective usage context. In some cases, multiple localities and stakeholders are necessary to provide the functionality of a TET. For example, several reviewed TETs use the user's mobile device to collect the user's location and transfer it to a remote service. The remote service hub serves the purpose of disseminating the location to a selected set of fellow users and allows originators to review queries of their data by the actual requestors.

1) HANDHELD DEVICE

Handheld devices (not including laptops), such as mobile phones and tablets, act as personal digital assistants in the immediate vicinity of a user. Contemporary handheld devices provide their users with a variety of different modalities that can serve as sources of personal data. Sensors, such as camera, microphone and compass, allow for sensory-enriched applications in the areas of healthcare, location-based service, education or entertainment. Each modality contributes to the amalgamation of personal data that is either processed on the device itself or sent to the cloud in order to be processed there.

Six reviewed TETs were implemented for Android [38], [40], [41], [45]–[47]. Pistoia et al. [47] offer an additional implementation for iOS, while Xu et al. [46] mention porting their prototype to iOS as a possible future project. Toch *et al.* [37] implemented their prototype on Symbios OS, a popular platform at the time of publishing.

2) COMPUTER

Computer refers to computer terminals with dedicated keyboards and screen diagonals of 12 inches or larger, such as desktops or laptops. Many computers feature additional HCI peripherals that facilitate interaction with screen-based applications. Unlike handheld devices, computers are particularly suited for long-term interaction with information systems.

The TETs presented by Hsieh *et al.* [30] and Sadeh *et al.* [34] are implemented as client-side notification applications for Microsoft Windows. The client-side component of the 'PeopleFinder' location-sharing platform employed by Kelley *et al.* [32] and Sadeh *et al.* [34] runs on Windows mobile cell phones, as well as 'PC and Apple laptops' [34]. The latest stand-alone version of 'Data Track' presented by Karegar *et al.* [29], which provides transparency for exported data, is available as source code, as well as precompiled executables for Windows, macOS and GNU/Linux [55]. Conversely, the former version of Data Track, called 'GenomSynlig,' is implemented as a remote web-based service [28]. Respective source data can, for example, be exported using Google's Takeout service.[13] Kolter *et al.* [36] implemented the transaction logging and review process of their TET as a Mozilla Firefox extension and Java application, respectively. The prototype by Popescu *et al.* [26] relies on a 'browser plugin' to detect the disclosure of personal data.

3) WEB-BASED SERVICE

The term 'web-based service' comprises a plethora of rich Internet applications (RIA). While applications designed for specific architectures or platforms can run only on the operating systems and run-time environments they have been designed for, RIAs can be run and interacted with by means of a standard web browser. Since both access to the Internet as well as demands for collaborative services have been

[13] https://myaccount.google.com/intro/privacy

growing, RIAs remain a stable competitor to platform-specific apps, especially if the RIA manages to incorporate the particular usage paradigms of both traditional computers and handheld devices.

Many reviewed TETs used generic web services as a convenient means to configure user preferences and to audit disclosed data [26], [30], [44], [45], [49]. They act as web-based front-ends for a server-sided business logic residing in the back-end. The 'online interactive tool' presented by Kani-Zabihi *et al.* [25] runs entirely on a remote web server. The TETs presented by [28], [29], [31], [33], [48] are implemented as RIAs that either run as stand-alone browser apps or as front-ends that communicate with remote services.

4) ONLINE SOCIAL NETWORK

Online social networks (OSNs) signify a special kind of online service dedicated to managing personal and group relationships in the context of specific interest groups. Social networks epitomise the large scale amalgamation and distribution of personal data to either subgroups of the network or the entire public. OSNs such as Facebook and Google+ allow for implementing customised services tailored for subgroups of these networks. Such add-ons can be as broad or narrow as is required to satisfy the demands of the respective interest group. OSN add-ons can leverage vast numbers of actors and tap into social structures that represent specific categories of socio-cultural backgrounds.

The TETs presented by Bilogrevic *et al.* [41], Louw *et al.* [42], Toch *et al.* [37], and Trabelsi *et al.* [39] specifically rely on the group structures and inter-person relationships reflected by OSNs. Kolter *et al.* [33] suggest publishing insight gathered about the behaviour of a particular service provider on a wiki-based collaborative platform. Other users are encouraged to comment on and rate these records in order to allow for community-driven statements about the trustworthiness of respective service providers.

Table 3 provides a comprehensive list of the hosting platforms of the reviewed ex post TETs keyed by operating system and run-time environment.

D. PREDICATION

Predication signifies the nature of the statements made about disclosed and processed personal data.[14] The nature of a statement pertains to the circumstances under which the data were originally collected or generated, the type of data and the emphasis employed by a TET to visualise the origin and relevance of the respective type of data. Predication and the characteristics discussed below relate to the legal transparency principles of providing access to data and informing data subjects about consequences, particularly in the context of automated profiling.

[14]Predication (noun): "The logical affirmation of something about another." [6]

TABLE 3. Categories of hosting platforms.

Platform	Publications
Android	Balebako et al. [40], Bilogrevic et al. [41], Mun et al. [45], Pistoia et al. [47], Schlegel et al. [38], Xu et al. [46]
iOS	Pistoia et al. [47]
Nokia N900	Biswas et al. [43]
Symbian	Toch et al. [37]
Win. phone	Kelley et al. [32], Sadeh et al. [34]
Firefox	Abdullah et al. [31], Kolter et al. [36], Popescu et al. [26]
Java	Kolter et al. [36]
Linux	Karegar et al. [29]
macOS	Karegar et al. [29], Kelley et al. [32], Sadeh et al. [34]
Windows	Hsieh et al. [30], Karegar et al. [29], Kelley et al. [32], Sadeh et al. [34]
Web-based	Angulo et al. [28], Bier et al. [48], Hsieh et al. [30], KaniZabihi et al. [25], Kelley et al. [32], Kolter et al. [33], Mun et al. [45], Popescu et al. [26], Riederer et al. [49], Sadeh et al. [34], Zavou et al. [44]
OSN	Bilogrevic et al. [41], Louw et al. [42], Toch et al. [37], Trabelsi et al. [39]

1) KIND OF DATA

Kind of data refers to the nature and origin of the data displayed by a TET, as well as to the stance the TET takes by displaying different information. On the one hand, the underlying data can be factual and indisputable. Such data are most likely related to data wilfully and knowingly provided by a data subject. On the other hand, data can be the result of interpolation or interpretation or, in general, represent the computational outcome with the goal to infer meaningful information by correlating multiple sets of data provided by one or more data subjects. Such data are subject to uncertainty, and thus may or may not represent actual facts about a data subject. In any case, in its Recitals 39, 58 and 60, the GDPR stipulates that data controllers must inform data subjects about why and how their data are being processed [56].

a: EXPLICIT DATA

As far as different kinds of data are concerned, 'explicitly disclosed personal data' [27] refer to data wilfully and knowingly provided by a data subject, and are stored and processed by the data controller with the data subject's consent. Such data could, for example, be entered via a sign up registration form for an online service or subsequently be provided by customising a user's online profile.

b: IMPLICIT DATA

'Implicitly disclosed personal data' [27] refers to personal data that are being processed or stored by a data processor without the explicit consent of the data subject. The data subject may or may not be aware of the fact that such data are being collected. The IP address of the user's communication device or the time of an online transaction are examples of implicitly disclosed personal data. Implicit data relate to what Hedbom [13] refers to as 'extended information,' denoting data that are not legally required to warrant the respective service but that are being collected nevertheless.

Many of the reviewed TETs that deal with location-based services served the purpose of reviewing queries of the user's disclosed location or availability, and provide temporal information about when such queries were issued. These data are not treated as implicit data in Table 2 because they are related to dates of queries rather than the target person's personal data. Conversely, the user's location is considered explicitly to be disclosed data, as long as the originator knowingly uses the service to share her location in the first place. In the case of TETs that monitor the unintentional leakage of the user's location, however, such data are considered implicitly disclosed data.

c: DERIVED DATA

Derived data denotes secondary information obtained by correlating a set of personal data in a larger context, and can be based on explicitly as well as implicitly disclosed data. Selected excerpts of such data should be sent back from a data controller to a data subject once the latter exercises her right to gain access to the personal data stored about her. Examples of derived data are profiling information generated on the basis of the personal data disclosed by a data subject. Google derives data such as the speed of a traveler from location data provided by a data subject while using Google's location-based services, and upon request transfers that information back to the data subject as part of the data dump.

Both, 'Data Track' ('GenomSynlig'), the TET presented by Angulo *et al.* [28], and 'PrivacyInsight,' the TET presented by Bier *et al.* [48], display derived data, if the service provider offers the technical means to access them. 'DataBait,' the TET toolchain presented by Popescu *et al.* [26], provides transparency about the value-added assets inferred from the user's disclosed personal data according to the principle of a data licensing agreement. DataBait derives numerical value indicators from individual data items and visualises these values using a web-based GUI.

d: PREDICTED DATA

Predicted data refer to conclusions that *might be drawn* by a TET based on a set of data disclosed by the data subject.[15] They represent statements that may be made by an entity that has access to the respective set of data. Predicted data differ from derived data in that the latter are data produced by a data processor and transferred back to the data subject, whereas the former represent predictions made by the TET. Such predictions may or may not be accurate, and they may or may not be congruent with the conclusions drawn by a data processor.

The TET presented by Riederer *et al.* [49] makes predictions about hypothetical facts based on actual personal data provided by the user. Once imported, 'FindYou' predicts statements regarding the ethnography of the data subject. This kind of predication is possible by combining the personal data with public data available through the United States Census database. Louw *et al.* [42] discuss the possibility to deduct certain personal traits of an individual or group of individuals even though the respective trait was not explicitly disclosed earlier. They argue, for example, that a person's gender can be deducted from her photograph or her name, while a description of activities and events may lead to the participants' location being inferred.

[15]Predict (verb): "Foretell on the basis of observation, experience, or scientific reason." [6]

TABLE 4. Usage contexts of the TETs.

Usage context	Publications
Availability	Hsieh et al. [30]
Location	Bilogrevic et al. [41], Hsieh et al. [30], Kelley et al. [32], Mun et al. [45], Riederer et al. [49], Sadeh et al. [34], Schlegel et al. [38], Toch et al. [37], Tsai et al. [35]
Monetisation	Popescu et al. [26]
OSN properties	Louw et al. [42]
Phone permissions	Balebako et al. [40], Biswas et al. [43], Xu et al. [46]
Search queries	Abdullah et al. [31]

2) SPECIFICITY

Specificity signifies the breadth and generality of the predication made by a TET.[16] The underlying usage contexts of the reviewed TETs follow two patterns of specificity. The first category of TETs supports users in detecting and analysing disclosed personal data in a specific usage or application context. For example, a TET might have been created in the context of a location-based service to track and display queries about the users' location. In that case, the usage context is clearly defined, and respective TETs would disregard any auxiliary information not tied to the predefined scope. Such TETs were designed to handle a relatively small number of different data items and allowed for specific predications within the chosen usage context. The publications listed in Table 4 refer to TETs that were classified as serving specific usage contexts.

Conversely, TETs oriented towards the visualisation of generic personal data have not been implemented with a specific usage context in mind. Such TETs treat data as abstract information and try to visualise them in the best possible way. Auxiliary information, such as transaction logs, may or may not be available. In the latter case, the TET would have to rely entirely on the actual personal data retrieved from the data controller. The TET might still try to determine the contextual nature of individual data items and display them accordingly.

E. VISUALISATION

Visualisation of transparency information works towards the usability principles of self-descriptiveness and 'conformity with user expectations' [16], 'visibility of the system status' and 'aesthetic and minimalist design' [17], as well as comprehension and consciousness [14]. In addition, visualisation

[16]Specificity (noun): "The quality of belonging or relating uniquely to a particular subject." [8]

is a means for presenting transparency information, and thus to enforce the legal principle of informing data subjects about the implications of data processing (GDPR, Recital 58 [56]).

All reviewed publications that either explicitly discuss their data visualisation or that provide screenshots of their implementations use textual information to a certain extent. The majority of TETs also make use of graphical displays specifically suited for their respective implementation platform, use case or contextual requirements.

1) REPRESENTATION

The types and forms of on-screen representation used by the reviewed TETs to convey meaningful information about a circumstance vary widely. The diversity of the various approaches stems most likely from the different usage contexts. The choice of a particular form of representation also depends on the focus the authors set while planning and implementing their respective prototypes. Some implementations suggest a clear focus on the logging locality, that is, on the process of recognising disclosed personal data, while the review process seems to play a secondary role. In such cases, the representation of the review process can be as simple as displaying textual information.

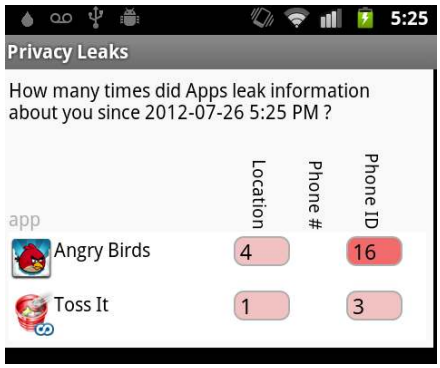
a: GRAPHICS

Graphical visualisation denotes a graphical display, such as abstract shapes or context specific symbols, either monochrome or coloured. Providing colour coding in addition to shape introduces an additional level of significance to the meaning of a representation and can, for example, induce emotional impact or subconscious connotation to the visualised facts. It can also be used to deliberately emphasise the immediate denotation conveyed by a graphical representation.

While relatively few TETs rely solely on the textual information, most TETs combine text with graphical information to visualise disclosed personal data or meta data. Colour codes are frequently used to emphasise the meaning of text and graphics [32], [34], [35], [37], [40], [45]. In most cases, the colour red is often used to signify a particularly critical state, and is either contrasted with additional colours, such as green or white, to denote respective neutral states, or continuous shades of colour ranging from the neutral to the critical state (Figure 6a). Along similar lines, in one of their design studies, Abdullah *et al.* [31] correlate the scalar values of data items to the radii of circles in a bubble chart.

Several TETs use bar graphs, either coloured or monochrome, to signify meaning associated with the properties of disclosed personal data [38], [41]. Unlike colours, which only convey the actual status as such, bar graphs allow for correlating such values to the entire range of values and might therefore be more appropriate to represent normalised numerical values. Biswas *et al.* [43] visualise quantitative values via segmented bars instead of continuous bars (Figure 6b). Riederer *et al.* [49] use pie charts to represent distinctive values as fractions of 100%. In this kind of

a)



b)

FIGURE 6. a) Colour coding by Balebako et al. [40], and b) colour-coded, segmented bar graphs by Biswas et al. [43].

representation, multi-coloured areas denote the respective contributions of various components to the whole set.

Louw *et al.* [42] and Trabelsi et al. [39] deal with scenarios that are concerned with the relationship between multiple stakeholders. The displays of their TETs connect stylised nodes by lines, thus signifying entities and their interrelations. Similarly, Zavou *et al.* [44] represent transactions between network entities by bundles of lines between the communication endpoints. In one of their display modes, Kolter *et al.* [36] use a directed line graph to signify a hierarchical structure of dependencies (Figure 7).

b: CONTEXT-SPECIFIC VISUALISATION

In many cases, the specific usage context of TETs suggests a form of graphical representation that is contextually related to the underlying functionality. Table 5 lists publications keyed by the visual representation chosen for the respective implementation. Section V-E.3 discusses TETs that employ multiple forms of representation. *Chronological* views, sometimes called timelines, display distinctive events in chronological order (Figure 11). *Data items* are singular atomic items of personal data. *Group* views comprise semantically related items, such as groups of users that are contextually related. *Hierarchical* views visualise hierarchical one-to-many relationships between superordinate and subordinate items (Figure 7). If multiple levels are displayed simultaneously, such views are sometimes referred to as 'tree views' [31]. *Home screen*

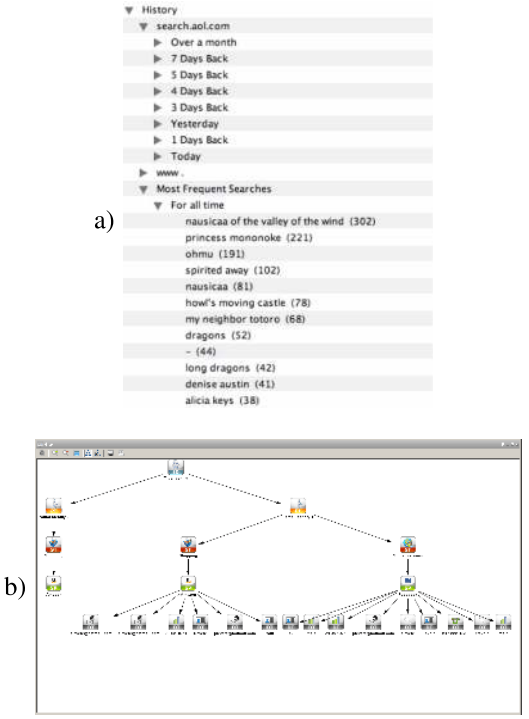


FIGURE 7. a) 'Tree view' by Abdullah et al. [31], and b) 'Graph view' by Kolter et al. [36].

TABLE 5. Types of visualisation implemented by the TETs.

Display	Publications
Chronological	Abdullah et al. [31], Karegar et al. [29], Kolter et al. [36], Sadeh et al. [34], Tsai et al. [35]
Data items	Bier et al. [48], Biswas et al. [43], Karegar et al. [29]
Group view	Hsieh et al. [30], Schlegel et al. [38]
Hierarchical	Abdullah et al. [31], Bier et al. [48], Karegar et al. [29], Kolter et al. [36], Trabelsi et al. [39]
Home screen	Schlegel et al. [38]
Map	Bilogrevic et al. [41], Biswas et al. [43], Karegar et al. [29], Kelley et al. [32], Mun et al. [45], Riederer et al. [49], Sadeh et al. [34], Toch et al. [37], Trabelsi et al. [39], Tsai et al. [35], Xu et al. [46]
Notification	Balebako et al. [40], Hsieh et al. [30], Pistoia et al. [47], Schlegel et al. [38], Sadeh et al. [34], Trabelsi et al. [39]
Service	Balebako et al. [40], Bier et al. [48], Kolter et al. [33], Kolter et al. [36]

refers to displaying data prominently on the home screen of a device. *Maps* visualise coordinates in a geographical representation (Figure 8). *Notification* denotes messages used to notify users about events at the time of the incident. *Service* refers to a view based on individual services or service providers to whom users have disclosed personal data.

For example, a considerable amount of the TETs reviewed were designed to enhance the transparency of location-based services. The majority of such TETs employ established web-based services, such as Google Maps[17] [41], [45], [49] or OpenStreetMap[18] [55]. Some TETs overlay the standard map views of these services with additional, contextually enriched

[17]https://maps.google.com/
[18]https://www.openstreetmap.org/

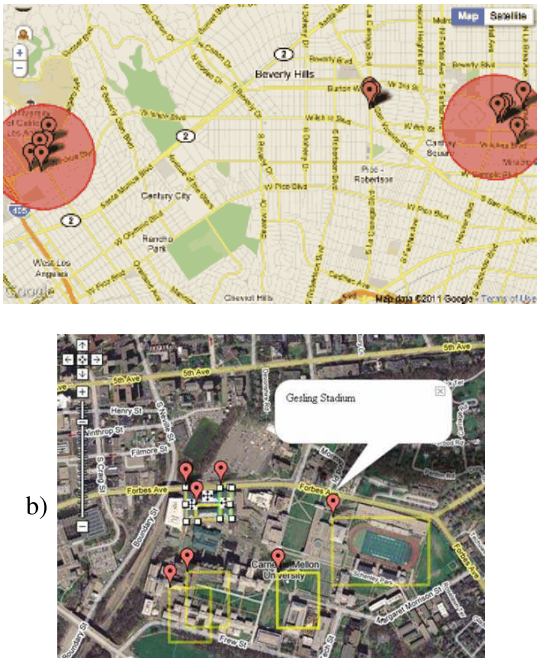


FIGURE 8. Geographical boundaries by a) Mun et al. [45], and b) Sadeh et al. [34].

information, such as blurry areas in which a particular person can be found without revealing that person's exact location. Four reviewed TETs use semi-transparent shapes to signify the respective areas of interest. Mun et al. [45] and Toch et al. [37] use circular boundaries to visualise contiguous shapes (Figure 8a), whereas Xu et al. [46] use polygonal shapes, and Sadeh et al. [34] circumscribe such areas with rectangular lines (Figure 8b). Biswas et al. [43] and Toch et al. [37] use heat maps to symbolise fuzzy areas based on geographic coordinates (Figure 9). By including coloured nuances in the visualisation, heat maps add an additional dimension to the location data, which Toch et al. [37] use to signify the entropy of individual geographic measuring points (Figure 8b).

c: ICONS

Iconified elements and pictographs count on the recognisability of graphical symbols. Once learned, icons can be used to convey codified meaning potentially quickly. A viewer recognises icons either due to her personal experience based on previous knowledge and socio-cultural imprint, or as a result of repetitive exposure to that icon in the same application context.

Ideally, icons employed by TETs would be self-descriptive and conform with the user's expectations [16]. If used infrequently, icons would still be recognised rather than recalled, ideally due to being standardised across multiple implementation platforms [17]. However, the icons discussed in the reviewed TETs are rarely universal but were found instead to be tailored to specific target audiences.

Some TETs complement their textual or graphical visualisations with icons that either stem from standard icon sets

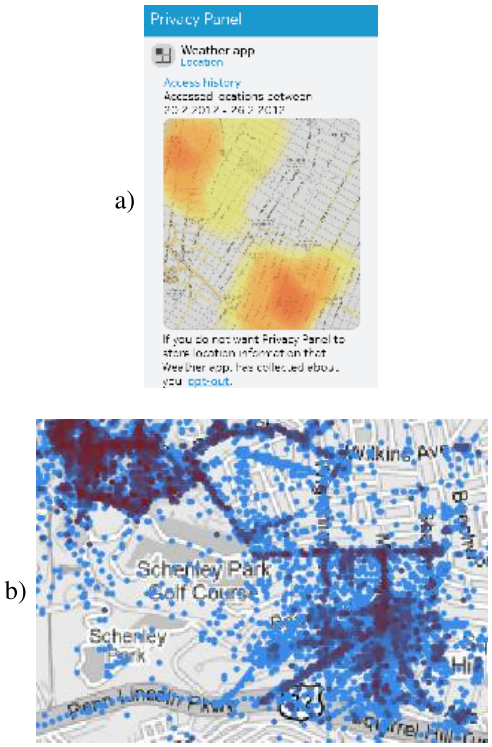


FIGURE 9. Geographical heat maps by a) Biswas et al. [43], and b) entropy densities by Toch et al. [37].

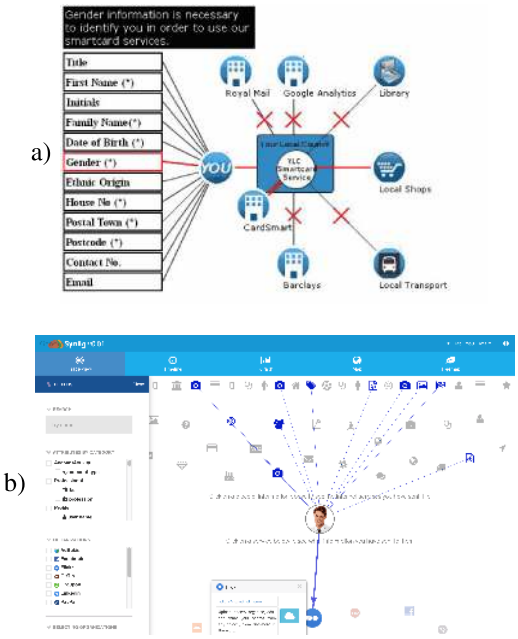


FIGURE 10. a) 'Translucence Map' by Kani-Zabihi et al. [25], and b) 'Trace view' by Fischer-Hübner et al. [27].

or are self explanatory enough to be recognisable in terms of their denotation (Figures 7 and 10). Abdullah et al. [31] use standard folder icons to represent nodes in hierarchical structures, while Bier et al. [48] and Angulo et al. [28] use pen icons to hint at the underlying functionality of editing

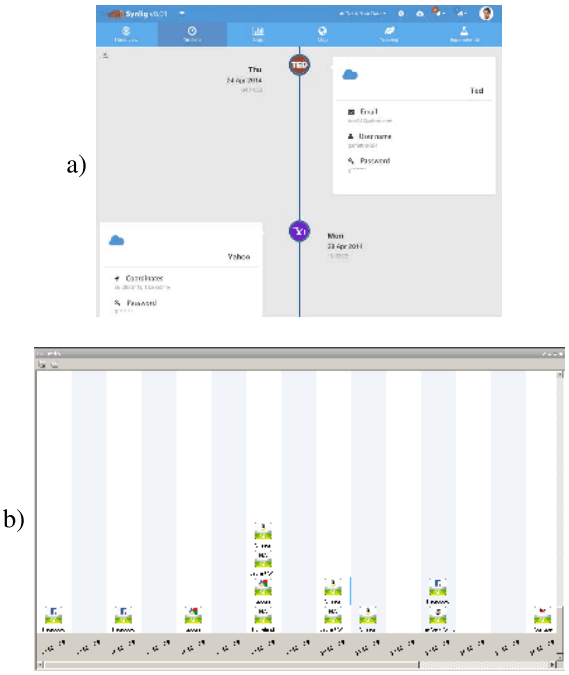


FIGURE 11. a) Chronological views by Fischer-Hübner et al. [27], and b) by Kolter et al. [36].

and modifying contents. Such icons are easily recognisable by regular users of these platforms.

Angulo et al. [28] use icons branded by online platforms to signify screen components that are related to the respective service providers, as well as individual icons for different kinds of data items. Kolter et al. [36] use highly customised icons to denote multiple entity types. Each type varies in colour and symbol, and each bears a textual acronym of its respective type, such as 'SP' for service provider, in the lower third of the icon (Figures 7 and 11). Icons that refer to online services show the branded logo of that service as an image. The primary visualisation of the TET by Schlegel et al. [38] relies on an iconic metaphor, a pair of eyes on the home screen of the device, to signify external queries regarding the user's location. Although the icon as such is unknown at first, its meaning becomes clearer by means of the icon's connotation, as well as by the dynamics of its appearance in correlation to the amount of disclosed data. The implementation of Hsieh et al. [30] makes use of a client-sided application that is used to receive local notifications. The colour of its run-time icon changes in response to the query status.

2) GUIDANCE

Guidance[19] on the part of a TET goes beyond matter-of-factly visualising details about disclosed personal data. TETs that guide users take deliberate stances as far as the extent of disclosed personal data is concerned. Such TETs may guide the user towards obtaining better awareness of a particular

[19]Guidance (noun): "Advice or information aimed at resolving a problem or difficulty, especially as given by someone in authority." [8]

circumstance, or even nudge her to take action due to certain disclosed data being considered detrimental or critical. Ultimately, guidance on the part of a TET implements the transparency principle of notification and, if necessary, encourages change in terms of reconsidering the user's previous decisions.

a: JUDGMENTAL STATEMENT

Some TETs take a judgmental stance in terms of displaying information. Such visualisations aim to hint at consequences that might arise for a data subject who disclosed her data. Respective implementations rely on thresholds that, once exceeded or fallen short of, result in changing the characteristics of the visualisation. For example, some TETs rely on a change of colour, size or shape of the visualisation to signify the level of impact of the disclosure on the user's privacy (Section V-E.1). Depending on the effect the designers of the TET intended to induce in the user, such alterations reside in the continuous range between subliminal and eye-catching.

Changes of characteristics can be used to indicate the severity of the circumstances more clearly, or even to nudge a user towards action. By making judgmental statements, such tools may, for example, stimulate a certain behaviour in the user, which may not be achievable by solely relying on neutral facts. However, a judgmental view is not mutually exclusive to a neutral stance. In fact, TETs that assume both stances by providing both types of data might satisfy scrutinising users better than the ones that provide just a singular view.

On the one hand, judgement or attempts to nudge a user into acting or reacting in a certain way might aid inexperienced users in getting a clearer picture of the privacy issues underlying their online activities. For example, the TET presented by Balebako et al. [40] changes the colour of their display, if the total amount of disclosures of a trait exceeds a certain threshold (Figure 6a), while Hsieh et al. [30] use a change of colour of the taskbar icon to indicate the fact that the user's personal data have been queried.

On the other hand, judgement on the part of an algorithm might be misleading in that it does not necessarily reflect the actual view of a particular user, let alone all possible users. Different users have different conceptions as regards the severity of disclosing particular data items, and many algorithms will not be able to satisfyingly take each user's preferences into account. The algorithm that determines whether the disclosure is acceptable, marginal or critical in a specific scenario is often not transparent to users, nor are the hardcoded settings of respective threshold values (Figure 6b). Many TETs reviewed do not seem to allow users to customise these values in order to accommodate their individual requirements for particular types of data. The TET presented by Biswas et al. [43] allows users to set individual ratings for the monitored modalities that serve as thresholds for judgmental statements made by the TET. A few other TETs handle individualisation by employing machine learning to learn the user's preferences by analysing the decisions she made in past [32], [34], [41]. Some of these implementations predict contextually related future decisions with high accuracy, or even allow trained classifiers to make decisions autonomously. Decisions made in lieu of a user of such TETs can be reviewed at any time. However, the fundamental functionality of automated decision-making processes may not be transparent to the majority of users.

b: RECOMMENDATION

Recommendations[20] relate to judgmental statements in so far as that they point out a state that is considered suboptimal in the respective usage context. Like judgmental statements, a recommendation might employ graphical means to coax users into action. Unlike judgmental statements, however, a recommendation goes further in that it more explicitly gives advice about the necessity of a change, or even offers a concrete substitute for the present state. Recommendations facilitate the user's decision-making process by offering favourable options, thus mitigating the necessary user's cognitive load for making rational decisions on her own. They work towards what is considered optimal in the respective usage context by aiding users in reaching that state.

Whereas ex ante TETs aim at guiding users in making beneficial decisions before they disclose their personal data, ex post TETs take these data into account and guide users towards adapting their previous decisions. Recommender systems scrutinise the user's privacy settings[21] in terms of improvability. The nominal value considered optimal by a recommender system may vary. The system might target the equivalent of a social norm, considering the decisions of a certain subset of users, such as a user's trusted friends, as convergence points. It might also consider individual users by trying to analyse the patterns of their previous decisions, and then try to detect outliers that deviate from these patterns.

In the context of privacy, unintentional deviations might be considered errors. Thus, a TET that aids users in recognising, diagnosing and recovering from errors would improve usability [17]. Recommendation builds upon the principles of consciousness, control and consent [14]. By recognising and pointing out the necessity for a change, a TET raises the user's awareness, at the same time providing her with an immediate means to make the change. Besides enabling control, the act of notification incorporates the user's consent into the decision-making process.

Recommendation is related to intervenability (Section V-F) in that it supports a user's decision-making process, which might eventually entail the rectification of her personal data. However, it is not tied to exercising the legal right of rectification or erasure as such (Sections I and II), but to facilitating an improvement of the user's choices as regards disclosing her personal data.

[20]Recommendation (noun): "A suggestion or proposal as to the best course of action, especially one put forward by an authoritative body." [8]

[21]Most publications reviewed either use the term 'privacy settings' or 'privacy policies,' denoting the settings that specify what, when and to whom personal data are disclosed.

The TET presented by Kelley at al. [32] is built on the concept of 'user-controllable policy learning,' a cooperative approach between the user and the policy management system. Based on the user's settings, the system makes automated decisions in lieu of an originator as regards disclosing or not disclosing that user's data to querying third parties. By reviewing and commenting on the choices made by the system, as well as by making changes to their settings, users help to train future decisions of the system, ultimately optimising the user's settings by applying incremental updates. Similarly, the TET presented by Mun et al. [45] is based on an architecture that implements a 'personal data vault.' The TET provides users with an active 'rule recommender' that suggests changes to the users' privacy settings. The tool visualises possible risks based on the user's settings, thus helping her find her optimal settings that best support utility and privacy. The recommender system of the TET presented by Sadeh et al. [34] specifically aids users in refining their privacy settings by providing them with meaningful suggestions for changes. Conversely, 'SPISM,' the TET presented by Bilogrevic et al. [41], assessed the nominal values as regards a user's sharing behaviour by means of an extensive online survey, which the authors use to measure the accuracy of the automated decision-making of their TET.

3) PERSPECTIVE

The reviewed TETs vary in terms of multi-facetted visualisation. Some TETs rely on a single form of visualisation, whereas others combine several perspectives or multiple levels of detail. Such flexibility lends itself to scrutinising disclosed data under different angles and may allow for richer insight into the exact circumstances under which personal data were disclosed.

a: MULTILAYERED

Multilayered visualisations display information in multiple levels of detail.[22] Multilayered designs usually start with an overview of generic, coarse-grained information. To be as clearly readable and as quickly digestible as possible, such data are often kept to a bare minimum. Buttons, hyperlinks or icons reveal secondary, more detailed information about the respective data item. Multilayered displays often implement a hierarchical, top-down navigation paradigm. Some visualisations support cross-references between multiple views, allowing for a sequential or contextual traversal of the available data.

Mun et al. [45] display location sample points on a map where each additional contextual detail can be displayed. Tsai et al. [35] display a 'show details'-button along with reviewed log records. Sadeh et al. [34] provide similar functionality complemented by a real-time notification that offers general and detailed information about queries regarding the user's location. The implementations presented by Bier et al. [48] and Angulo et al. [28] work similarly in how they visualise disclosed personal data. Both provide an initial overview that shows the relationships of data subjects with whom the stakeholders they share personal data. Upon request, both TETs provide detailed information on individual data controllers, as well as on the individual data items that have been disclosed to these stakeholders.

TABLE 6. Overview of multi-perspective TETs.

Publication	Perspectives
Abdullah et al. [31]	Histogram over time, bubble chart, hierarchical view, Seesoft view
Kolter et al. [36]	Service-providers, chronological, hierarchical ('graph view')
Biswas et al. [43]	List of apps disclosing data, details about individual data items, details about access to location, contacts, and file system
Hsieh et al. [30]	Notification, disclosure history, summary of data processors
Fischer-Hübner et al. [27]	Connections between data processors and data items ('trace view,' Figure 10b), map view, chronological event log ('timeline view,' Figure 11a)
Trabelsi et al. [39]	Hierarchical access control graph, hierarchical view about distribution of data
Schlegel et al. [38]	Metaphoric home screen, access details grouped by customisable groups of users.
Xu et al. [46]	Customised audio, camera, and map views

b: MULTI-ANGLED

Multi-angled visualisations provide multiple views in order to display different angles of the same underlying data set.[23] Unlike multilayered visualisation, multi-perspective visualisation is not necessarily arranged in a hierarchical top-down order but provides multiple perspectives of the same basic phenomenon. Each of these views represents a self-reliant visualisation in its own right. A perspective might, for example, comprise a sub set of data associated with a specific partial aspect of a data item, such as a compound view of certain decoupled modalities that collectively bear a contextual meaning. It might represent a particular data type and choose a form of representation that meaningfully visualises the respective properties of that type. A multi-angled visualisation might also literally represent the vantage points of multiple stakeholders involved in the scenario, such as the views of multiple data processors on a data subject's personal data.

For example, a map view is suitable for visualising geographic coordinates, whereas a timeline might be more appropriate for displaying these coordinates in temporal order. The TET presented by Karegar et al. [29] visualises geographical measurement points as time stamps of events on a chronological time line. Alternatively, it displays these geographical locations as the vertices of a directed graph on a map view. Table 6 lists exemplary publications along with the perspectives they employ.

[22]Multilayered (adjective): "Having or involving several distinct layers, strata, or levels." [6]

[23]Multi-angled (adjective): "Involving a view or approach from several angles." [8]

c: DATA FLOWS

In cases where multiple stakeholders exchange or disseminate a data subject's personal data, such micro transactions are treated as data flows between these entities. Data flows can result from immediate action on the part of a data subject, such as submitting a web form. They could also be triggered by querying a downstream processor for the subject's personal data controlled by a primary data controller. In the latter case, the data subject did not trigger the data flow proactively, but instead acts as a query target of a third party. TETs that visualise data flows need to take into consideration not only processes performed by an individual data controller but must also retrieve necessary information from respective downstream processors.

In this classification scheme, data flows are treated as a visualisation technique because they provide practical insight into the path that a particular data item has taken over time. From a user's point of view, they therefore allow for an additional perspective where personal data stored and controlled by a stakeholder can be scrutinised. That is not to say that data flows could not also be classified as a type of predication (Section V-D).

The TETs presented by Bier et al. [48] and Zavou et al. [44] visualise data flows between multiple stakeholders. Zavou et al. [44] call their review process 'audit trails' and represent data flows quantitatively on a schematic map using distinctive lines between network entities. The architecture described in the paper relies on a central authority that maintains the centralised infrastructure necessary to log the data flows between respective entities, which, in turn, provide services for end users. Kani-Zabihi et al. [25] visualise flows of personal data on a conceptual level by interactively highlighting the communication channels between entities that exchanged the data subject's personal data (Figure 10, left). The TET of Bier et al. [48] allows for pursuing individual data items between and along the chain of downstream processors involved in processing them.

F. SUPPORT FOR INTERVENABILITY

Intervenability denotes a data subject's legal right to rectify and erase her personal data as stipulated by the GDPR, Art. 16 et seq. [56]. Transparency is a prerequisite for intervenability. Even though intervenability as a subsequent step goes beyond transparency, the legal transparency principle pursuant to the GDPR not only informs data subjects about their intervenability rights, but also makes them aware of how to exercise them. One way of making users aware of their intervenability rights is to support them in exercising those rights with regard to their data when those data are being made transparent. In that way, the context of exercising their rights may be comprehensible to them. To facilitate the process of intervention, TETs may tap directly into an automated functionality maintained by a data controller, provided such means exist.

Intervenability relates to an 'interactive' means of control and verification in Hedbom's survey [13], which also states that interactive control goes beyond 'read-only' access to disclosed personal data in that it allows data subjects or their proxies to "actively influence the stored data." It relates to the HCI principles of being able to exercise control [14]–[17] over the process that involves storing and processing the data subject's personal data, as well as providing the means necessary for maintaining or revoking consent given previously [14].

'PrivacyInsight' by Bier et al. [48] enables data subjects to exercise their legal rights as regards rectification and erasure of personal data. 'Data Track' ('GenomSynlig') [28] offers similar functionality, enabling data subjects to rectify and erase individual data items stored in the cloud. Both publications discuss and explicitly build upon the stipulations of the GDPR [56], and, in theory, provide the technical means necessary to exercise the data subject's rights. Kani-Zabihi et al. [25] introduce 'Privacy Enquiry,' effectively an online chat, as a featured communication channel to the data controller. The primary purpose of the chat is to promptly express privacy concerns. It is left open as to whether this medium could also be used to issue a request to rectify or erase disclosed personal data.

In the classification scheme of this survey, the adaptation of a user's privacy policies in terms of modifying the access control used to validate queries for the data subject's personal data by third parties is not considered an act of rectification. In particular, data disseminated throughout shared environments (Section V-A.2) can not be revoked that way. An adaptation of a user's preferences represents a purely technical operation that affects future queries of the user's personal data rather than being a legal process that entails the exertion of personal rights.

G. USER STUDIES

Some of the reviewed TETs are either the result of, or tested by the means of user studies that have been conducted before, during or after the implementation of the presented prototypes. The classification distinguishes between pre studies and usability tests.

Pre studies are conducted before or during the implementation phase. Their purpose is to better understand the previous knowledge, preferences and expectations of the intended target audience. A pre study plays an essential role in the elicitation of requirements during the conception of HCI systems. In the case that evaluation of a designed prototype does not meet the specified requirements, the study phase may be revisited, resulting in another iteration of the development life cycle [57].

Conversely, *usability tests* evaluate the effectiveness, efficiency and satisfaction on the part of the intended audience as regards performing the task for which the TET was designed [15]. Depending on the exact purpose of the TET, usability tests of implementations may be conducted during or after the implementation phase. Usability tests of mockups

may precede the actual implementation in order to detect conceptional or design flaws even before the first prototypical implementation. The classification distinguishes between a single test ('Usability 1') and two or more test iterations ('Usability 2+') to emphasise the fact that the designers of some TETs attached particular importance to testing the usability of their implementation.

1) EFFECTIVENESS AND EFFICIENCY

Stipulated ISO usability principles of effectiveness[24] and efficiency[25] [15] seek to provide conclusive measures of the usability of interaction systems. ISO 16982 [58] specifies various methods for assessing the usability of HCI systems. Methods such as observation, performance measurements, questionnaires and interviews can either be used solely or jointly to assess whether and to what extend an interactive system is actually usable by the respective user group. They allow for qualitative as well as quantitative analysis of the artifacts evaluated.

Individualisation [16] of TETs is considered desirable, the actual extent of its applicability and ultimate benefit for the user depending largely on the type and complexity of the application. Flexibility in terms of individualising the workflow associated with completing a task might lead to improved effectiveness and efficiency by adapting to the user's actual requirements and level of expertise.

Following a qualitative evaluation approach, Abdullah et al. [31] state that the participants of the user study felt that the TET effectively achieved its intended goal. In contrast, Schlegel et al. [38] rely on a game-based approach to elicit the effectiveness of their notification mechanism and UI quantitatively. The authors state that the TET proved to inform the participants of their user study effectively and meaningfully, and argue that their approach is easier to use than TETs that rely on the retrospective analysis of access logs. Bier et al. [48] use questionnaires in the form of a System Usability Scale and a User Experience Questionnaire. The authors provide numerical and graphical representations of their results that reflect the usability of their TET in terms of various aspects covered by the questionnaires. The user study conducted by Bilogrevic et al. [41] relies on customised questionnaires, some of whose follow-up questions depend on answers given previously. The authors present and discuss the results in numerical and graphical form, and relate it to the capabilities of semi-automatic decision-making on part of their machine learning algorithm. Mun et al. [45] evaluated the effectiveness of the policy recommender of their TET by monitoring the number of participants in their user study that adapted their settings after being notified by the tool. They observed that the number of users who changed their settings after being notified declined over time and concluded that their recommendations effectively helped them to establish settings that met their personal requirements.

2) COMPREHENSIBILITY

Comprehensibility[26] issues may arise due to the violation of one or more design principles for usable software, such as 'suitability for the task,' 'self-descriptiveness' and the 'conformity with the expectations of the users' [16]. Such discrepancies relate to a lack of comprehension and consciousness on the part of the user [14], mitigating her ability to correctly interpret the system status or to aptly exercise control in order to change that status as a result of a rational decision [14], [16]. The availability of 'help and documentation' [17] is desirable; however, it would ideally not be necessary for TETs that are truly self-descriptive. A deviation of the user's mental model from the functionality provided by a TET can be detected via user evaluations. However, only some of the surveyed papers include evaluation results about the users' ability to comprehend the data processing and data flows visualised by the evaluated TET.

In the user study conducted by Kolter et al. [36], participants stated that they found the user control of the TET 'intuitive' and that all information was clearly presented. Likewise, most test subjects of the user study conducted by Hsieh et al. [30] stated that they found the TET 'intuitive' and 'easy to use.' However, some users stated the flexibility of the UI comes at the price of a tedious bootstrapping process. Some test subjects in the user study conducted by Mun et al. [45] stated that they appreciated the functionality of the TET but would have preferred an UI that is more intuitive.

The study conducted by Balebako et al. [40] indicates that users have difficulty distinguishing between technical terms that the designers of the TET had taken for granted. Users mentioned, for example, that the difference between the 'phone number' and 'phone ID' of a mobile phone is not self-explanatory.

Evaluations of 'Data Track' ('GenomSynlig') by Angulo et al. [28] revealed that test subjects had difficulty differentiating the client site, where data disclosures were logged locally, from the service side assessable via the UI in exercising their data subject rights to access and intervenability. These results confirmed results gained via previous usability studies that revealed that the users' mental models of data flows between client and services sites and of Internet data flows often do not match with the real world [59], thus conflicting with the usability principle 'match between system and the real world' [17].

3) AWARENESS

Multiple user studies evaluate the change of awareness of users regarding their personal data being disclosed.[27]

[24] Effective (adjective): "Successful in producing a desired or intended result." [8]

[25] Efficient (adjective): "Preventing the wasteful use of a particular resource." [8]

[26] Comprehensible (adjective): "Able to be understood; intelligible." [8]

[27] Awareness (noun): "Concern about and well-informed interest in a particular situation or development." [8]

Awareness relates to 'self-descriptiveness' and the 'conformity with the user's expectations' [16], as well as the 'visibility of the system status,' and the 'match between the system and the real world' [17]. It is also key for the user's comprehension and consciousness [14].

To verify the impact on the test subjects' awareness, Hsieh et al. [30] deliberately introduced an irregular event during their field study. After the field study, they combined interviews with surveys and questionnaires to assess the usability of their TET. The authors state that, after becoming more familiar and comfortable with the TET, the users' awareness about which data had been disclosed to whom increased between the first and second iterations of their study.

The participants of the user study conducted by Balebako et al. [40] state that the evaluated TET helped them develop a better understanding of the fact that apps installed on mobile devices leaked personal data. Abdullah et al. [31] state that visualising the search terms that users used in the past raised these users' overall awareness about the traces they left on the Internet. Sadeh et al. [34] conclude that an increase in the test subjects' context awareness leads to privacy settings that more accurately reflect these users' actual preferences.

4) FEEDBACK

The 'visibility of the system status' as a core usability heuristic [17] merits particular attention. The availability of meaningful information about the status of a system is a necessary condition for rational decision-making on the part of a user. Without feedback[28] from a TET, a user might be unable to assess the current status of her personal data [14]. Consequently, such a user might be unable to make a rational decision as to how to interact with and exercise control over the TET.

Multiple user studies examine the impact of system feedback on the users of a TET. The findings of Schlegel et al. [38] show that system feedback makes users more comfortable in sharing their location data. Along similar lines, Tsai et al. [35] state that the users' level of comfort in terms of sharing their location data differs depending on whether they receive meaningful feedback from the system about the queriers of their data. In contrast to a control group that had not received feedback, test subjects who had received system feedback were more comfortable sharing their location.

The user study conducted by Hsieh et al. [30] shows that users particularly value immediate system feedback on queries to their location, and also appreciate the ability to audit disclosed personal data in general. Mun et al. [45] write that their user study shows that users appreciated system feedback in that it helped them to better understand whether their respective settings matched their actual preferences, as well as what kind of data were actually disclosed to whom. Kani-Zabihi et al. [25] concede that the online chat implemented for their TET proved to be the least favourable of the feedback controls evaluated. According to the test subjects, chat as a medium was considered inappropriate in terms of serving as a means to convey privacy concerns to a data controller.

5) AESTHETICS

Of the usability heuristics, aesthetics[29] and the look and feel of an UI play important roles in working towards a satisfying user experience.

The user study conducted by Abdullah et al. [31] shows that participants preferred visual designs that are 'user friendly' and 'well organised,' exemplifying the principle of 'aesthetic and minimalist design' [17]. The test persons favoured a traditional hierarchical design over aesthetically pleasing but unusual forms of visualisation, such as bubble charts, exemplifying a preference for 'consistency and standards,' as well as 'recognition rather than recall' [17]. The reiterated user study of a Firefox plug-in implemented according to the findings of the first study in the form of a 'file tree view' confirmed the usability of the evaluated TET.

6) SATISFACTION

An ISO usability principle, satisfaction,[30] denotes personal comfort and encouragement, as well as the perceived usefulness of an application. A user experience that is entirely satisfying has the potential to entail an extended use of an application.

The interviews conducted by Kolter et al. [36] with test persons that evaluated the usability of their TET showed that they ''understood and valued the advantages'' of the tool. The participants of the user study conducted by Abdullah et al. [31] attested to the usefulness of the browser extension that was developed, but some questioned its usefulness in a home environment. Most participants in the user study conducted by Balebako et al. [40] found the TET useful and would like to install it, or a similar app, on a mobile device. Likewise, the participants in the user studies conducted by Mun et al. [45] and Toch et al. [37] stated that the respective TET represented a useful tool for managing their data and were willing to use it in the future. Toch et al. report that about one third of the test subjects actually used the tool one month after the study had finished. The usability tests conducted for 'Data Track' ('GenomSynlig') showed that the majority of test users considered Data Track to be a potentially useful tool, appreciated its transparency options, and would use it on a regular basis. Hence, the perceived usefulness of ex post TETs seems to be high, which has been confirmed by the reported evaluation results in the surveyed publications.

[28] Feedback (noun): ''The modification or control of a process or system by its results or effects'' [8]

[29] Aesthetic (adjective): ''responsive to or appreciative of what is pleasurable to the senses'' [6]

[30] Satisfaction (noun): ''a source or means of enjoyment'' [6]

VI. DISCUSSION

A. MATURITY

From what can be assessed from the publications themselves, the maturity of the TETs reviewed seems to vary. Kani-Zabihi *et al.* [25] explicitly point out the prototypical state of their TET. Popescu *et al.* [26] conducted their user studies using mockups and refer the reader to the future implementation of the actual tool. The functionality of some TETs, such as [39], [42], [44], [47], were not described with technical specifications, such as the hosting platforms of the TETs. No user studies or usability tests were conducted to evaluate these implementations. It remains unclear whether the TETs described actually exist in the form of a prototypical implementation. In some cases, it remains unclear whether the graphics depicted in the respective publication represent actual UIs of prototypical implementations or preliminary mockups. Consequently, the actual usability of such TETs, that is, their suitability for their designated task [16] could not be assessed.

Conversely, a considerable amount of the reviewed TETs were available in their second development cycle, and their authors reported that the prototypes had been evaluated and improved in each iteration. Usability tests conducted during and after each cycle underpinned not only their actual usability, but in some instances also satisfaction on the part of the test subjects.

B. TRENDS

In the course of this survey, location-based services could be identified as the one scenario that was discussed by far by the most publications. sixteen publications [29], [30], [32], [34], [35], [37], [38], [40]–[43], [45]–[47], [49] explicitly refer to location data as personal data that can be reviewed using their TET, while seven [32], [34], [35], [37], [38], [41], [45] treat the user's location as the primary personal asset on which their respective usage context is focused. Eleven TETs that were reviewed rely on map-based visualisation of geographic data (Table 5). The fact that much research has been conducted in this area seems to underscore the significance of more transparency of location-based services.

While cloud computing is at least the scope of application for some TETs, such as the one presented by Angulo *et al.* [28], the area of Internet of Things (IoT) is not specifically addressed by the reviewed TETs. As the privacy principle of transparency is also at stake in smart environments, TETs for IoT scenarios will be an area that is in need of further research and development in the future.

C. GAPS

The aspects discussed throughout this section are specifically related to shortcomings observed in the reviewed TETs as regards deviations from the principles for transparency and usability, as specified in Sections I and II. These shortcomings also point out areas where further research on TETs will be needed in the future.

1) SELF-DESCRIPTIVENESS

The prototypes of many TETs seemed either moderately abstract or focused on a specific usage context. The ones that leant towards abstract contexts, such as large-scale infrastructures based on central authorities [39], [42], [44], [47], were often not discussed in terms of their actual usability. The question of whether TETs that reflect such highly abstract scenarios were self-descriptive enough and in accordance with the expectations of their respective users [16] in order to be actually usable remained unanswered.

2) TRANSPARENCY AND CONTROL OF JUDGMENTAL STATEMENTS

Some TETs that operate in a data sharing environment (Section V-A.2) allow users to customise their privacy settings in terms of deciding which party has access to their data. In this respect, they are suitable for individualisation as regards the users' preferences [16]. However, some TETs that make judgmental statements about the users' personal data (Section V-D.1) do so without the user knowing the grounds on which these judgments were made. Consequently, respective functionality leans towards 'invisibility' as far as the transparency of the underlying process is concerned (Section I). In contrast to ex ante TETs, many ex post TETs do not allow users to set their own preferences for individual thresholds of such statements. However, being able to customise these thresholds might be desirable when targeting different target audiences.

3) SUITABILITY FOR INDIVIDUALISATION

Some TETs lack a combination of multilayered, multi-perspective forms of visualisation that provide both general and highly specific information about disclosed personal data. Combining both might not only enable users with different levels of knowledge, but also different roles and backgrounds, to more meaningfully and satisfyingly review the personal data they disclosed to a data controller. By lacking respective versatility, such TETs do not seem to satisfy the 'conformity with user expectations' [16] and 'flexibility and efficiency of use' [17] expected by the various representatives of the target audiences. Generally speaking, not adapting to the user's mental model can be considered a lack of 'suitability for individualisation and learning' [16].

4) ERROR PREVENTION

Configuring privacy settings in shared environments (Section V-A.2) typically entails tedious decision-making processes on the part of users due to the potentially large number of stakeholders involved. The diversity of the groups of users involved and the various levels of trust required to express a data subject's relationship with them demands an equally high cognitive load in terms of customising respective privacy settings. It is noticeable that the recommender systems discussed in Section V-E.1 were exclusively implemented for shared environments, underscoring the fact that

users of such systems know that they are disclosing certain personal data in the first place. In that regard, respective TETs are specifically designed to aid users in optimising their sharing behaviour.

However, active recommendation is also imaginable for TETs designed for solitary environments. Respective functionality might not only hint at inadequacies detected in a user's settings but also provide an immediate, context-related means to facilitate changes that lead to more favourable privacy settings for users. By doing so, these TETs would aid users to better recognise and recover from errors regarding the disclosure of their personal data [17].

5) SUPPORT INTERVENABILITY

While intervenability goes beyond transparency, TETs should create awareness and guidance for data subjects in terms of exercising their rights for intervenability. As discussed earlier, this can be achieved if online access functions for exercising data subject rights are provided, enabling users of TETs that leverage such functionality to review their data and related information. However, only a few TETs that are currently available provide access to respective functionality. It may turn out that one of the greatest challenges will be the development of and agreement on technical standards for the implementation of the functionality necessary to issue legitimate change and deletion requests on behalf of data subjects.

6) STANDARDISED ICONS

Similarly, there are currently no recommended standard sets of icons available to aid developers in designing meaningful UIs that build upon the principles of 'self-descriptiveness' and 'conformity with user expectations' [16], as well as 'consistency and standards' and 'recognition rather than recall' [17]. Conversely, the GDPR mentions that ex ante transparency information may be accompanied by standardised icons, which should be machine-readable.

Icons are also used in many ex post TETs, for example for displaying data types, purposes of processing or data recipients. Such pictographs should be intuitive and, for reasons of consistency, be the same as in ex ante TETs. Hence, the standardisation of meaningful policy icons will also be important for ex post TETs.

Research conducted in this area [60]–[62] has also mostly focused on ex ante scenarios, exploring alternative ways to inform users about the privacy policies of online services while minimising the cognitive load required to comprehend their meanings. Many of the design proposals discussed failed to reflect the complexity of real-world scenarios. Even if individual prototypical designs were pointed out as promising, there has been no successful standardisation yet of recommended policy icons and of protocols for making them machine-readable. They are therefore far from being universally applicable to ex post scenarios.

7) DATA BREACH NOTIFICATION

Most reviewed TETs are not designed for supporting and advising on data breach notification (GDPR, Art. 4 (12) [56]). Pertaining to the TET presented by Angulo *et al.* [28], respective functionality was conceptually discussed in [63]. However, support for data breach notification and automated advice on subsequent actions has not been implemented in the final TET. As the client-sided module of the TET logs all disclosed personal data, it has additional contextual information at its disposal for advising of data breaches. If, for example, it receives a notification about a compromised password database that contains the user's password, it might advise the user about other organisations for which the same credentials are being used, and that therefore should be changed. Research on users' expectations about the type of guidance they would like to obtain in the case of data breaches was conducted by Angulo *et al.* [64].

By recognising respective incidents, guidance on parts of a TET would improve the users privacy and would implement the usability principle of error prevention [16], [17]. With the upcoming requirements of data breach notifications (GDPR, Art. 33 et seq. [56]), further research on extensions of TETs for issuing data breach notifications in a usable manner will be important.

8) SUPPORT ACCOUNTABILITY

Ex post transparency and data breach notification are important prerequisites for enforcing the accountability of data controllers. The reviewed ex post TETs are not designed to provide 'hard' proof that support data subjects in making data controllers accountable for illegitimate data processing operations. In that regard, future research could address techniques, such as verifiable computing, that can be used to achieve transparency with accountability support. The latter technique provides proof of whether computations of certain authorised functions were carried out correctly.

D. AWARENESS AND TRUST

Some user studies conducted in the publications reviewed in this survey indicate that, in general, test persons appreciate the service of the TETs, most notably because they allowed for an increased level of awareness of the circumstances under which their personal data were disclosed. On these grounds, TETs have achieved the goal of improving the transparency of the underlying process. Conversely, Balebako *et al.* [40] state that average users ''lack any consumer education'' and tend to be mostly unaware of the potential risks that arise from using technology that will or might disclose their personal data. On the one hand, this discrepancy between desired and actual awareness on the part of users encourages further research on TETs. On the other hand, it gives rise to the question as regards the general decisiveness of statements made by test persons who evaluate processes about which they may have little actual knowledge.

Kani-Zabihi *et al.* [25] state that the majority of their test subjects (68%) considered the service provider of the TET trustworthy, whereas the rest either disagreed or were indifferent. Trabelsi *et al.* [39] and Zavou *et al.* [44] discuss the aspect of trust with regard to a remote entity, such as an online service provider. They describe TETs as potential enabler technologies that make transactions more transparent. The architecture designs presented by [45], [38], and [44] rely on a central trusted authority that either controls or stores personal data, and whose purpose is to protect the data from unauthorised access by potentially untrusted parties. In these scenarios, data subjects would have to trust a single centralised entity with a superset of their personal data that they may want to share with other parties.

Xu *et al.* [46] describe a model of trust based on the various components of the system architecture on top of which their TET is built. [31], [30], [38], and [45] rely on the assumption that the TET as such is trustworthy. However, only Balebako *et al.* [40] and Kani-Zabihi *et al.* [25] explicitly address the aspect of trust with regard to the test subjects' perception of their evaluated TETs, that is, whether and why such users would trust a TET, while at the same time scrutinising the trustworthiness of a different stakeholder.

At first glance, a data subject's lack of trust in a particular data controller suggests using a TET as an obvious means to verify and, if necessary, rectify disclosed personal data. However, reassigning personal trust from one party to another inevitably raises the question as to whether such a shift is reasonable or justified, if only because introducing an additional link complicates the chain of trust as a whole.

Trust, or the absence thereof, in stakeholders relates to Hedbom's [13] categorisation of trust requirements as regards the entity that provides the privacy-enhancing functionality. Hedbom defines that entities, such as client, server or third party, be either trusted, or that "no trust [is] needed." Conversely, Janic *et al.* [12] summarise that better understanding privacy issues "increases the importance of privacy for trust." They state that at the time of their publication, no tools could be identified that enabled users to better understand scenarios that dealt with complex data processing scenarios. They conclude that classifying the appropriate type of visualisation required to promote trust is a major goal in future work.

E. LOGGING, COMPLIANCE, AND TRUST

The advantage of performing logging locally is that data subjects have better control over the logging mechanism as such and are, at least theoretically, able to verify the compliance of the logging process. In such a scenario, however, the responsibility for the installation, maintenance and security of the TET typically lies with the user herself, which might not be feasible for laypersons.

The advantage of performing service-side logging is that logging lies with the one entity that is responsible for providing the actual service, and that has access to all necessary data and meta data. Consequently, the data can reside solely in the data center of the service provider, and would not have to be retransmitted to other entities. However, users of such services would have to trust the service provider with regard to the soundness and completeness of the logging process.

The advantage of relying on a third party is that the user's trust shifts from the service provider towards an independent, ideally certified service entity that is responsible for carrying out the task. However, including another entity in the chain of stakeholders complicates the overall process on a technical, administrative and legal level. It also requires that the data be retransmitted and disclosed to that party, and that that party be trusted with regard to complying with the standards on all levels.

F. LIMITATIONS

The publication retrieval process described in Section IV was meant to be systematic but not exhaustive. It was not exhaustive in that it started out with a limited set of databases and search terms and in that it traced the references of the publications retrieved during the initial search only up to one generation backwards and forwards. It was systematic in that it followed a rigorous methodology, and in that the screening of the retrieved publications was conducted according to strict, well-defined criteria.

The screening process conducted after retrieving the publications filtered out the ones that contextually qualified as ex post TETs but that failed to meet the specified screening criteria. Most notably, these criteria limited the selection to publications that presented usable implementations of TETs, that is, TETs that must at least be available in a prototypical stage or evaluated mockup. In some cases, the actual maturity of the TET could not be determined unequivocally because the status of the implementation was not discussed by the authors of the publication (see Section VI-A). In such cases, the respective publication was disregarded because the screening criteria could not be applied reliably. The screening process of the retrieved publications was conducted independently by both authors of this survey, and the current selection of TETs represents the superset of articles that both authors agreed upon.

Established ex post TETs, such as Google-Dashboard,[31] were not considered in this survey as they were not discussed in the set of publications that were retrieved during the literature research. This is not to say that respective TETs do not meet the criteria specified for the research but only that there were no scientific publications available about them that surfaced during the search process.

VII. CONCLUSIONS

On the basis of the publications retrieved via a systematic literature review, this survey has discussed the state of

[31] https://www.google.com/dashboard/

research of 24 ex post transparency enhancing tools (TETs) that have been published in the scientific literature with the intended purpose of enhancing privacy. The criteria that formed the scope of the review focused on usable implementations of TETs. The intended outcome of the review was to scrutinise existing TETs in terms of their actual usability and functionality for the intended target audience.

One main contribution of this survey has been a new fine-grained classification of ex post TETs. The TETs have been analysed in terms of common features, such as the stakeholders involved in processing personal data, the hosting platform, the actual predication they make and the visualisation techniques they employ. Due to the focus on the usability of the TETs, the course of pre studies and evaluations that led to the implementation of the TET have received particular scrutiny. The publications reviewed have been classified according to characteristics elicited in the TETs, in particular those relevant for the principles of transparency and usability. They have been arranged using a tabular classification scheme that allows mapping characteristics to TETs and vice versa. This scheme allows for quickly pointing out clusters and singularities as regards individual characteristics.

The survey at hand relates to existing surveys on PETs and TETs in that it uses similar but more fine-grained classification characteristics. Similar to former surveys, it discusses questions such as trust and user acceptance. However, it goes beyond existing work in that its set of reviewed TETs are based on a systematic retrieval process that takes into account recent developments. Thematically, this survey specifically covers usable implementations of ex post TETs.

The spectrum of the reviewed TETs varies considerably as regards their maturity, usage context and targeted audience. Referencing individual publications with the classification scheme allows for pinpointing trends and gaps in existing TETs, as well as possible future research areas. Most TETs available today were designed for highly specific usage contexts that address users who rely on a particular data service, such as sharing one's geographic location in the context of location-based services. Areas such as IoT and smart environments have not been a focus of research in the reviewed literature. Few TETs provide the means necessary to customise and individualise the functionality and UI of the TET according to the preferences and necessities of individual users. It has also been found that only few TETs allow users to both review and rectify disclosed personal data, a functionality that European data protection authorities might be interested in investigating in the foreseeable future. Moreover, future research and development efforts should focus on error prevention and context-related help for configurations, the standardisation of machine-readable policy icons, and advice and support in terms of data breach notifications and enforcing accountability.

The objective of this survey was to provide researchers and developers of privacy enhancing technologies with an overview of the characteristics of state of the art ex post TETs, on which they can build to achieve Privacy and Transparency by Design.

ACKNOWLEDGEMENT

The authors would like to thank Melanie Volkamer and Lothar Fritsch for their advice on survey methodology, Irina Persson and Leonardo Iwaya for their advice on literature research, Sarah Spiekermann for her advice on normative frameworks for classification systems, Tobias Pulls for reviewing and discussing the manuscript, and Janet Vesterlund for proofreading the manuscript.

REFERENCES

[1] C. Andersson *et al.*, "Trust in prime," in *Proc. 5th IEEE Int. Symp. Signal Process. Inf. Technol.*, Dec. 2005, pp. 552–559.

[2] S. Crane, H. Lacohée, and S. Zaba, "Trustguide—Trust in ICT," *BT Technol. J.*, vol. 24, no. 4, pp. 69–80, 2006.

[3] R. Calo, "The boundaries of privacy harm," *Ind. LJ*, vol. 86, p. 1131, Oct. 2011.

[4] G. Danezis *et al.*, "Privacy and data protection by design—From policy to engineering," Eur. Union Agency Netw. Inf. Secur. (ENISA), Heraklion, Greece, Tech. Rep., 2014, doi: 10.2824/38623.

[5] G. C. Court, "Volkszahlungsurteil," *BVerfGE*, vol. 65, no. 1, 1983.

[6] Merriam Webster Inc. (Jul. 2017). *Online Dictionary*. [Online]. Available: https://www.merriam-webster.com/

[7] M. Turilli and L. Floridi, "The ethics of information transparency," *Ethics Inf. Technol.*, vol. 11, no. 2, pp. 105–112, 2009.

[8] Oxford Dictionaries. (Jul. 2017). *Oxford Online Dictionary*. [Online]. Available: https://en.oxforddictionaries.com/

[9] OECD. (2013). *The OECD Privacy Framework*. [Online]. Available: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[10] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, document 2016/679, European Commission, 2016.

[11] M. Hildebrandt, FIDIS WP7 Deliverable. (2009). *Behavioural Biometric Profiling and Transparency Enhancing Tools. WP7 Deliverable*, Accessed: Nov. 15, 2016. [Online]. Available: http://www.fidis.net/

[12] M. Janic, J. P. Wijbenga, and T. Veugen, "Transparency enhancing tools (TETs): An overview," in *Proc. 3rd Workshop Socio-Tech. Aspects Secur. Trust*, Jun. 2013, pp. 18–25.

[13] H. Hedbom, "A survey on transparency tools for enhancing privacy," in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrcek, and P. Švenda, Eds. Berlin, Germany: Springer, 2009, pp. 67–82. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03315-5_5, doi: 10.1007/978-3-642-03315-5_5.

[14] A. S. Patrick and S. Kenny, "From privacy legislation to interface design: Implementing information privacy in human-computer interactions," in *Proc. Int. Workshop Privacy Enhancing Technol.*, 2003, pp. 107–124.

[15] ISO, "Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems," Int. Org. Standardization, Geneva, Switzerland, Tech. Rep. ISO 9241-11:1998(E), Mar. 1998. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1654.txt

[16] ISO, "Ergonomics of human-system interaction—Part 110: Dialogue principles," Int. Org. Standardization, Geneva, Switzerland, Tech. Rep. ISO 9241-110:2006(E), Apr. 2006. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1654.txt

[17] J. Nielsen, "Heuristic Evaluation," *Usability Inspection Methods*, vol. 17, no. 1, pp. 25–62, 1994.

[18] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quart.*, vol. 26, no. 2, pp. 13–23, 2002.

[19] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, 2013.
[20] EBSOhost. (2016). *InSpec*, Accessed: Nov. 15, 2016. [Online]. Available: http://search.ebscohost.com/
[21] Schloss Dagstuhl at Universität Trier. (2016). *DBLP: Computer Science Bibliography*, Accessed: Nov. 15, 2016. [Online]. Available: http://dblp.dagstuhl.de/
[22] ACM.org. (2016). *ACM Digital Library*, Accessed: Nov. 15, 2016. [Online]. Available: https://dl.acm.org/
[23] IEEE.org. (2016). *IEEE Xplore Digital Library*, Accessed: Nov. 15, 2016. [Online]. Available: http://ieeexplore.ieee.org/
[24] P. Murmann and S. Fischer-Hübner, "Usable transparency enhancing tools: A literature review," Dept. Math. Comput. Sci., Karlstad Univ., Karlstad, Sweden, Tech. Rep., Jul. 2017.
[25] E. Kani-Zabihi and M. Helmhout, "Increasing service users' privacy awareness by introducing on-line interactive privacy features," in *Proc. 16th Nordic Conf. Secure IT Syst. (NordSec)*, Tallinn, Estonia, Oct. 2011, pp. 131–148.
[26] A. Popescu *et al.*, "Increasing transparency and privacy for online social network users—USEMP value model, scoring framework and legal," in *Privacy Technologies and Policy: Third Annual Privacy Forum*, B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, and S. Schiffner, Eds. Cham, Switzerland: Springer, 2016, pp. 38–59. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-31456-3_3, doi: 10.1007/978-3-319-31456-3_3.
[27] S. Fischer-Hübner, J. Angulo, F. Karegar, and T. Pulls, "Transparency, privacy and trust—Technology for tracking and controlling my data disclosures: Does this work?" in *Proc. IFIP Int. Conf. Trust Manage.*, 2017, pp. 3–14.
[28] J. Angulo, S. Fischer-Hübner, T. Pulls, and E. Wästlund, "Usable transparency with the data track—A tool for visualizing data disclosures," in *Proc. 33rd Annu. ACM Conf. Extended Abstracts Hum. Factors Comput. Syst.*, 2015, pp. 1803–1808.
[29] F. Karegar, T. Pulls, and S. Fischer-Hübner, "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*. Springer, 2016, pp. 164–181.
[30] G. Hsieh, K. P. Tang, W. Y. Low, and J. I. Hong, *Field Deployment of IMBuddy: A Study of Privacy Control and Feedback Mechanisms for Contextual IM* (Lecture Notes in Computer Science Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 4717, J. Krumm, G. D. Abowd, A. Seneviratne, and T. Strang, Eds. 2007, pp. 91–108.
[31] K. Abdullah, G. Conti, and R. Beyah, "A visualization framework for self-monitoring of Web-based information disclosure," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1700–1707.
[32] P. G. Kelley, P. H. Drielsma, N. Sadeh, and L. F. Cranor, "User-controllable learning of security and privacy policies," in *Proc. 1st ACM Workshop Workshop (AISec)*, 2008, pp. 11–18.
[33] J. Kolter, T. Kernchen, and G. Pernul, "Collaborative privacy—A community-based privacy infrastructure," in *Emerging Challenges for Security, Privacy Trust*, vol. 297, D. Gritzalis and J. Lopez, Eds. Berlin, Germany: Springer, 2009, pp. 226–236.
[34] N. Sadeh *et al.*, "Understanding and capturing people's privacy policies in a mobile social networking application," *Pers. Ubiquitous Comput.*, vol. 13, no. 6, pp. 401–412, Aug. 2009.
[35] J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh, "Who's viewed you? The impact of feedback in a mobile location-sharing application," in *Proc. Conf. Hum. Factors Comput. Syst.*, 2009, pp. 2003–2012.
[36] J. Kolter, M. Netter, and G. Pernul, "Visualizing past personal data disclosures," in *Proc. Int. Conf. Availability, Rel. Secur. (ARES)*, Feb. 2010, pp. 131–139.
[37] E. Toch *et al.*, "Empirical models of privacy in location sharing," *Proc. ACM UbiComp*, 2010, pp. 129–138.
[38] R. Schlegel, A. Kapadia, and A. J. Lee, "Eyeing your exposure: Quantifying and controlling information sharing for improved privacy," in *Proc. 7th Symp. Usable Privacy Secur. (SOUPS)*, 2011, pp. 14-1–14-14. [Online]. Available: http://doi.acm.org/10.1145/2078827.2078846
[39] S. Trabelsi and J. Sendor, "Sticky policies for data control in the cloud," in *Proc. 10th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Jul. 2012, pp. 75–80.
[40] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "'Little brothers watching you': Raising awareness of data leaks on smartphones," in *Proc. 9th Symp. Usable Privacy Secur. (SOUPS)*, 2013, pp. 12-1–12-11. [Online]. Available: http://doi.acm.org/10.1145/2501604.2501616
[41] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, and J.-P. Hubaux, "Adaptive information-sharing for privacy-aware mobile social networks," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput. (UbiComp)*, 2013, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/2493432.2493510
[42] C. Louw and S. von Solms, "Personally identifiable information leakage through online social networks," in *Proc. South African Inst. Comput. Sci. Inf. Technol. Conf. (SAICSIT)*, 2013, pp. 68–71. [Online]. Available: http://doi.acm.org/10.1145/2513456.2513467
[43] D. Biswas, I. Aad, and G. P. Perrucci, "Privacy panel: Usable and quantifiable mobile privacy," in *Proc. 8th Int. Conf. Availability, Rel. Secur. (ARES)*, Sep. 2013, pp. 218–223.
[44] A. Zavou, V. Pappas, V. P. Kemerlis, M. Polychronakis, G. Portokalidis, and A. D. Keromytis, *Cloudopsy: An Autopsy of Data Flows in the Cloud* (Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8030. Berlin, Germany: Springer, 2013, pp. 366–375. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-39345-7-39, doi: 10.1007/978-3-642-39345-7-39.
[45] M. Y. Mun, D. H. Kim, K. Shilton, D. Estrin, M. Hansen, and R. Govindan, "PDVLoc: A personal data vault for controlled location data sharing," *ACM Trans. Sensor Netw.*, vol. 10, no. 4, p. 58, 2014.
[46] Z. Xu and S. Zhu, "SemaDroid: A privacy-aware sensor management framework for smartphones," in *Proc. 5th ACM Conf. Data Appl. Secur. Privacy (CODASPY)*, 2015, pp. 61–72. [Online]. Available: http://doi.acm.org/10.1145/2699026.2699114
[47] M. Pistoia, O. Tripp, P. Centonze, and J. W. Ligman, "Labyrinth: Visually configurable data-leakage detection in mobile applications," in *Proc. 16th IEEE Int. Conf. Mobile Data Manage.*, vol. 1. Jun. 2015, pp. 279–286.
[48] C. Bier, K. Kühne, and J. Beyerer, *PrivacyInsight: The Next Generation Privacy Dashboard* (Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9857, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Springer, 2016, pp. 135–152. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-44760-5_9
[49] C. Riederer, D. Echickson, S. Huang, and A. Chaintreau "FindYou: A personal location privacy auditing tool," in *Proc. 25th Int. Conf. Companion World Wide Web (WWW)*, 2016, pp. 243–246.
[50] E. K. Jacob, "Classification and categorization: A difference that makes a difference," *Library Trends*, vol. 52, no. 3, pp. 515–540, 2004.
[51] E. H. Bradley, L. A. Curry, and K. J. Devers, "Qualitative data analysis for health services research: Developing taxonomy, themes, and theory," *Health Services Res.*, vol. 42, no. 4, pp. 1758–1772, 2007.
[52] D. S. Cruzes and T. Dybå, "Recommended steps for thematic synthesis in software engineering," in *Proc. Int. Symp. Empirical Softw. Eng. Meas. (ESEM)*, Sep. 2011, pp. 275–284.
[53] B. H. Kwasnik, "The role of classification in knowledge representation and discovery," *Library trends*, vol. 48, no. 1, p. 22, 1999.
[54] S. Fischer-Hübner, J. Angulo, and T. Pulls, "How can cloud users be supported in deciding on, tracking and controlling how their data are used?" in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 2013, pp. 77–92.
[55] T. Pulls. (Sep. 2016). *The Data Track*. [Online]. Available: https://github.com/pylls/datatrack
[56] *Regulation (EU) 2016/679 of the European Parliament and of the Council*, The European Parliament and the Council of the European Union, Apr. 2016.
[57] ISO, "Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems," Int. Org. Standardization, Geneva, Switzerland, Tech. Rep. ISO 9241-210:2010(E), Mar. 2010. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1654.txt
[58] ISO, "Ergonomics of human-system interaction—Usability methods supporting human-centered-design," Int. Org. Standardization, Geneva, Switzerland, Tech. Rep. ISO/TR 16982:2002(E), Jun. 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1654.txt

[59] J. S. Pettersson *et al.*, "Making PRIME usable," in *Proc. Symp. Usable Privacy Secur.*, 2005, pp. 53–64.
[60] L.-E. Holtz, K. Nocun, and M. Hansen, "Towards displaying privacy information with icons," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Berlin, Germany: Springer, 2010, pp. 338–348.
[61] J. S. Pettersson, "A brief evaluation of icons in the first reading of the European parliament on COM (2012) 0011," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 2014, pp. 125–135.
[62] J. Siljee, "Privacy transparency patterns," in *Proc. 20th Eur. Conf. Pattern Lang. Programs*, 2015, p. 52.
[63] J. Angulo *et al.*, "D-5.3 user-centric transparency tools V2," Dept. of Inf. Syst. Project Manage., Karlstad Univ., Karlstad, Sweden, 2015. [Online]. Available: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A885472&dswid=-4845
[64] J. Angulo, M. Ortlieb, J. Angulo, and M. Ortlieb, "'WTH..!?!' Experiences, reactions, and expectations related to online privacy panic situations," in *Proc. Symp. Usable Privacy Secur. (SOUPS)*, 2015, pp. 19–38.

PATRICK MURMANN received the M.Sc. degree in computer science and the B.Eng. degree in media engineering. He is currently pursuing the Ph.D. degree with the Privacy & Security Research Group, Department of Mathematics and Computer Science, Karlstad University, Sweden. He is an Early Stage Researcher with the H2020 Marie Skłodowska-Curie ITN Privacy&Us (Privacy & Usability). His research focuses on usable transparency in the context of transparency enhancing tools. He has been a Research Assistant with the FP7 FET Project SmartSociety, Karlstad University and in other research projects at TH Nuremberg and also a lab engineer, a software architect and a media engineer of several international projects.

SIMONE FISCHER-HÜBNER (M'14) received the Diploma degree in computer science with a minor in law in 1988 and the Ph.D. and Habilitation degrees in computer science from Hamburg University, Germany, in 1992 and 1999, respectively. She has been a Full Professor with Karlstad University, Sweden, since 2000, where she is the Head of the Privacy and Security Research Group. Her research interests include privacy-enhancing technologies and usable privacy. She is the Vice Chair of the IEEE Sweden Computer/Software Engineering Chapter, the Chair of IFIP WG 11.6 on Identity Management, the Swedish IFIP TC 11 Representative, a member of the Scientific Advisory Committee of Science Europe, a member of the advisory board Swedish Civil Contingency Agency's Information Security Advisory Board, and has been an Expert for European Network and Information Security Agency. She has contributed as a Partner in the CREDENTIAL, PRISMACLOUD, A4Cloud, SmartSociety, PrimeLife. PRIME, FIDIS and Bugyo EU projects. She is the Scientific Coordinator of the EU H2020 Marie Skłodowska-Curie ITN Privacy&Us.