Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work?

Simone Fischer-Hübner, Julio Angulo, Farzaneh Karegar, Tobias Pulls

Transparency, Privacy and Trust – Technology for Tracking and Controlling my Data Disclosures: Does this work?

Simone Fischer-Hübner, Julio Angulo, Farzaneh Karegar and Tobias Pulls

Department of Computer Science
Karlstad University, Sweden
Email: {first name, last name}@kau.se

Abstract. Transparency is a basic privacy principle and social trust factor. However, in the age of cloud computing and big data, providing transparency becomes increasingly a challenge.
This paper discusses privacy requirements of the General Data Protection Regulation (GDPR) for providing ex-post transparency and presents how the transparency-enhancing tool Data Track can help to technically enforce those principles. Open research challenges that remain from a Human Computer Interaction (HCI) perspective are discussed as well.

Keywords: Privacy, transparency, transparency-enhancing tools, usability

1 Introduction

Transparency is an important factor for establishing user trust and confidence, as trust in an application can be enhanced if procedures are clear, transparent and reversible, so that users feel in control [1, 19]. However, especially in the context of cloud computing and big data, end users are often lacking transparency, as pointed out by the Art. 29 Data Protection Working Party [4, 5].

Big data analyses practices raise concerns in regard transparency, as individuals, unless they are provided with sufficient information, are often subject to decisions that they do not understand nor have control over.

Moreover, cloud users and data subjects lack transparency in regard to the involved supply chain with multiple processors & subcontractors, different geographic locations within the EEA (European Economic Area), transfers to third-party countries outside the EEA, and how a cloud service reacts to requests for access to personal data by law enforcement. In addition, there is a lack of intervenability for individuals, as there is a lack of tools for them for exercising their data subjects' rights.

Empirical research conducted in the EU project A4Cloud[1] for eliciting cloud customer requirements revealed that cloud customers will increase their trust that their data

[1] EU FP7 project A4Cloud (Accountability for the Cloud), http://www.a4cloud.eu/

is secure in the cloud, if there is transparency about what is possible to do with the data, possible exit procedures ("way out") and the ownership of the data [16].

Transparency of personal data processing is also an important principle for the individual's privacy as well as for a democratic society. As the German constitutional court declared in its Census Decision[2], a society, in which citizens could not know any longer who does when, and in which situations know what about them, would be contradictory to the right of informational self-determination. Consequently, the European Legal Data Protection Framework is granting data subjects information, access and control rights enforcing transparency and intervenability. Transparency-Enhancing Tools (TETs) can help to enable the individual's right for transparency also by technological means.

In this article, we discuss the data subject rights in regard to transparency and intervenability by the EU General Data Protection Regulation (GDPR [10]) (Section 2), and how they can be technically enforced by TETs and particularly by different versions and functions of the Data Track tool that has been developed at Karlstad University within the scope of the PRIME[3], PrimeLife[4] and A4Cloud EU projects (Section 3). We discuss HCI and trust challenges in regard to the Data Track (Section 4), related work (Section 5) and conclude with follow-up research questions (Section 6).

2 Transparency

The concept of transparency comprises both 'ex ante transparency', which enables the anticipation of consequences before data are actually disclosed (e.g., with the help of privacy policy statements), as well as 'ex post transparency", which informs about consequences if data already have been revealed (e.g., what data are processed by whom and whether the data processing is in conformance with negotiated or stated policies) [15].

The EU General Data Protection Regulation, which is likely to be enacted in the first half of 2016, comprises different data subject rights for providing both ex ante and ex post transparency as well as means for intervenability and control, which are extending the fundamental rights of data subjects that were provided by the EU Data Protection Directive 95/46/EC [9].

[2] German Constitutional Court, Census decision ("Volkszählungsurteil"), 1983 (BVerfGE 65,1).

[3] EU FP6 project PRIME (Privacy and Identity Management for Europe), https://www.prime-project.eu/

[4] EU FP7 project PrimeLife (Privacy and Identity Management for Europe for Life), http://prime-life.ercim.eu/

Ex ante Transparency

Ex ante transparency is a condition for data subjects of being in control and for rendering a consent[5], which has to be informed, valid.

Pursuant to Art 14 GDPR, the data controller must ensure that the data subject is provided with required privacy policy information at the time when the data is collected from the data subject, including information about the identity of the data controller and the data processing purposes, and for ensuring fair and transparent processing also information about recipients/categories of recipients, intention to transfer data to a recipient in a third country or international organization, data subject rights incl. the right to withdraw consent at any time and the right to lodge complaint with supervisory authority, the legal basis and whether the data subject is obliged to provide the data and consequences of not providing the data, as well as the existence of automated decision making including profiling, the logic involved, significance and envisaged consequences.

Ex ante TETs include policy tools and languages, such as P3P [29] the PrimeLife Policy Language PPL [26] or A-PPL [6], which can help to make the core information of privacy policies and information on how far a services side's policy complies with a user's privacy preferences more transparent to an end user at the time when he is requested to consent to data disclosure.

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 information about the data being processed, data processing purposes, data recipients or categories of recipients, as well as information about the logic involved on any automatic processing including profiling. In extension to the EU Data Protection Directive, data subjects should also be informed about the significance and envisaged consequences of such processing, as well as about safeguards taken in case of transfer to a third country. Another new provision of the GDPR for increasing transparency demands that the controller shall provide a copy of his/her personal data undergoing processing to the data subject, and if the data subject makes the request in electronic form, the information should be provided in "*an electronic form, which is commonly used*".

Furthermore, the newly introduced right to Data Portability (Art.18), which is the right to receive data in a structured and commonly used and machine-readable format and the right to transmit it to another controller (or to have it transmitted directly from controller to controller). It can thus also be used as a means for enhancing transparency, even though its objective is to prevent that data subjects are "locked" into privacy-unfriendly services by allowing them easily to change providers along with their data.

[5] 'The data subject's consent' is defined by the Data Protection Directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

However, 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 may only contain the data that the data subject explicitly or implicitly disclose, but not data that the service provider derived from that data, as such derived data (e.g., in the form of user profiles) may comprise business value for a company and a transfer to a competing service provider would thus have a strong impact on that company.

This data subject right that is providing ex post transparency is also a prerequisite for exercising the data subject rights to withdraw consent at any time, which should be made as easy as to give it (Art. 5), to obtain the 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).

In addition to the transparency rights in the GDPR, specific ex post transparency rights are, for instance, provided by the Swedish Data Patient Act [28] to data subjects by requiring that health care providers have to inform patients upon request about who has accessed their medical information.

In the next section, we will discuss how the subsequent version of the Data Track can empower users to exercise these ex post transparency rights.

3 The Data Track

The Data Track is a user side ex post transparency tool, for which different versions with subsequent enhancements have been developed within the EU research projects PRIME (FP6), PrimeLife (FP7), and A4Cloud (FP7).

PRIME and PrimeLife Data Track

The first version developed within the PRIME project includes a history function (see [24]), which was later complemented in the PrimeLife project with online access functions. The history function stores in a secure manner for each transaction, in which a user discloses personal data to a service, a record for the user on which personal data were disclosed to whom (i.e. the identity of the controller), for which purposes and, more precisely, under which agreed-upon privacy policy the user has given his/her consent, as well as a unique transaction ID. These records of consents can serve users as a reference for exercising his or her right to easily revoke consent at any time. The data disclosures are tracked by a middleware called the PRIME Core, running both on the user's side and at the remote service.

For exercising his or her rights to access, correct, delete or block data, the user needs to prove that he or she is the respective data subject. This can be done by proving knowledge of a unique transaction ID, which is stored in his/her Data Track and at the services' side for each transaction of personal data disclosure. Notably, for authentication, the data subject does not have to disclose any more personal data than what the service already knows. This allows in principle also anonymous or pseudonymous users to access their data at the services' side.

These records of provided consent stored in the user's Data Track can serve users as a reference for exercising his or her right to easily revoke consent at any time.

The Data Track's user interface version developed under the PrimeLife EU FP7 project provided search functions for the locally stored Data Track records as well as online access functions, which allowed users to easily get a tabular overview about what data they have disclosed to a services side and what data are still stored by the services' side, or what data have been inferred and added. This should allow users to check whether data have been changed, processed, added or deleted (and whether this was in accordance with the agreed-upon privacy policy).

Complete descriptions of the Data Track proof-of-concept and user interfaces developed under the PrimeLife project can be found in [30]. Usability tests of early design iterations of the PrimeLife's Data Track revealed however that many test users had problems to understand whether data records were stored in the Data Track client on the users' side (under the users' control) or on the remote service provider's side [11].

A4Cloud Data Track

Within the scope of the A4Cloud project, we have for developed and tested in several iterations alternative user interfaces (UIs) and HCI concepts consisting of graphical UI illustrations of where data are stored and to which entities data have been distributed. Graphical illustrations of data storage and data flows have a potential to display data traces more naturally as in real world networks. Moreover, previous research studies suggest that network-like visualizations provide a simple way to understand the meaning behind some types of data [13, 7] and other recent studies claim that users appreciate graphical representations of their personal data flows in forms of links and nodes [17, 18].

Therefore, for the A4Cloud Data Track (also called "*GenomSynlig*"), we developed the so-called "*trace view*" (see **Fig. 1**), presenting an overview of which data items have been sent to service providers, as well as which service providers have received what data items about the user.

The idea is that users should be able to view what selected personal data items stored in the Data Track (displayed by icons in the top panel of the UI) that they have submitted to services on the Internet (that are shown in the bottom panel of the interface). The user is represented by the panel in the middle by giving him or her the feeling that the Data Track is a user-centric tool.

If users click on one or many Internet service icons, they will be shown arrows pointing to the icons symbolising data items that those services have about them; in other words they can see a *trace* of the data that services have about them. Similarly, if they select icons of one or many data items (on the top), they will be shown arrows pointing to the Internet services that have received those data items.

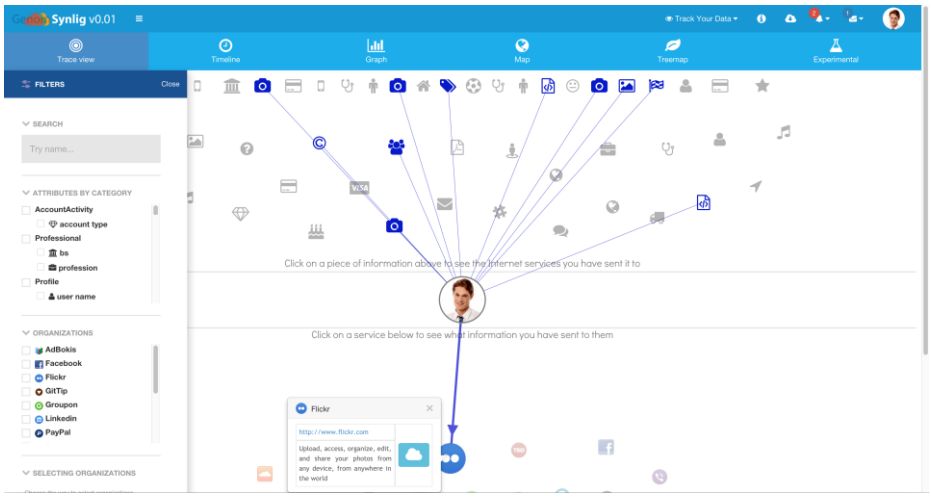

Fig. 1. The trace view user interface of the Data Track

In addition to this "*local view"* of the trace view, which is graphically displaying the information that is stored locally in the Data Track about what data has been disclosed to whom, a user can also exercise online access functions by clicking on the cloud icon next to the service provider's logo, and see "*remote views*" in a pop-up window (see **Fig. 2**) what data the service provider has actually stored about him, which it either received explicitly or implicitly from the user or derived about him.

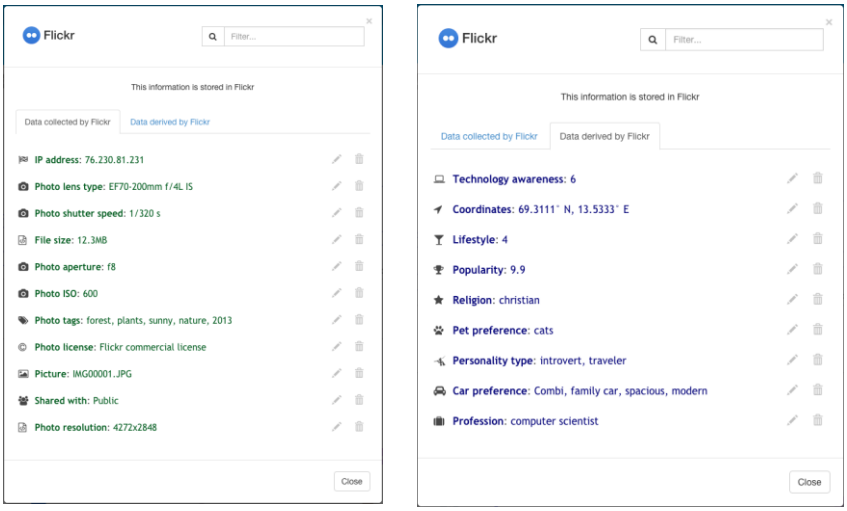

Fig. 2: Remote views of data stored at the services side that was either collected from the user (shown in the left side pop-up window) or derived about him (shown in the right side pop-up window).

Clicking on the pencil or trash bin icons located right to the data items will activate functions for requesting correction or deletion of data at the services side.

An alternative *timeline view* has been developed as well for the Data Track, which lists the information about data disclosures in the Data Track records in chronological order for selected time intervals (see **Fig. 3**).

Within the scope of A4Cloud, a cryptographic system for performing privacy-preserving transparency logging for distributed systems (e.g., cloud-based systems) has been developed [27]. In combination with the transparency logging, the Data Track could also visualise personal data flows along a cloud chain.

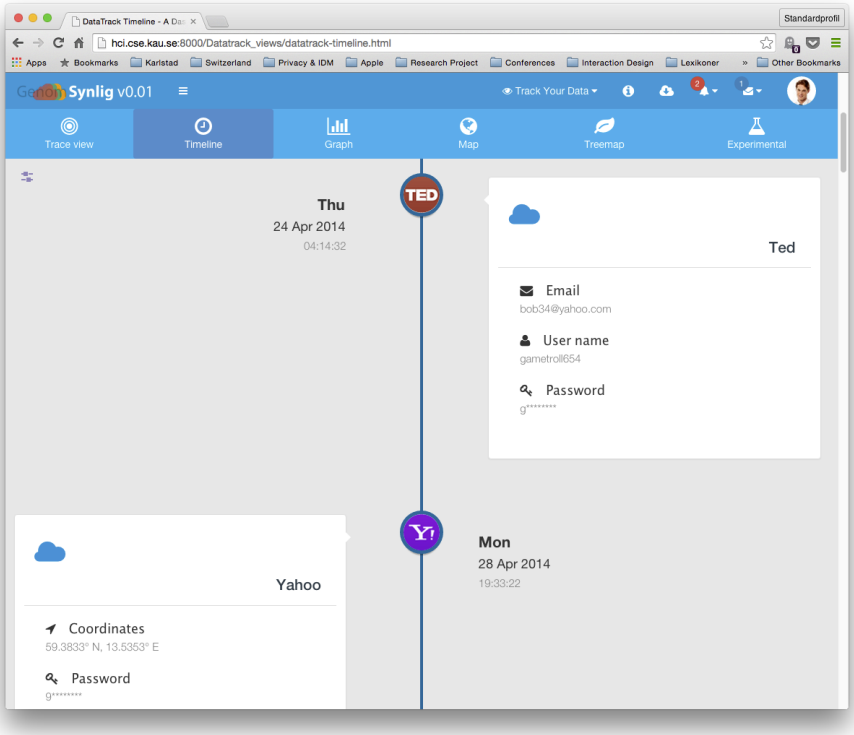

Fig. 3: The timeline view showing data disclosures in chronological order.

At the end of the A4Cloud project, we developed an open source and standalone version of the Data Track that allows the visualisation of data exported from the Google Takeout service. We focused on the Google location history, as part of the Takeout data, and developed an additional a graphical map view to complement the trace view and timeline view. As depicted in figure 4, the map view allows to visualize location, activity and movement patterns as described in the location history provided by Google. Notably, activities are data derived by Google based on primarily the location reported by Android devices.

Table 1 provides an overview of the functions of the different Data Track versions and functions and the legal privacy principles that they address pursuant to the GDPR. It shows that the different functions of the Data Track that we have developed in the subsequent versions are complementing each other, as they address different legal privacy requirements for enabling transparency and intervenability.

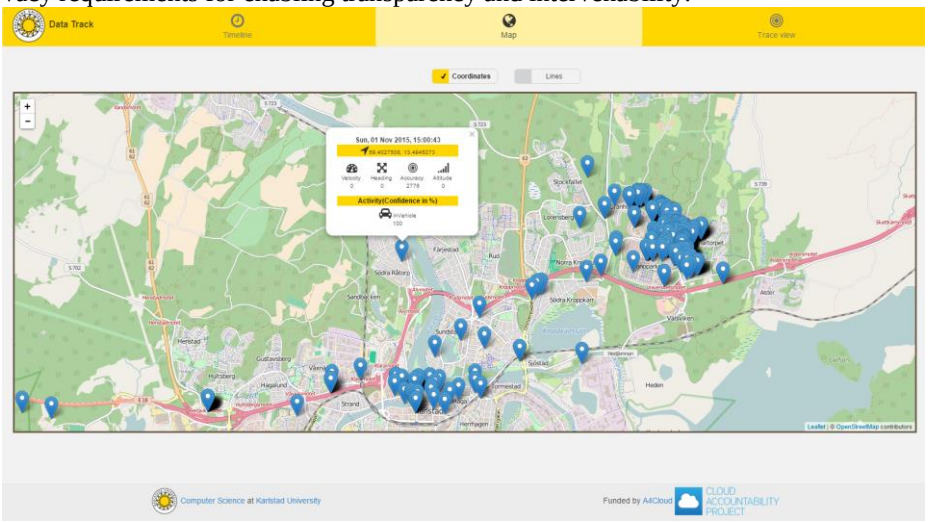

Fig. 4: The map view showing data locations, activities and movement patterns.

Table 1: Data Track Versions, Functions and GDPR legal privacy principles addressed for achieving transparency and intervenability.

Version	**Functions**	**GDPR Legal Principles addressed**
PrimeLife Data Track [11, 30]	Local database of data disclosed, transaction pseudonyms, consent given. Online access functions UI: Tabular Form	Consent Management – helps to enforce the right to object / revoke consent, pursuant to Art. 5. (Electronically provided) Data subject access functions (Art. 16, 17, 17a).
A4Cloud Data Track ("GenomSynlig") [3, 8]	Local database of data disclosed, Consent given. Online access functions Graphical UI: Trace View & Time line, search functions and tutorials	(as PrimeLife Data Track)

A4Cloud – Export Data Track Stand-alone Version[6]	Local visualisation of data exports UI: Additional graphical map view	Transparency of personal "big data" retrieved via data portability (Art. 18) or electronic copy of data (Art. 15) functions.

4 HCI Evaluation and Challenges

As pointed out in [23], the legal privacy principles, such as transparency principle, have HCI (Human Computer Interaction) 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 principles requires that data subjects comprehend the transparency and control options, are aware of when they can be used, and are able to use them. Therefore, another important design criterion for TETs is usability.

Throughout the A4Cloud project, the user interface of the Data Track has gone through three iterations of design and user evaluations with 13-16 test participants in each iteration. The evaluations were performed at Karlstad University's Ozlab for an e-Shopping scenario and consisted of a mixture of a user-based cognitive walk and a talk-aloud protocol, with which participants were encouraged to express their opinions and understanding aloud, followed by a post-test questionnaire. The evaluations had not only the objective of testing the level of comprehension of the interface, but was also a method for gathering end-user requirements on the needs and expectations that such a tool should provide to its users. Details about the results of the test iterations are reported in [2, 3, 8, 12].

In general, evaluations have also shown that participants understand the purpose of the tool and ways to interact with it, identifying correctly the data that has been sent to particular service providers, and using the filtering functions to answer questions about their disclosed personal data. The set of search functions provided for the last Data Track iteration led generally to better tracking results. Throughout the test iterations, the majority of test users also saw the Data Track as a potentially useful tool and appreciated its transparency options and would use it on a regular basis. Most test users of the last test iteration preferred the trace view over the timeline view.

Also at an evaluation workshop organised by A4Cloud partner SINTEF, the advantages and possible risks of using a tool such as the Data Track were discussed, as well as the requirements to make such a tool not only usable but also adopted in their daily Internet activities. It was for instance commented by one participant that transparency provided by the Data Track, would encourage service providers to comply with their policies and be responsible stewards of their customers data, "*it would keep me*

[6] https://github.com/pylls/datatrack

informed and hold big companies in line." Another participant mentioned as a benefit the increased awareness of disclosures made to service providers, "*makes you aware of what information you put on the Internet, you probably would be more careful*" (see [16]).

Usability tests of earlier designs of the Data Track already revealed that users expressed feelings of surprise and discomfort with the knowledge that service providers analyse their disclosed data in order to infer additional insights about them, like for instance their music preferences or shopping behavior. Hence, making data processing practices for user profile should be an important functionality of an ex post TET.

The tests also revealed that there remain still difficulties for a larger portion of users to differentiate the local from the remote view, i.e. to differentiate between what data is locally stored under their control on their computers (shown by the trace or timeline view) and what data is stored on the services' side but accessible via the online access functions shown through the pop-up dialog).

Some test users as also voiced scepticism of the level of security of their data. The Data Track storing big personal data becoming a single point of failure was also mentioned as a potential risk by participants of the SINTEF workshop [16].

Understanding that the data stored in the Data Track are under the user's control, is however an important prerequisite for end user trust and adoption, along with effective means of security that are communicated to the users.

Security for the A4Cloud Data Track mainly relies on encryption (data is encrypted at rest). To avoid risks associated with long-term collection and central storage of personal data in the Data Track, the latest standalone version of the Data Track takes a different approach. Since the primary purpose of the standalone Data Track is to visualise data exported from online services, there is no need for long-term local storage. Once the Data Track is closed, all data collected locally is deleted together with the ephemeral encryption key that was used to temporarily store data while the Data Track was running.

However, results from first usability tests conducted on latest stand-alone Data Track version with 16 test users revealed once more the problem that test participants had problems to differentiate between what data was under their control (after they exported the data to their computers) and to what data the controller (in this case Google) still had access. Several of the test users did not understand that their exported location data that was visualised with the Data Track was a local copy stored on the user's machine, but rather got the impression that the exported data was synchronized with Google's remote data storage. Consequently, the idea behind deleting all exported data after closing the Data Track was not well understood by them.

5 Related work

Related data tracking and control tools for end users are in contrast to the Data Track usually restricted to specific applications, cannot be used directly to track data along cloud chains or are not under complete control of the users. Examples are Mozilla's Lightbeam [21] that uses interactive visualizations to show the first and third party sites that a user is interacting with on the Web, and Google Dashboard [14], which grants its

users access to a summary of the data stored with a Google account including account data and the users' search query history. In contrast to the Data Track, the Dashboard provides access only to authenticated (non-anonymous) users.

Related to the Data Track are services that are targeting at giving users back control of their own data, such as datacoup.com, as well as personal data vaults, such as [20] developed for participatory sensing applications, which includes a logging functionality that allows displaying transactions and transformations of users' data and enables users to track who has accessed their data.

The DataBait tool [25], developed within the EU FP7 research project USEMP[7], allows users of online social networks to share their data with a secured trusted research platform, which uses Machine Learning algorithms to provide profile transparency by explaining how users may be targeted on the basis of their postings and behavioural data. In contrast to the Data Track, its emphasis has not been put on graphical visualisation of data traces. Besides, requires end users to entrust all their data to a transparency service operated by a third party, while the Data Track is a user-side tool that allows the user to keep complete control over the Data Track data. While user control is advantageous from a privacy perspective, it does however also put higher demands on the end users for setting up and running the Data Track in a safe system environment.

6 Conclusions and Outlook

Transparency is a basic privacy principle and social trust factor. In this paper, we discussed legal principles pursuant to the GDPR for providing transparency and intervenability for users and discussed how these principles can be enforced by TETs, and particularly by the Data Track as an example of an ex-post TET that can operate under complete user control. We show that the different Data Track functions that we have developed for the different Data Track versions are complementing each other, because they are addressing different legal privacy requirements of the GDPR for enabling ex-post transparency and intervenability.

While several iterations of usability tests have shown that end users appreciate the transparency functionality of the Data Track, the user's perception of control and security in regard to the Data Track remain challenges to be tackled for also promoting end user trust in the Data Tack.

Further research challenges that we would like to tackle in our future research relate to transparency about the consequences of potential big data profiling by both service providers and other government agencies, such as for instance tax authorities conducting social network analyses for detecting tax fraud. In particularly, we are interested to analyse how the right to data portability and/or the right to receive an electronic copy of one's data together with the right to information about the logic involved in profiling, can enable citizens to aggregate their data and to infer and understand what government applications might deduce from them via profiling and what the possible consequences can be.

[7] EU FP7 project USEMP (User Empowerment for enhanced Online Management), http://www.usemp-project.eu;

References:

1. Andersson, C., Camenisch, J., Crane, S., Fischer-Hübner, S., Leenes, R., Pearson, S., Pettersson, J.S. & Sommer, D. (2005). Trust in PRIME. In Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology. IEEE Xplore.
2. Angulo, J., Fischer-Hübner, S., Pettersson, J.S. (2013) General HCI principles and guidelines for accountability and transparency in the cloud. A4Cloud Deliverable D:C-7.1, September 2013. A4Cloud Project.
3. Angulo, J., Fischer-Hübner, S., Pulls, T., & Wästlund, E. (2015). Usable transparency with the Data Track: A tool for visualizing data disclosures. In Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems – CHI 2015 (pp. 1803-1808). ACM.
4. Art. 29 Data Protection Working Party (2012). Opinion 5/2012 on Cloud Computing. (July 1st, 2012). European Commission.
5. Art. 29 Data Protection Working Party (2013), Opinion 03/2013 on Purpose Limitation (April 2, 2013). European Commission.
6. Azraoui, M., Elkhiyaoui, K., Önen, M., Bernsmed, K., De Oliveira, A.S., Sendor, J. (2015): A-PPL: An accountability policy language. In: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, pp. 319–326. Springer.
7. Becker, R.A., Eick, S.G. & Wilks, A.R. (1995). Visualizing network data. IEEE Transactions on Visualization and Computer Graphics, 1 (1), 16-28.
8. Bernsmed, K., Fischer-Hübner, S., et al. (2015), A4Cloud Deliverable D.D-5.4 User Interface Prototypes, 31.09.2015.
9. European Commission (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Office Journal L. 281. 23.11.1995.
10. European Commission (2015). Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 15 December 2015.
11. Fischer-Hübner, S., Hedbom, H. and Wästlund, E. "Trust and Assurance HCI." Privacy and Identity Management for Life. Springer Berlin Heidelberg, 2011. 245-260.
12. Fischer-Hübner, S., Angulo, J., & Pulls, T. (2013). How can cloud users be supported in deciding on, tracking and controlling how their data are used?. In Privacy and Identity Management for Emerging Services and Technologies (pp. 77-92). Springer Berlin Heidelberg.
13. Freeman, L.C. (2000). Visualizing social networks. Journal of social structure, 1 (1), 4.
14. Google. Google dashboard. https://www.google.com/settings/dashboard
15. Hildebrandt, M. (2009). Behavioural biometric profiling and transparency enhancing tools. FIDIS Deliverable, D7.12. FIDIS EU project.

16. Jaatun, M. G., Cruzes, D. S., Angulo, J., & Fischer-Hübner, S. (2015). Accountability Through Transparency for Cloud Customers. In Cloud Computing and Services Science (pp. 38-57). Springer International Publishing.
17. Kani-Zabihi, E., Helmhout, M. & Coles-Kemp, L. (2012). Increasing Service Users' Privacy Awareness by Introducing On-line Interactive Privacy Features. IAAC Symposium 2011, [Online].
18. Kolter, J., Netter, M. & Pernul, G. (2010). Visualizing past personal data disclosures. In ARES'10 International Conference on Availability, Reliability, and Security, IEEE.
19. Lacohée, H., Crane, S. & Phippen, A. (2006). Trustguide: Final Report.
20. Maguire, M. & Bevan, N. (2002). User requirements analysis. In Proceedings of IFIP 17th World Computer Congress. Mun, M. Hao, S., Mishra, N., Shilton, K., Burke, J., Estrin, D., Hansen, M., Govindan, R.: Personal data vaults: a locus of control for personal data streams. CoNEXT 2010: 17. ACM Digital Library.
21. Mozilla. Lightbeam add-on for Firefox, https://www.mozilla.org/en-US/lightbeam/.
22. Nielsen, J. (1995). Usability inspection methods. In Conference companion on Human factors in computing systems. ACM.
23. Patrick, A.S. & Kenny, S. (2003). From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In Privacy Enhancing Technologies. Springer.
24. Pettersson, J. S., Fischer-Hübner, S., & Bergmann, M. (2007). Outlining "Data Track": privacy-friendly data maintenance for end-users. In Advances in Information Systems Development (pp. 215-226). Springer US.
25. Popescu, A., et al (2015) "User Empowerment for Enhanced Online Presence Management – Use Cases and Tools", Amsterdam Privacy Conference 2015, pages 23-26, 8 October 2015, Amsterdam.
26. PrimeLife, "Privacy and Identity Management in Europe for Life - Policy Languages," http://primelife.ercim.eu/results/primer/133-policy-languages.
27. Pulls, T., Peeters, R., and Wouters, K. (2013). Distributed Privacy-Preserving Transparency Logging. In Workshop on Privacy in the Electronic Society. ACM.
28. Svensk Författningssamling Riksdagen.Patientdatalag (2008: 355).
29. W3C, "P3P – The Platform for Privacy Preferences 1.1 (P3P1.1) Specification," W3C Working Group Note, 13 November 2006. http://www.w3.org/P3P/.
30. Wästlund, E. & Fischer-Hübner, S. (2010). End User Transparency Tools: UI Prototypes. PrimeLife Deliverable D.4.2.2. PrimeLife project.