Citizen Empowerment by a Technical Approach for Privacy Enforcement

Sascha Alpers[1], Stefanie Betz[2], Andreas Fritsch[2] ,Andreas Oberweis[1, 2], Gunther Schiefer[2] and Manuela Wagner[2]
[1]*FZI Forschungszentrum Informatik, Karlsruhe, Germany*
[2]*Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany*
{alpers, oberweis}@fzi.de, *{stefanie.betz, andreas.fritsch, andreas.oberweis, gunther.schiefer, manuela.wagner}@kit.edu*

Keywords: Data Protection, Mobile Apps, Privacy Enhancing Technologies, Data Sovereignty, Legal Conformity, Usability.

Abstract: It is a fundamental right of every natural person to control which personal information is collected, stored and processed by whom, for what purposes and how long. In fact, many (cloud based) services can only be used if the user allows them broad data collection and analysis. Often, users can only decide to either give their data or not to participate in communities. The refusal to provide personal data results in significant drawbacks for social interaction. That is why we believe that there is a need for tools to control one's own data in an easy and effective way as protection against economic interest of global companies and their cloud computing systems (as data collector from apps, mobiles and services). Especially, as nowadays everybody is permanently online using different services and devices, users are often lacking the means to effectively control the access to their private data. Therefore, we present an approach to manage and distribute privacy settings: PRIVACY-AVARE is intended to enable users to centrally determine their data protection preferences and to apply them on different devices. Thus, users gain control over their data when using cloud based services. In this paper, we present the main idea of PRIVACY-AVARE.

1 INTRODUCTION

Our life is characterized by connected services and ubiquitous internet. Businesses are connected via the Cloud, citizens use available services via the global network. This leads to fundamental changes in society and business life as well as communication in general. Internet of things, digital social networks, commercial rebate systems, cloud applications and ubiquitous services lead to an increasing value of personal information. This information is collected, stored, used and exploited (partly without the user being aware of it) although European data protection provisions require an adequate level of transparency (Christl and Spiekermann, 2016, p. 121).

Currently, many services require more privileges than they actually need. It is a legal obligation to minimize data collection, but this is not actual practice (Felt et al., 2011a, 2011b). Moreover, it is not always necessary, that users are clearly identifiable via IDs (for instance, in case of iOS the Unique Device Identifier), but many applications use this information and transfer it only partially encrypted to the respective provider (Smith, 2010). More problems occur, if users disclose also third persons' personal information (like photos or contact data) without their consent. This can lead to data protection infringement (*Local Court Bad Hersfeld 15.05.2017 - F 120/17 EASO*, 2017).

This situation shows the problems for users to protect their privacy, especially on different devices. Moreover, researchers face the so called privacy paradox: On the one hand users and industry often express their concerns on phenomena like Big Data or Internet of Things and the desire for enhancing privacy. But, on the other hand they use privacy infringing services without applying privacy protecting solutions (Vervier et al., 2017). There exist several approaches to explain this paradox, like for example the users' missing awareness of privacy risks due to a lack of proper information (Leibenger et al., 2016). Or the possible low availability of privacy preserving solutions and the high effort or expenses involved (Forum Privatheit, 2014). Also discussed in research are network effects that determine which network is used. Think for example about more privacy sensitive alternatives to

WhatsApp like e.g. Threema. They fail to get a big market share as they enter the market after the big player (Schreiner and Hess, 2015). Taking this example, users can decide to either give their data to the service provider or not to participate in communities. So it is possible that the refusal to provide personal data results in drawbacks participating in digitalized social interaction. Therefore, it is important to help users to protect their personal data through user-friendly privacy enhancing technologies, while still allowing them to benefit from the full range of useful services – often only offered for free in "exchange" for personal data.

In Europe, the upcoming General Data Protection Regulation (GDPR) empowers the citizens' self-determination and obliges providers to apply privacy by design. These obligations also apply to international companies outside the EU, if they offer goods and services to people located within the EU or monitor their behaviour. If providers violate these obligations, technical control and enforcement mechanisms can empower users to claim their right to data protection. But, they need to be legally compliant because if users risk legal consequences they might feel discouraged from using privacy solutions. Moreover, the technology should be user friendly and users should be able to centrally define privacy settings in accordance to their individual preferences once, which afterwards are distributed and enforced on (all) devices of the user. Thus, in this position paper we are presenting such an approach: PRIVACY-AVARE

The outline of the paper is as follows: We first present existing approaches for privacy enforcements (in section two), then we present our approach: PRIVACY-AVARE in section three (The Idea). Finally, we end the paper with a short summary and outlook.

2 DATA PRIVACY PREFERENCES

It is already possible to allow or deny access to certain categories of data on many systems. For example, since Android 6 it is possible to allow or deny apps the access to address book, calendar, location and sensors. But it is not possible to set fine granular preferences. In a typical address book for each contact forename, surname, birthdate, email address, postal address, telephone numbers, mobile numbers, company information and maybe role information are stored. For a network application like WhatsApp or Threema only a few of this information is needed, typical users need name and mobile number (and for Threema also mail address). So users need the possibility to allow apps to access only certain fields of each address. Additionally, the users want to hide selected contact information for example, if the relationship is socially taboo.

Fine granular preferences also exist for other data categories, e.g. for the location information. There are some apps / services like turn-to-turn-navigation that need the exact location. But, for other apps it is enough to know the position in a wider radius. For a weather forecast app for example a lower accuracy would be enough.

We miss this functionality in existing solutions. Three kinds of approaches do exist from a technical viewpoint:

1. Remove authorizations via the modification of the manifest file (e.g. Advanced Permission Manager)
2. Add a security library (e.g. SRT AppGuard)
3. Make a modification at the operating system level (e.g. XPrivacy)

Figure 1 shows these three approaches, visualizing modifications of the (source) code in dark colour. The latter two solutions use sandboxes. A sandbox is referred to as environment, which restricts actions by an application according to defined rules (Bishop, 2012). By an access restriction the risk of a violation of the defined rules is reduced (Goldberg et al., 1996). This concept, derived from IT security, was adopted to data protection, e.g. by Backes et al. (2015).

We have published an overview of our analysis on existing solutions regarding access management for user support (Alpers et al., 2017a), including a comprehensive assessment concerning usability and functionality aspects. In the following, we shortly present the main limitations of the examined existing solutions:

a) Only few solutions enable the user to reveal just selected parts of information (e.g., chosen contacts (from all) or only telephone numbers hiding further information).
b) Currently, only a few solutions grant the option to provide substitute data to ensure the ongoing performance of the used services. Existing solutions are for example PDroid or MoboClean (partially).
c) Users are not supported when applying privacy settings. For example, very few solutions provide group settings.
d) Overall, basic usability should be provided, however it is often overlooked in existing privacy solutions.

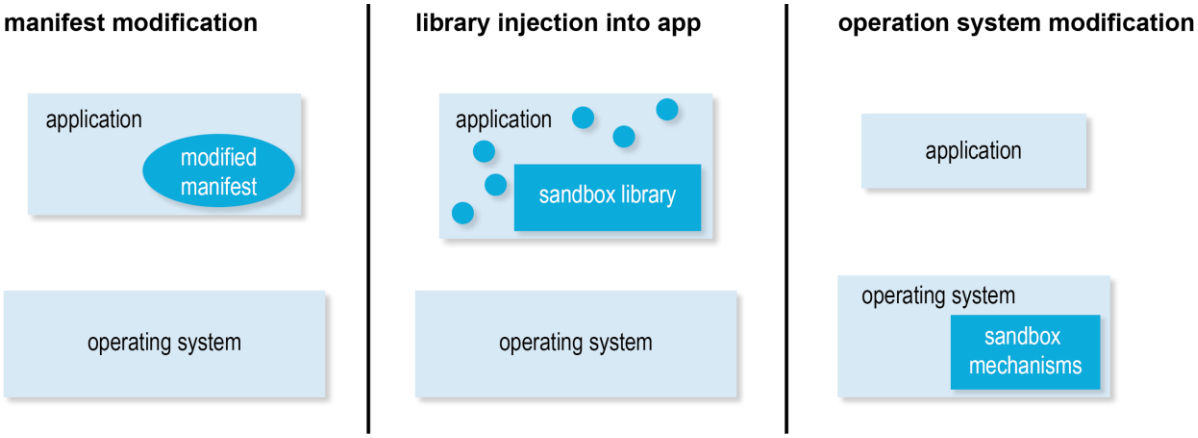

Figure 1: Different mechanisms for right management (Alpers et al., 2017b).

e) Users need to have a relatively high level of technical proficiency to use the existing solutions, especially when using those with more functionalities than just blocking the data access.
f) Legal compliance is often not ensured for existing solutions (see 3.3).

Thus, a new, more comprehensive solution for privacy enforcement is needed.

3 THE IDEA

To empower users to decide themselves about their own data we suggest more privacy settings options. A typical user utilizes different apps (like WhatsApp, Threema, Maps, etc.) and services (routing, mail, internet, etc.) on different operating systems (Android, iOS, Windows, Linux) and devices (smartphones, tablets, notebooks, SmartTVs, cars, etc.). Many of these devices, systems, services and apps have access to stored personal information or the chance to collect information by sensors or user tracking. For every app and service, a user has an idea which data may be shared or collected. Even if every system would allow the user to control the access, he will not describe the preference manually on each system for each service or app. It should be possible to describe them once (for a category of apps and services) and enforce them on every device.

The best way would be that system manufacturers develop a standard for fine-grained privacy settings and their privacy friendly distribution. But they seem not motivated enough to do so. So states (governments) or confederation of states should help their citizens and enforce such a concept by law. It remains to be seen, whether the concept of privacy by design and by default combined with the increase of sanctions by the upcoming GDPR will have the effect to foster such solutions. Until policies like this exists we want to help users to describe and enforce their privacy preferences. Based on the requirements described above, we have developed a concept for a distributed privacy management solution, named PRIVACY-AVARE. In the following, we first refine the basic functional requirements and then describe a system concept that implements these refined functionalities. We also describe in more detail, how such a system can account for the defined compliance and usability requirements.

3.1 Refined Functional Requirements

In order to enhance privacy our software application PRIVACY-AVARE will have the following three essential functionalities:

(1) Enter the user's preference profile: PRIVACY-AVARE can be used to record the user's privacy preferences. The user of PRIVACY-AVARE is supported by suitable explanations for technical and legal laypersons. It creates a personal preference profile. Therefore, we need a user-friendly comprehensive GUI (see section 3.5) and local data storage capabilities.

(2) Distribute the user's preference profile: The preference profile can be distributed via a central service to all devices of the user. In order to secure the exchange, a technical requirement is an end-to-end encryption. Therefore, the user uses a locally created symmetric key to encrypt the preferences (e.g. using AES-256). The key is distributed to other devices by embedding it into a QR code, displayed on the first device and photographed by the second one. This means that the user does not have to entrust his preferences to a central service in plain

text; the key itself is not known to the central service.

(3) Enable the user to control data access: PRIVACY-AVARE enables the user to allow fine-grained data access. Therefore, PRIVACY-AVARE has different levels of data access control. Data access can be blocked or filtered. Furthermore, PRIVACY-AVARE provides the possibility to use substitute data (no data or specially generated data) in case the app stops working otherwise. This leads to the following technical requirements:

a) PRIVACY-AVARE has to monitor data access requests at runtime and block data flows corresponding to the blockage rules set by the user (privacy profile).

b) PRIVACY-AVARE has to extract data from resources (e.g. address book) as defined by filtering rules at runtime.

c) PRIVACY-AVARE has to deliver substitute data to an application that would react with failure to a denied data access otherwise. Thus, PRIVACY-AVARE has to be able to generate plausible substitute data.

d) PRIVACY-AVARE has to incorporate permission settings of existing applications.

Those data flow filtering and blockage mechanisms are executed during runtime.

3.2 System Concept

From the refined technical requirements, we derive the following architecture: Figure 2 shows an overview of the operating principle.

PRIVACY-AVARE is based on client server architecture. The server is responsible for storage and delivery of encrypted privacy profiles. The client enables the user to set his privacy preferences in three different levels of granularity. The privacy settings result in rules for data flow control. Furthermore, the client enforces these privacy data flow rules. It controls which data flows from hardware, sensors or other data sources to an app using blocking, filtering or substitute data. The client's architecture is designed independently from specific platforms (i.e. Android, iOS, Windows). This facilitates the usage of PRIVACY-AVARE on several devices (mobiles, tablets, smart homes, cars, etc.) with different operating systems in various versions.

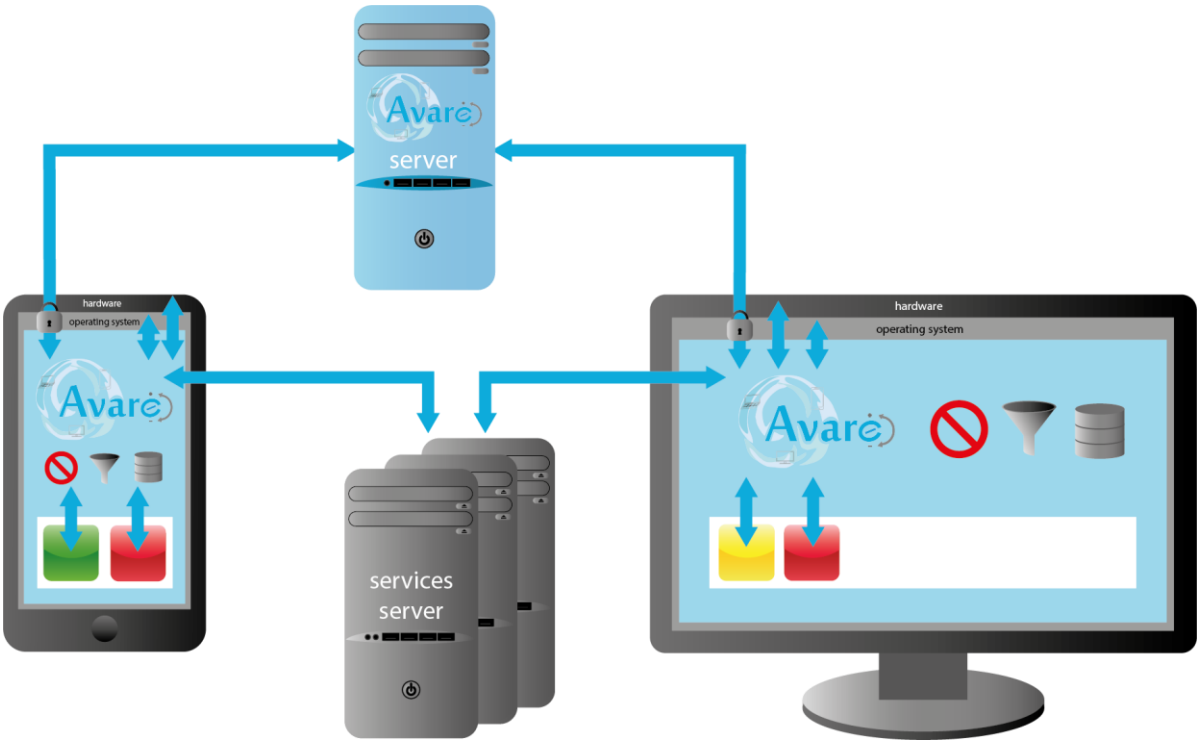

Figure 2: Operating Principle of PRIVACY-AVARE (Alpers et al., 2017b).

3.3 Compliance

As it should not be the obligation of the user to decide on complex legal questions, our concept addresses potential legal infringements. First, the chosen technical solution should not interfere with copyrights. Computer programmes are mostly protected as long as the programming required an act of certain creativity. While the functionality of a programme is not protected, there is a dispute whether only the programme code itself or also the programme routine is protected under copyright law, so that every change of programme sequences would require a licence by the author or an exemption by law (Spindler, 2012). Regarding Android, alterations are permitted under the Apache licence, except manufacturers' modifications. The privacy solution might alter such programme components, which fall within an open source licence, so that other proprietary components are just not triggered. Thus, this could be considered as an interference with the function of a programme, but not an alteration of the proprietary code (*KG Berlin 17.03.2010 - 24 U 117/08*, 2010). Even if an infringement of code is inevitable, an exemption by law provides the possibility to alter computer programmes in order to achieve the intended usability, which is especially necessary, if flaws in the programming must be corrected. A "correction" of data protection infringements could be subsumed under this provision (Bodden et al., 2013), but still legal uncertainty remains.

If modifications of the operating system require users to root their device, they face the risk of losing the guarantee or warranty. While warranty claims have to be fulfilled under the respective legal obligations unless the defect was the result of the modification, a voluntarily provided guarantee can be revoked in case users violate contractual conditions (as long as these conditions comprise no unreasonable disadvantage to the customer). So, from a user's point of view rooting comprises certain drawbacks which should be avoided.

The best solution to prevent copyright infringements would be to avoid permanent modifications of the proprietary code and to limit alterations of the programme routine to a minimum, using existing interfaces redirecting communication between app and operating system.

Regarding substitute data, potential legal infringements should be minimized by using escalation steps. Even if apps are provided "for free", users enter a contractual relationship. Whether or not users risk to violate rights of their contractual partners when they provide wrong information, depends on the individual case. A "right to lie" might apply in case of data protection infringements, but a privacy solution should not require the user to evaluate the legality of data collection as this would require certain legal skills. Thus, the solution should minimize implications by design choices. Only if the blocking of data access leads to a loss in the functionality of the app, empty data is provided (like an empty address book and calendar, no sound, etc.), so that the opponent cannot learn anything (wrong) from such data. If the app detects this protective measure, substitute data consisting of publicly available information is provided, in order to reveal no personal information about the user or third users and meanwhile reduce potential damages due to false data. Substitute data could be e.g. public holidays (calendar), public authorities / companies (address book), background noise (microphone), image noise (camera). Special cases are location data and IDs, as providing false location data could also lead to negative consequences for other users, e.g. when data is used by the app provider for traffic jam prediction. To solve this, we propose a solution that does not provide false location data, but blurred substitute locations. These substitute locations are randomly selected within a given radius. This radius can then be given to the app provider as a corresponding uncertainty. The app provider will only receive the substitute location and uncertainty information - information that is not false, but blurred.

3.4 Categorization

As Kelley et al. (2012) have shown, smartphone users have difficulties to understand the implications of their privacy settings. The goal of PRIVACY-AVARE is therefore to reduce the complexity of privacy decisions. We propose a categorization of apps with similar profile of privacy settings based on expert judgements. For example, one category consists of applications providing navigation functionality. Apps within the category navigation need the location of the user, but can generally be restricted, say, when accessing other sensor data. Apps can be sorted within these predefined categories, reducing the cognitive load for the user. This way, the user does not need to make a decision for every single app and every single privacy setting. The predefined categorization can also be supported by explanatory text to teach the user about sensible settings regarding possible privacy risks. To provide the necessary flexibility for apps that do not fit within one category, the user still has the possibility to overwrite specific settings for one app or to create custom categories.

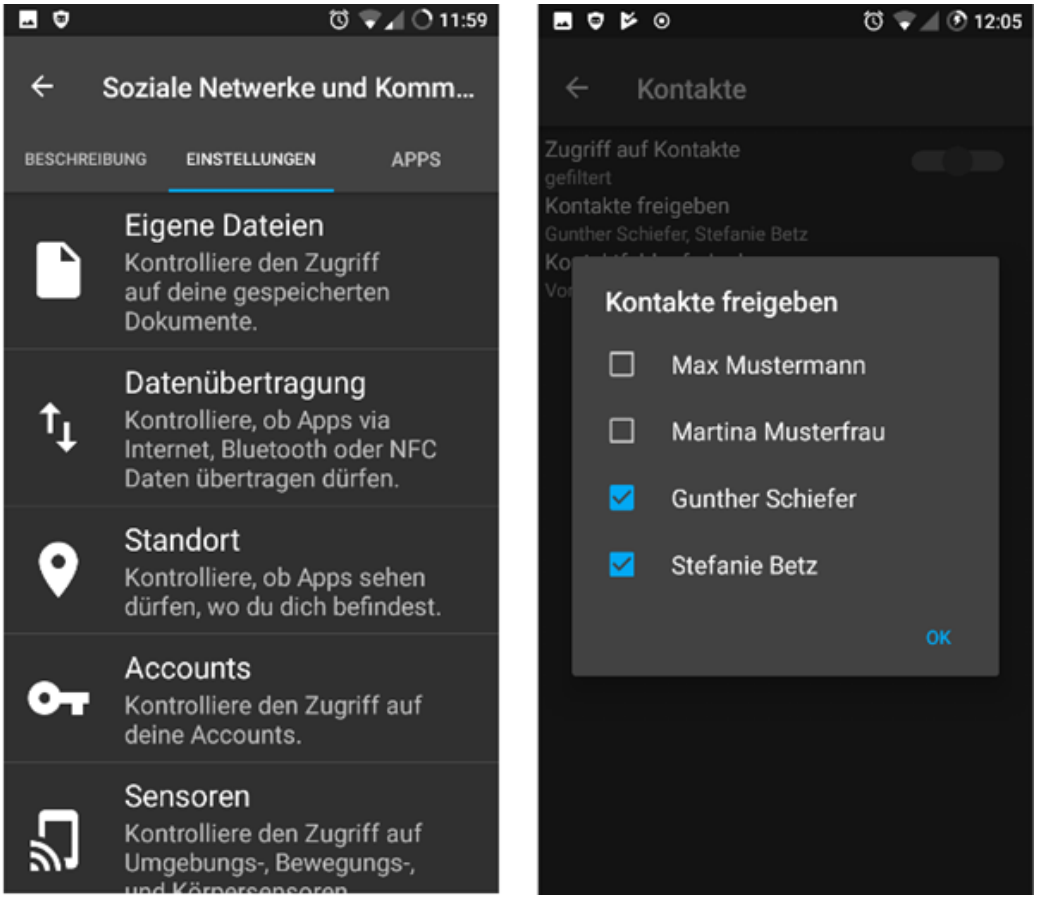

Figure 3: Screenshots of UI Prototype.

3.5 UI Prototype

We have developed an early UI prototype to illustrate our idea. Initially, the user is shown a list of predefined app-categories, as explained above. Figure 3 shows exemplary screenshots of the available settings within one category. On the left side, the user has selected the app-category "Social Networks and Communication" (containing Apps like, for example, Facebook or WhatsApp). The currently selected tab lists all available privacy settings, like access to personal files, location, sensors, contacts, and so on. Another tab "Apps" allows adding and removing apps from the category, which is not shown here.

The screenshot on the right in Figure 3 shows an example, how the user could manipulate the settings for contacts within one app-category (similar possibilities are available for the other privacy settings). The user may choose to block access to contacts altogether, or to provide substitute date, in case the app does not work without access to contacts. As explained in section 3.3, this could be addresses of public authorities or companies. The user may also choose to filter data access. In this example, the user decides to share the contact data of "Gunther Schiefer" and "Stefanie Betz", but to hide the contact data of "Max Mustermann" and "Martina Musterfrau". These settings are then applied to all apps within the category "Social Networks and Communication". Additionally, there is the possibility for the user to create custom categories or to override the settings for one app within a category (not shown in the screenshots).

4 SUMMARY AND OUTLOOK

In this position paper, we presented an approach (PRIVACY-AVARE) to empower the privacy enforcements of citizens. The approach is based on an analysis of existing solutions for privacy enhancement and the main functional requirements are presented. We presented the general operating

principle of PRIVACY-AVARE and discussed some non-functional compliance and usability requirements. PRIVACY-AVARE enables users to gain control over their data and thus enhances confidence in cloud based services.

Currently, we are implementing our approach (for Android devices) with a focus on privacy enforcement for German citizens. The code is Open Source (Apache 2.0) and available on GitHub[1].

ACKNOWLEDGEMENTS

This work has been financed by the Baden-Württemberg Stiftung gGmbH within the project 'AVARE'.

REFERENCES

Alpers, S., Betz, S., Fritsch, A., Oberweis, A., Pieper, M., Schiefer, G., Wagner, M., 2017a. Existing Software [WWW Document]. URL http://projects.aifb.kit.edu/avare/existing_software/ (accessed 24.01.2018).

Alpers, S., Oberweis, A., Pieper, M., Betz, S., Fritsch, A., Schiefer, G., Wagner, M., 2017b. PRIVACY-AVARE: An Approach to Manage and Distribute Privacy Settings, in: 3rd IEEE International Conference on Computer and Communications. pp. 1460–1468.

Backes, M., Bugiel, S., Hammer, C., Schranz, O., Von Styp-Rekowsky, P., 2015. Boxify: Full-fledged App Sandboxing for Stock Android, in: Proceedings of the 24th USENIX Conference on Security Symposium, SEC'15. USENIX Association, Berkeley, CA, USA, pp. 691–706.

Bishop, M., 2012. Computer security: art and science. Addison-Wesley, Boston ; Munich

Bodden, E., Rasthofer, S., Richter, P., Roßnagel, A., 2013. Schutzmaßnahmen gegen datenschutz- unfreundliche Smartphone-Apps: Technische Möglichkeiten und rechtliche Zulässigkeit des Selbstdatenschutzes bei Apps. Datenschutz Datensicherheit - DuD 37, 720–725. https://doi.org/10.1007/s11623-013-0300-1

Christl, W., Spiekermann, S., 2016. Networks of control: a report on corporate surveillance, digital tracking, big data & privacy. Facultas, Wien.

Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D., 2011a. Android permissions demystified, in: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, pp. 627–638.

Felt, A.P., Greenwood, K., Wagner, D., 2011b. The effectiveness of application permissions, in: Proceedings of the 2nd USENIX Conference on Web Application Development. pp. 7–7.

Forum Privatheit, 2014. White Paper Selbstdatenschutz.

Goldberg, I., Wagner, D., Thomas, R., Brewer, E.A., 1996. A Secure Environment for Untrusted Helper Applications Confining the Wily Hacker, in: Proceedings of the 6th Conference on USENIX Security Symposium, Focusing on Applications of Cryptography - Volume 6, SSYM'96. USENIX Association, Berkeley, CA, USA, pp. 1–1.

Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D., 2012. A conundrum of permissions: installing applications on an android smartphone, in: International Conference on Financial Cryptography and Data Security. Springer, pp. 68–79.

KG Berlin 17.03.2010 - 24 U 117/08, 2010.

Leibenger, D., Möllers, F., Petrlic, A., Petrlic, R., Sorge, C., 2016. Privacy Challenges in the Quantified Self Movement – An EU Perspective. Proc. Priv. Enhancing Technol. 2016. https://doi.org/10.1515/popets-2016-0042

Local Court Bad Hersfeld 15.05.2017 - F 120/17 EASO, 2017.

Schreiner, M., Hess, T., 2015. Examining the role of privacy in virtual migration: The case of whatsapp and threema.

Smith, E., 2010. iPhone applications & privacy issues: An analysis of application transmission of iPhone unique device identifiers (UDIDs). URL Www Pskl Uswpwp-Contentuploads201009iPhone-Appl.-Priv.-Issues Pdf.

Spindler, G., 2012. Grenzen des Softwareschutzes. Comput. Recht 28. https://doi.org/10.9785/ovs-cr-2012-417

Vervier, L., Zeissig, E.-M., Lidynia, C., Ziefle, M., 2017. Perceptions of Digital Footprints and the Value of Privacy: SCITEPRESS - Science and Technology Publications, pp. 80–91. https://doi.org/10.5220/0006301000800091

[1] https://github.com/fzi-forschungszentrum-informatik/PRIVACY-AVARE