Towards Transparency in the Internet of Things

Stephan Escher(✉), Benjamin Weller, Stefan Köpsell, and Thorsten Strufe

TU Dresden, Dresden, Germany
{stephan.escher,benjamin.weller,stefan.kopsell,
thorsten.strufe}@tu-dresden.de

Abstract. The establishment of IoT devices in all areas of public and private life raises, besides many new possibilities, also a number of new privacy issues. In particular, the establishment of almost invisible audio-visual sensors, like in smart speakers or smart cars, affects not only the user who purchases these IoT devices, but all those who are within the recording radius of them. At present, it is almost impossible for such uninvolved users to recognize all the surrounding recording IoT devices and their data processing, let alone object to this recording. This means, there currently is exclusively foreign control of the personal data of bystanders. Therefore we present our work in progress, to get towards transparency about the capturing and processing of audiovisual data by surrounding IoT devices one step closer. In this we assume that in the future such devices will have to identify themselves and their respective privacy policies. We have implemented a first prototype of our concept and show the need of such transparency solution by pre-evaluating it.

Keywords: Internet of Things · Transparency Enhancing Tools · Privacy · Biometric data

1 Introduction

Visions of ubiquitous computing and the Internet of Things (IoT) have existed since the end of the 20th century [15]. Today, these visions are turning into reality. Small, unobtrusive and networked sensors that measure and monitor their environment or users are continuously integrated into all types of physical objects, thereafter called smart devices. This development enables many new possibilities and increased efficiency, for example in mobility (self-driving cars), in energy supply (smart meters), in production (smart manufacturing), in medicine (mHealth) or in home automation (smart home).

The integration of IoT devices in all areas of public and private life, however, also raises a number of new privacy issues, especially in terms of unnoticed, ubiquitous data capturing that people cannot escape. The reason for this is that with the sensors becoming invisible, the data acquisition, transfer, processing and storage remain invisible to the user at the same time. In particular, the

L. Antunes et al. (Eds.): APF 2020, LNCS 12121, pp. 186–200, 2020.
https://doi.org/10.1007/978-3-030-55196-4_11

constant capturing and processing of *acoustic and visual signals*, e.g. through cameras and microphones in smart home devices, augmented reality glasses or smart cars[1], affects not only the user who purchases these IoT devices, but all those who are within the recording radius of them. May the owner of such devices still be informed about terms of use and data protection declarations when purchasing or setting up these devices, the independent user who is now constantly surrounded by these devices, currently has no possibility to intervene against the recording of his personal data. It is probably even impossible to just recognize all devices and their functionalities, let alone the involved companies and related privacy policies. There currently is exclusively foreign control of the personal data of bystanders, interference is hard, giving consent difficult, and being informed about its ramifications impossible, in consequence.

Therefore in this paper we want to present our work in progress to get towards transparency about audiovisual data capturing and processing in the world of the Internet of Things. The aim is to develop a concept that informs the user transparently and comprehensibly about the current situation regarding nearby devices with audio and/or video recording functionality, i.e. the possible recording of biometric data such as voice or face, as well as their processing and storage, and to evaluate this solution with the user according to its comprehensibility and usefulness.

2 Related Work

To design a suitable transparency solution for such audiovisual devices, first of all several challenges have to be considered:

1. How can such recording devices be recognized?
2. How could the information about data processing be transmitted to the user?
3. Which information should be transmitted?
4. How could transmitted information be presented in an understandable way?

Therefore, in the following, we take a closer look at state-of-the-art solutions for these questions.

2.1 Detecting Recording Devices

To be able to give the user a transparent overview of his environment, first of all, surrounding audiovisual capturing IoT devices have to be detected. On the one hand this could be done using technical approaches. Possibilities are for example object detection via augmented reality glasses or by wireless traffic pattern analysis [3]. However such technical approaches only work for certain recording devices, cannot give a complete overview and are therefore not suitable for daily usage.

[1] github.com/tevora-threat/scout.

Another approach is the assumption of regulation of IoT devices. Several proposals have been made out of mostly ethical reasons, to give people the possibility of being informed, and thus can allow or deny access to their personal information [6,8,14]. In 2018, the EU settled on the General Data Protection Regulation (GDPR) [1]. One of its main goals is the protection of natural persons in regard to their personal data. Article 13[2] states, that if personal data is collected from a data subject, they shall be provided with information about the data controller as well as insights into data processing and storage. Recent studies base their work on the assumption of regulation due to the GDPR [2,5,11] which mostly means, that IoT devices need to make themselves noticeable, e.g. through some kind of broadcast signal. In contrast, other work questions whether the GDPR alone may not be concise enough to deal with the complexity of IoT yet, due to the imbalance between data controller (the person owning the recording device) and data processor (the company, which handles the processing of the data) [10].

2.2 Information Transmission

If we assume that the identification of such IoT devices is regulated, we need a channel to transmit the information about data collection and processing to the user. On the one hand, this can be implemented analogously, like current warning signs for video surveillance in public areas (e.g. regulated in Germany through BDSG[3]). For example, the data controller (owner of the device) could offer a sign for possible data acquisition, as in their smart home, or the data processor/manufacturer could integrate a light signal in the IoT device that visualizes active data acquisition. However, we argue that such analogues information transmission is not suitable for the dynamic IoT world. Such concepts would lack on information, are not suitable for mobile IoT devices, flexible and adaptable.

On the other hand, the information transmission could be done via a digital communication channel. Such a channel could be either direct or indirect [11]. Using *direct communication*, a channel between the IoT device and a user device (e.g. smart phone) is constructed whenever they are in range. Therefore the IoT devices reveal themselves via broadcasting all needed information (e.g. recorded data type, range, privacy policies etc.). Alternatively, an identification number is transmitted, and additional information is queried via an external database. The user devices listen on this channel and display the information to the user.

Langheinrich proposed one of the first transparency systems for IoT [8]. For audiovisual data recordings, which he calls *active policy announcement*, he proposes a *privacy beacon*, which communicates with the user device over a short-ranged wireless link. Thereby a service id is transmitted to the user device, which will in turn communicate with a service proxy on the network to request the privacy policy. Several technologies for the communication between IoT and user

[2] gdpr.eu/article-13-personal-data-collected/.
[3] www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0044.

device are proposed, such as Infrared, Bluetooth, Wireless LAN, and ZigBee. His decision to use infrared was also due to the fact, that the technology was readily available in then-common PDAs.

Morel et al. describe another design of a transparency and consent system for IoT [11]. Similarly to Langheinrich, they use a direct communication between IoT and user device. As the communication channel, Bluetooth Low Energy (BLE) is proposed over alternative short-ranged wireless technologies, due to high availability in today-commonplace smartphones, and privacy benefits due to no involvement of other systems. IoT devices are enhanced with a *Privacy Beacon*, which is responsible for the declaration of this device. Beacons use *advertisement packets* (a specification of BLE), which are able to carry data, and sent out as a broadcast in set intervals. All information required by the GDPR is transmitted using the advertisement packets.

In contrast, Das et al. offer a solution for transparency and consent tracking in IoT, using an *indirect communication* setup [5]. For this, they introduce IoT Resource Registries (IRR), where IoT devices are registered and their privacy policies are held. They decided to use an indirect approach for openness and scalability. IoT device owners are expected to register their device in the local IRR. A *Personalized Privacy Assistant* (PPA) is proposed as a smartphone app, which queries the local IRR and notifies the user about functionality, position, privacy policy etc. of surrounding IoT devices. The PPA is designed with mobile app privacy preferences in mind. In their implementation, the user devices detect specific WiFi access points and Bluetooth beacons to determine the location of the user.

If we consider the time of transparency relative to the time of data collection and processing, transparency solutions could be distinguish between Ex Ante (transparency before data collection) and Ex Post/Real-time (after/during data collection) [16]. Thereby direct communication only allows real-time transparency since the user is informed when he is already in range of data capturing, indirect communication on the other hand is conceivable to achieve ex-ante transparency, but the implementation for mobile IoT devices is more difficult.

2.3 Information Content

Next we have to think about the information which has to be transmitted to the user. The GDPR requires, that the data subject must be informed about the processing of their personal data by the data controller. Such information includes, but is not limited to, identity and contact details of the data controller, purposes of the processing, recipients, data retention time, as well as information regarding rectification and erasure of personal data. Morel et al. [11] represent the point of view, that position and range of the IoT device should be included as well, to make the given information more contextual.

Further, we argue, that for IoT transparency even the information about the data processor are almost more important than about the data controller, cause in most cases the data controller (the one who deploys the IoT device) does

not have complete control over the data process owed to the current design of IoT devices. This means there are multiple responsible actors which should be considered.

For transparency it could also be interesting, next to explicit information about data processing, to think about predicted data, especially in the field of biometric data, where sensitive data could potentially be inferred, such as the health status of the user [4].

Depending on the information which is transmitted, additional privacy issues concerning the device owners have to be addressed. As already said, the data controller has to provide information regarding the circumstances and processing of personal data. Whenever a data controller broadcasts data, information about them is inevitably leaked, e.g. about available devices in his smart home, device types or traces of his movement via mobile IoT devices. The more specific the transmitted information becomes, the higher the risk for the device owner.

2.4 Information Visualization

If the content is determined the information has to be presented to the user understandable and intuitive. Since IoT devices are ubiquitous, the transparency solution must also be omnipresent. Therefore the solution needs to be unobtrusive enough and must provide a usable interface in an everyday scenario without overwhelming the user. This has to be kept in mind when designing user interfaces (UIs) and experience (UX). Research on application use in everyday situations reflects this [6,8,9,14]. These can be combined with general usability paradigms (e.g. by Krug [7]) to achieve a well-integrated UI and UX. Further, not every bit of information needs to be immediately presented, as user interfaces rely on comprehensibility and ease of use [7].

In addition to a UI that can be used daily, the information transmitted must also be easily accessible and quickly understood. It is conceivable that most users do not want to constantly read privacy policies about nearby IoT devices in their daily routine. Therefore most Transparency Enhancing Tools abstract and simplify the information [12]. Thus, various projects aim to make privacy policies more accessible and easier to understand. *ToS;DR*[4], for example, is an initiative, which grades websites and companies according to their privacy policies. They define various aspects of user privacy from which a final *privacy grade* is derived. The websites or companies are then classified by marks from A (best) to E (worst privacy practices). *DuckDuckGo Privacy Essentials*[5] is an extension for web browsers, which utilizes the ToS;DR framework and further extends the rating with the presence of connection encryption and integrated tracking networks of the website. In this way, the user receives a quick, comprehensible and unobtrusive indication of the current privacy situation when visiting the website. Others attempt to simplify the individual provisions of a privacy policy, such as the mozilla privacy icons project[6], which has created icons for privacy policy

[4] tosdr.org.
[5] duckduckgo.com/app.
[6] wiki.mozilla.org/Privacy_Icons.

settings such as the retention period to provide a quick and understandable view of ongoing data processing without reading the full privacy policy. Related work in this area is thereby mainly focused on web browsing or mobile app usage [12]. For IoT transparency their has to be done additional work, cause additional information could be important, like the usage of a wake-up word (like "Alexa") before data processing or local processing of biometric data (e.g. transcription of voice directly on the IoT device). Of course, simplification also leads to a loss of information, which must be taken into account when developing a transparency solution, i.e. weighing up between functionality and usability.

3 An Audit TET for IoT

In the following we want to present our work in progress of the development of an audit TET (Transparency Enhancing Tool) for IoT devices. Audit TET means thereby the transparent visualization of insights into data capturing, processing and storage at realtime without the possibility of interaction [16].

3.1 Information Transmission

Similar to related work, we assume a regulation of audiovisual IoT devices, which means that they have to identify themselves through some kind of broadcast signal. Due to the low energy consumption, the generally suitable range and the high availability in current mobile user devices, we have, like Morel et al. [11], decided to use a direct and digital BLE communication channel to transfer information from the IoT device to the user device. The main idea is that an IoT device continuously broadcasts a specific ID via BLE advertising mode whereas the user device is in scanning mode. The scan interval should be configurable, so that the user can weigh up the actuality of the transparency against the battery life of his device, or update the transparency status manually. If the device of the user receives such an ID, a database is queried anonymously, where the information about data capturing, processing, etc. has been deposited. The separate database is useful to be able to react flexibly to changes in data protection guidelines of IoT devices or legal requirements. After retrieving the information, the user device can directly inform the user about the current situation regarding nearby recording devices and their characteristics.

For the daily use of this transparency solution, our approach for notification and visualization is to support user devices that are directly accessible, i.e. wearables like smart watches or smart glasses. Thus, the user can be informed quickly and efficiently without being torn from his activities. For the concrete implementation, the user's smart phone would take over the scanning mode, query correlating information when devices are detected and then display a notification and/or forward important information to a wearable of the user. The whole communication setup is shown in Fig. 1.

Challenges for this communication setup are on the one hand to adjust the range of the BLE communication to the real recording range of the device and on

the other hand the increased energy consumption especially for mobile IoT and user devices. Furthermore, users without a mobile user device still have no transparent overview of their current data recording. Fast moving IoT devices, such as integrated cameras of a smart car, might not be noticeable by the recorded user as they may not be able to react fast enough.

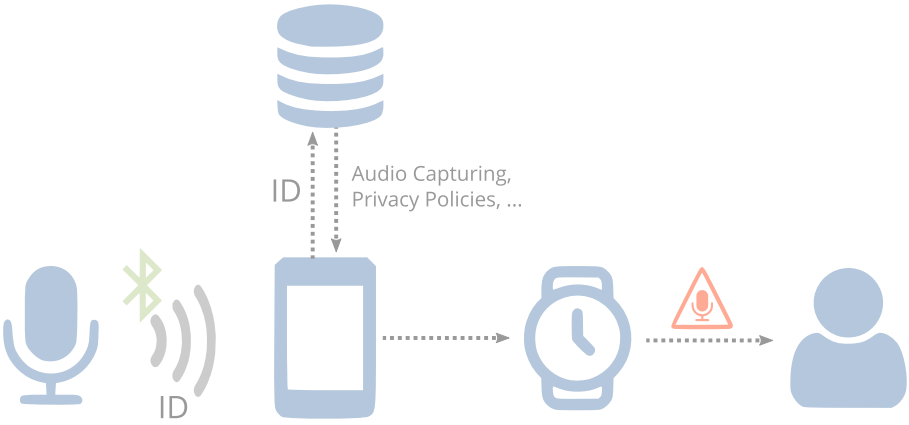

Fig. 1. Communication setup for transparency solution

3.2 Information Content

Transmitted content should at the best entail information and privacy policies about the data controller (the IoT device holder) as well as the data processor (the company which processes the data). For our first concept we focus on information about the nearby IoT device itself (device type, recording channel, ...) as well as the privacy policies of the specific data processor and exclude the data controller for now. Our scenario provides for the data processor to embed a BLE beacon with a corresponding transmission ID into the IoT device during production, and then to enter information about this ID (device type, range, recording channel, privacy policies, erasure etc.) into a corresponding database. The handling of the data controller is much more difficult, but has to be considered in future, because they of course have also (in part) access to the data, even though most of them probably have no idea how to handle them.

3.3 Information Visualization

In order to provide the user with an overview of nearby recording devices in a quick and understandable way, we have decided to use a hierarchical visualization structure.

The first level represents the corresponding device type respective *recording channel*, i.e. audio or video recording, and the number of devices of each type in

the vicinity. This level corresponds to the well-known traditional warning signs (e.g. for video surveillance) and should always be accessible, e.g. as a notification of the smart phone or as a icon on the smart watch, in order to get a quick and transparent overview of which type of biometric data could be captured.

For more information the 2nd layer shows the IoT device type (e.g. smart speaker or smart tv) per recording category and the 3rd layer shows the device model and/or manufacturer of the specific IoT device (e.g. Amazon echo) and its specific privacy policies. Dependent on the device type (e.g. AR glasses) it is possible that also third party applications could have access to the capturing interface. Therefore additional application-based information has to be shared (4th layer) about the data processing of this third party apps involving their additional privacy policies. However, this layer cannot be realized with the separate database but the information has to be sent directly by the IoT device.

As already mentioned in Sect. 2.3, the lower the layer, the more details can be presented to the user, but they also carry a higher privacy risk for the IoT device owners.

Further, instead of simply linking the privacy policies of the data processor we want to simplify them and make them easier to understand, based on the work mentioned in Sect. 2.4 (see also Sect. 3.6).

3.4 A First Prototype

We decided to use a Fitbit smart watch for the first prototypical implementation, since our focus lies on wearable as the user device. These watches mainly function as fitness trackers, but offer high customizability of the user interface in a simple way. To be more specific, the whole UI is represented by HTML, CSS and JavaScript. For this work, we used a "Fitbit Ionic".

Regarding the detection of smart devices, we chose the approach of a mock-up of the communication between smart device and watch app. Fitbit watches allow for remote shell access, and thus a change on the device can be triggered remotely in real-time.

For our prototype, we implemented layer 1 (represents recording channel, e.g. audio/video) and layer 3 (represents specific device information) of our information hierarchy. The UI is shown in Fig. 2. The left and middle image represents the default watch face, showing time and 2 *complications*. Complications are small badges, holding a specific part of information, which is usually represented with text and an icon.

The leftmost image shows the privacy state of the user. This is conveyed through a dashed eye icon, and enriched with a corresponding text denoting "private". The complication is also tinted in green, using a well-known color to indicate a good situation. The middle image shows an ear, as well as the text "Audio", showing that there might be devices **listening** to the user. For this, the typical warning color yellow is used. Using these colors, the privacy state is preliminary classified.

To convey the clickability of the complications, the privacy complication and the step counter can be tapped. The popup by tapping the privacy complication

Fig. 2. First smart watch prototype

is shown on the rightmost image. To make the concept of complications more intuitive, we decided to include a footstep counter as the right complication.

The popup consists of a short text describing the found smart device, i.e. its name. Additionally, a button allows for the user to request more information about the device. If it is tapped, the connected smartphone shows additional information about the device, e.g. data retention time, recording channel or whether it is activated with a wake word.

3.5 Pre-evaluation

To gain a first impression of the usefulness, we presented our solution to a group of 18 users (see Table 1) at the Dresden Science Night[7] and had them evaluate it.

Table 1. Overview of the participants

Age	10–20	20–30	30–40	40–50	50–60
Count	5	5	2	4	2

For this purpose, a booth was set up with an IoT sample device (Amazon Echo) and the implemented smart watch TET solution. The project was explained to the visitors and they could try out both the Amazon Echo and the smart watch. When the Amazon Echo was activated, the communication channel was also triggered and the transparency display of the smart watch visualized an audio recording device nearby. In addition, the user was prompted to visit different rooms, making the change in state of the transparency solution practically visible when leaving and entering the exhibition space. After the practical evaluation, the users were asked to fill out a small survey.

[7] www.wissenschaftsnacht-dresden.de.

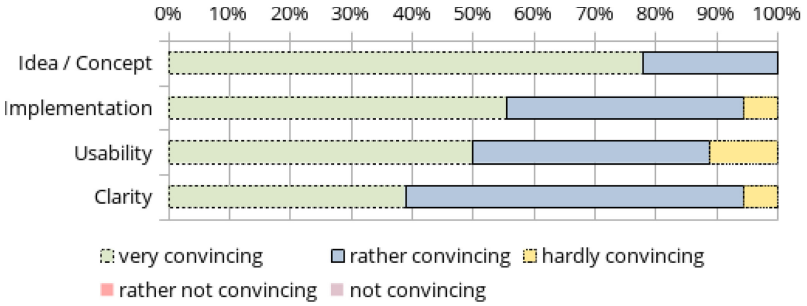

Fig. 3. Pre-evaluation of our TET solution by 18 test persons.

The overall feedback regarding the transparency solution developed was very positive (see Fig. 3). Especially the overall concept of the solution was felt to be very useful. In addition, 95 % of the test persons stated that they wanted to use this solution in daily life. More than half (59 %) of them said that they had already found themselves in a situation where the app would have been useful. The deficiencies in implementation, usability and comprehensibility were mainly due to the fact that many of the test persons wore a smart watch for the first time. In this regard, the implementation of the transparency solution for smart phones was started, which would also be preferred by most of the test persons (see Fig. 4).

Suggestions for improvements and remarks were in particular a desired control of the own data (e.g. by integrated switch-off function), as well as a listing of the range of the device located nearby. Furthermore different design suggestions were introduced.

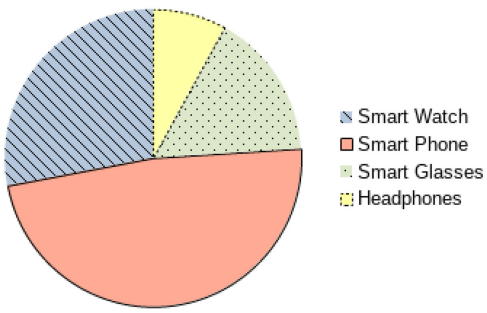

Fig. 4. Which device would you prefer for the transparent presentation?

3.6 Extending the Prototype

Based on the pre-evaluation we have started to expand our transparency solution.

First, as already mentioned, we started an implementation for smart phones based on Android. We integrated all levels of information (except third party applications). Figure 5 shows level 1 to 3 of the information hierarchy.

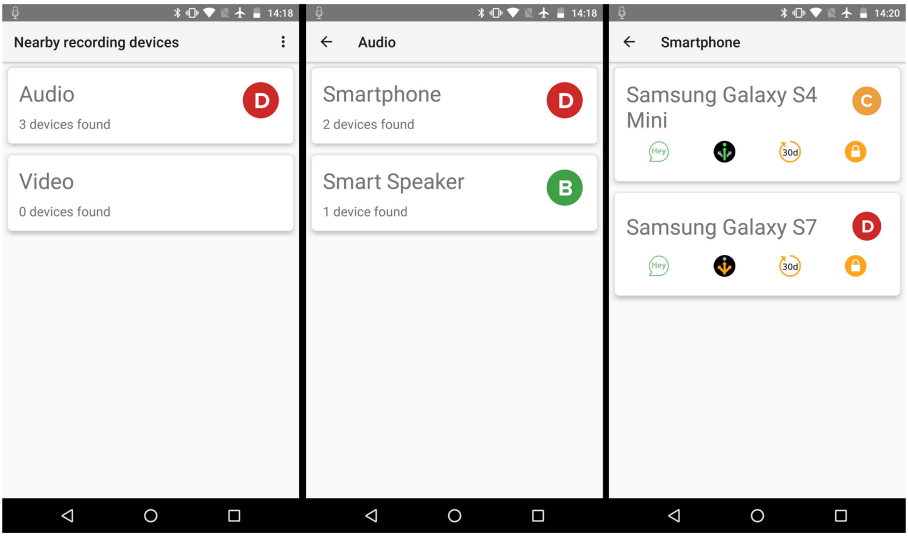

Fig. 5. Smart phone implementation (ltr: level 1, level 2, level 3)

The first layer is the main view, where the second layer can be accessed by clicking "Audio" or "Video". Layer 3 can be accessed by layer 2 respectively. Additionally, information of layer 1 is shown as a notification with a text and corresponding icon to allow for a quick overview of the users' privacy situation (see left image of Fig. 7).

The icons set were changed since it turned out during our pre-evaluation that they were partly ambiguous. Current icons representing the privacy state were chosen to be concise, and easily understandable: A mask represents no nearby recording devices, microphone represents only audio processing devices, eye respectively for video devices, and microphone and eye combined if audio and video processing devices are present.

Second we expand the smart watch solution for Wear OS devices. The implementation of the smart watch is shown in Fig. 6. Similarly to the pre-evaluation, a complication provides a quick overview of the current privacy state. The leftmost image shows a private state, without any recording devices nearby, whereas the middle image shows 3 recording devices nearby, with all being audio processing devices and no video processing devices. On click, the view on the right

Fig. 6. Wear OS implementation

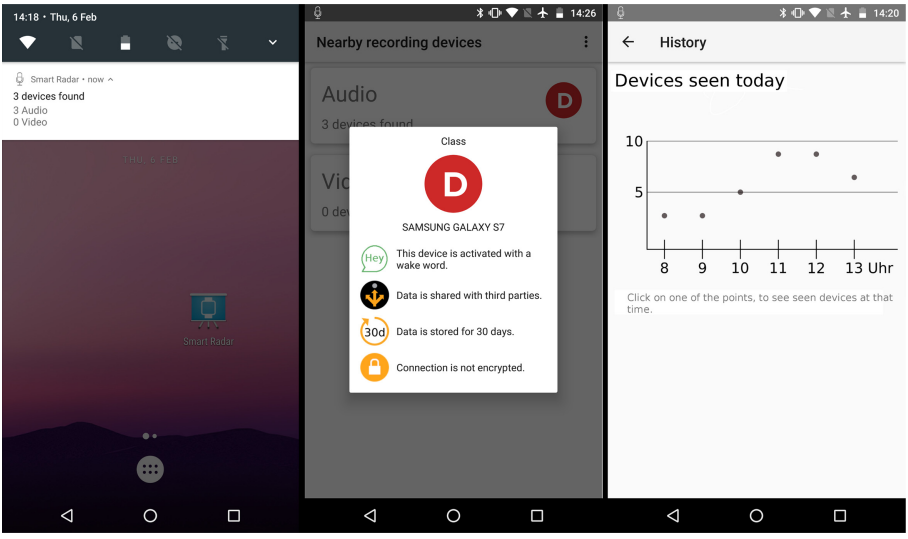

Fig. 7. Smart phone implementation (ltr: notification, popup view, history view)

image is shown, where the first information level is visualized, as well as the worst processing device from a privacy perspective and whether the device is always recording or is waiting for a wake word. Changes in the smartphone app are instantly reflected in the watch app.

The communication structure is implemented as shown in Fig. 1. The IoT-device broadcasts information using BLE GAP (Generic Access Profile), which defines the **central** and **peripheral** role. GAP offers 5 link layer states: Advertising, Scanning, Standby, Initiating and Connection. The advertising mode features 2 possible methods for inter-device communication: Advertising packets and Scan Response packets. The former can be sent in an interval from 20 ms to 10.24 s, and can contain up to 31 bytes of payload. IoT-devices use the peripheral role and broadcast information using this advertising packets, using an interval

of 1 s. Advertising data contain an ID, which reflects device parameters and associated privacy policies.

User devices use the scanning mode to receive such broadcasts. Due to the short advertising interval, devices are detected in real-time. If data is received, the payload of the advertisement packet is extracted. Then, the included ID is queried in a database, which returns the privacy parameters of this IoT-device. We implemented this communication channel using separate bluetooth dongles from Nordic Semiconductor.

Further to simplify and visualize the important privacy parameters of the specific IoT-device we integrated icons from the Mozilla privacy icon project, as well as choosing icons which are more concise. To achieve an effective transparency solution, the presentation has to be adjusted to take the circumstances of IoT into account, like the activation of data capturing through a wake-up word. Furthermore we mock-up a scoring system (grades from A to F), similar to DuckDuckGo Privacy Essentials, to give the user a possibility of a quick assessment of their current privacy situation. The worst data processing from a privacy perspective will be displayed at the highest information level (shown on smart watch and smartphone level 1), to achieve a sense of awareness, as well as providing a quick overview of the privacy state. A tap action on such a privacy class leads to a popup, which explains the reason for the rating (see middle image in Fig. 7).

Additionally, the amount of found devices is recorded and presented in a history view (see right image in Fig. 7). There, users can reflect on their privacy situation over the past day, which also may help to raise awareness about IoT-devices in everyday situations. Individual points can be tapped, to reveal the devices which were found at this specific time.

4 Outlook

Continuing after completion of the development we will evaluate the solution to get answers to acceptability (is transparency important to the user), to usability and comprehensibility (is the visualization understood), to information requirements with regard to privacy issues for the device holder (what information is important to users), as well as to the impact of transparency in IoT to the user (do users feel better or worse if they can perceive their surrounding capturing devices, do they change their behavior).

Further UI design decisions should be carefully evaluated, as an evaluation in a clinical setting may not reflect the usage and usability of the tool in an everyday scenario, similar to the privacy paradox [13].

In addition, we are working on the rating system and the visualization/simplification of privacy policy parameters, which are better adapted to the IoT world and further, have to be evaluated.

Finally, we are working on concepts for integrating user-related interaction (opt-in/opt-out) to extend the audit TET to an interaction TET and thus give the user the opportunity for informed consent. Some concepts on interaction

with IoT-devices in an everyday scenario have already been proposed [6,14]. This raises new challenges, as a connection has to be established between user device and IoT-device, where data regarding the consent of the user needs to be transmitted. This may include biometric data, e.g. a voice profile, enabling the IoT-device to filter specific information and to determine, how recorded information is to be processed.

5 Conclusion

Advancements in the Internet of Things introduces many positive aspects, such as alleviated life and efficiency, e.g. in mobility, energy supply or production. The integration of IoT-devices in all areas of public and private life, however, also raises a number of new privacy issues, especially in terms of unnoticed, ubiquitous data capturing that people cannot escape. May the owner of such devices still be informed about terms of use and data protection declarations, the independent user who is now constantly surrounded by these unobtrusively IoT-devices, does not even have the possibility to recognize them. Therefore in this paper we presented our work in progress for a first concept towards transparency in IoT, with focus on IoT-devices which capture acoustic and visual signals and thereby biometric data. Under the assumption of regulation, we define several challenges which a Transparency Enhancing Tool shall fulfill in order to be usable in an everyday scenario. A first prototype for a smart watch was then derived, which we tested at the Dresden Science Night. Visitors were able to try out the tool and voice their opinions and usability suggestions. The concept was well received, and thus we developed an extended implementation based on their feedback. Since many test persons stated interest in a smartphone app, the implementation is developed for watches and phones. Additionally, to support understandability and ease of use, given information is enriched with a classification of the users' current privacy state, depending on the privacy policies of surrounding IoT-devices.

References

1. General data protection regulation (2018). https://gdpr.eu/. Accessed on 02 Apr 2020
2. Castelluccia, C., Cunche, M., Le Metayer, D., Morel, V.: Enhancing transparency and consent in the IoT. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 116–119. IEEE (2018)
3. Cheng, Y., Ji, X., Lu, T., Xu, W.: DeWiCam: detecting hidden wireless cameras via smartphones. In: Proceedings of ASIACCS 2018 (2018)
4. Cohn, J.F., et al.: Detecting depression from facial actions and vocal prosody. In: 2009 3rd International Conference on Affective Computing and Intelligent Interaction and Workshops (2009)
5. Das, A., Degeling, M., Smullen, D., Sadeh, N.: Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. IEEE Pervasive Comput. **17**, 12 (2018)

6. Gomer, R., Schraefel, M.C., Gerding, E.: Consenting agents: semi-autonomous interactions for ubiquitous consent. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication - UbiComp 2014 Adjunct, pp. 653–658 (2014)
7. Krug, S.: Don't Make Me Think. A Common Sense Approach to Web Usability. Revisited. New Riders, Thousand Oaks (2014)
8. Langheinrich, M.: Personal privacy in ubiquitous computing: tools and system support. Ph.D. thesis, ETH Zurich (2005)
9. Lederer, S., Hong, J.I., Dey, A.K., Landay, J.A.: Personal privacy through understanding and action: five pitfalls for designers. Pers. Ubiquit. Comput. **8**, 440–454 (2004)
10. Lindqvist, J.: New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? Int. J. Law Inf. Technol. **26**, 45–63 (2018)
11. Morel, V., Cunche, M., Le Metayer, D.: A generic information and consent framework for the IoT. In: 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 366–373. IEEE (2019)
12. Murmann, P., Fischer-Hübner, S.: Tools for achieving usable ex post transparency: a survey. IEEE Access **5**, 22965–22991 (2017)
13. Norberg, P.A., Horne, D.R., Horne, D.A.: The privacy paradox: personal information disclosure intentions versus behaviors. J. Cons. Aff. **41**, 100–126 (2007)
14. Wegdam, M., Plas, D.J.: Empowering users to control their privacy in context-aware systems through interactive consent. CTIT Technical report Series, p. 10 (2008)
15. Weiser, M.: The Computer for the 21st Century, p. 13. Scientific American, New York (1991)
16. Zimmermann, C.: A categorization of transparency-enhancing technologies. arXiv (2015)