Enhancing Transparency and Consent in the IoT

Claude Castelluccia, Mathieu Cunche, Daniel Le Métayer, Victor Morel

Enhancing Transparency and Consent in the IoT

Claude Castelluccia
Inria
Grenoble, France
claude.castelluccia@inria.fr

Mathieu Cunche
INSA Lyon, Inria
Lyon, France
mathieu.cunche@insa-lyon.fr

Daniel Le Métayer
Inria
Lyon, France
daniel.le-metayer@inria.fr

Victor Morel
Inria
Lyon, France
victor.morel@inria.fr

***Abstract*—The development of the IoT raises specific questions in terms of privacy, especially with respect to information to users and consent. We argue that (1) all necessary information about collected data and the collecting devices should be communicated electronically to all data subjects in their range and (2) data subjects should be able to reply also electronically and express their own privacy choices. In this position paper, we take some examples of technologies and initiatives to illustrate our position (including direct and registry-based communications) and discuss them in the light of the GDPR and the WP29 recommendations.**

***Index Terms*—privacy, IoT, transparency, consent, GDPR, regulation**

I. Introduction

The development of the IoT raises specific privacy issues especially with respect to information and consent. Data subjects are surrounded by a growing number of objects discretely collecting/processing information about them and sending it to unknown third parties. The current situation is far from satisfactory :

- As far as user information is concerned, solutions such as stickers or wall signs are not effective since they remain unnoticed from most data subjects.
- As far as consent is concerned, data subjects do not have simple means to communicate with data controllers and express their privacy preferences.

Furthermore, most of the devices used to collect data in IoT environments have scarce resources; some of them do not have any user interface, are battery-operated or/and are passive (they collect data but do not emit any signal). In addition, their costs should remain as low as possible, which places further constraints on any technical solution.

The General Data Protection Regulation (GDPR) [10] puts emphasis on the control of data subjects over their personal data. Its application to the IoT is not obvious though. The WP29 has published guidelines on transparency [16] and consent [15] and an opinion on the development of the IoT [14]. Starting from these recommendations, we discuss the specific challenges raised by the IoT in terms of transparency and consent, and suggest combinations of technical and regulatory instruments to address them.

In a nutshell, our position is that :

1) All necessary information about data collecting devices (including mandatory information such as their existence, data collected, associated privacy policies, but also their location and range) should be communicated electronically to all data subjects in their range.
2) Data subjects should be able to reply, also electronically, to express their own privacy choices.
3) The above communications could either be direct or be implemented through registries, such as servers, from which relevant information can be retrieved.

We argue, in this paper, that:

- The above solutions are technically feasible, at a reasonable cost.
- It is of prime importance that the above solutions are implemented in a secure and privacy-preserving way. For example, the declarations of the data subjects and their interactions with the registries should not entail additional privacy risk.
- The effectiveness of these solutions depends also on organizational and regulatory measures. For example, data controllers deploying or using IoT devices must have the legal obligation to declare their devices (with the required information) and announce them to users. Furthermore, audits should be conducted by independent third parties to check their compliance. Ideally, registries should be under the control of independent trusted third parties[1]. These solutions also require a standardization effort (e.g. about the protocol used to declare devices and the language used to express privacy policies, etc.).

In this paper, we discuss our position in the light of the GDPR and the WP29 recommendations (Section II). We also provide some examples of technologies and initiatives that illustrate different implementation options for transparency (Section III) and consent (Section IV).

II. European Regulation and WP29 recommendations

Over the last decades, the idea that individuals should have an effective control over their personal data has become a key part of the EU position and strategy in the field of data protection. In many policy documents, control is advocated as an important tool for protecting privacy and achieving the empowerment of data subjects [7]. As an illustration, Recital

From *Proceedings of the International Workshop on Privacy Engineering*, IWPE2018, London, IEEE, April 2018.

[1]These trusted third parties could be certified by data protection authorities.

7 of the GDPR [10] states that "Natural persons should have control of their own personal data" and the current draft of the new ePrivacy Regulation refers to the right for natural and legal persons to "control electronic communications". Control is not defined precisely in the GDPR but it is backed up by a number of provisions, including enhanced obligations for data controllers in terms of transparency and consent.

The application of the GDPR requirements is not obvious though, especially in the context of the IoT. To facilitate their interpretation, the WP29 has recently published two guidelines on transparency [16] and consent [15]. The WP29 has also published two opinions which are relevant to this paper, on the development of the IoT [14] and on the draft ePrivacy Regulation [17] respectively.

As far as transparency is concerned, the GDPR defines the categories of information to be provided to data subjects (identity of the controller, purpose of the processing, categories of personal data concerned, recipients, etc.) and introduces some requirements on acceptable communication modes. Recital 39 states "The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used". According to the WP29, "the *easily accessible* element means that the data subject should not have to seek out the information; it should be immediately apparent to them where this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question." The WP29 also suggests that IoT devices have a QR code that can be scanned to display the transparency information. However, it is questionable whether informing data subjects through QR codes or signposting is consistent with the idea, also put forward by the WP29, that "the data subject must not have to take active steps to seek the information covered by these articles or to find it amongst other information". Our position is that all the required information should be communicated to data subjects in electronic form and without any effort on their part. Considering that IoT devices are by definition electronic objects collecting data from subjects, there is no reason why electronic means could not be used also to inform them. The implementation of this requirement may need some adjustments in the IoT infrascturure but they are not out of reach, neither from the technical point of view, nor from an economic standpoint, as discussed in the next sections.

The GDPR also defines a number of conditions for the validity of consent: it should be freely given, specific, informed and unambiguous. The third condition (information) was discussed in the previous section. The other conditions also raise new challenges in the context of IoT. For example, Recital 42 states that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment". In the context of IoT, this should entail that consent to physical tracking is not valid if the only alternative for the data subject is to turn off his WiFi and thereby be deprived of useful services. To ensure the lack of ambiguity, consent should, according to the GDPR, "be given by a clear affirmative act", which should exclude the collection of identifiers such as MAC addresses for example, without any affirmative action from the user. These issues are all the more important for data controllers given that the GDPR requires that they must be able to demonstrate that valid consent was obtained. As far as the IoT is concerned, the WP29 advocates the design of new consent mechanisms on the devices themselves, such as "privacy proxies"[2]. We agree that this is a key condition for the effective implementation of consent and discuss this further in the next sections.

III. Transparency

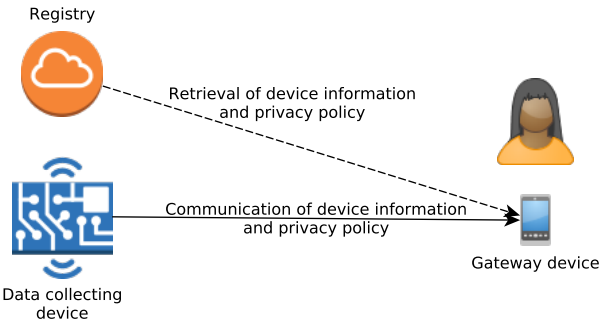

Fig. 1. Implementation of transparency

A. Direct declaration

A first option to implement transparency is through direct communications between data collecting devices and a device carried by the user such as a smartphone (acting as a *gateway* device). In this option ("direct declaration" in the sequel), data collecting devices use a communication channel to advertise their presence, capabilities and privacy policies within their area of operation. Direct declaration has two main benefits: (1) the locality of the communications reduces the risk of further tracking by a remote entity and (2) it does not require an Internet connectivity. It also raises several challenges :

- All devices should be able to declare themselves. Tracking systems involving passive devices thus need to be enhanced (for example with a beacon) to enable these declarations.
- The communication protocol should support the transmission of privacy policies.
- The communication range of the privacy policies should match the operational range of the system collecting data.
- The above features should be possible at reasonable cost and without disrupting existing services.

[2]"In practice, today, it seems that sensor devices are usually designed neither to provide information by themselves nor to provide a valid mechanism for getting the individual's consent. Yet, new ways of obtaining the user's valid consent should be considered by IoT stakeholders, including by implementing consent mechanisms through the devices themselves. Specific examples, like Privacy Proxies and Sticky Policies, are mentioned later in this document." [14]

Direct declaration can typically be implemented using medium and short range wireless communications technologies such as Wi-Fi and Bluetooth. Most gateway devices (smartphones) are equipped with these technologies and their range (typically several meters to tenths of meters) matches the scale of the area of operation of IoT systems. In addition, the protocols used by these technologies could be extended to include the transmission of privacy policies. Wi-Fi and Bluetooth technologies feature service discovery mechanisms that allow mutual detection and identification, and the exchange of detailed information about a system. In Wi-Fi, the access-point (AP) service discovery allows stations to detect APs through the transmission of advertising frames (beacons and probe requests/responses) prior to association. These frames are filled with Information Elements (IE) that are used to advertise information such as identifiers and supported capabilities [1, sec. 8.4.2]. These IEs could be used by data collectors to announce their presence, the type of data they collect and their privacy policies.

A more interactive mechanism is possible in Wi-Fi thanks to the Generic Advertisement Service (802.11u - GAS) protocol [5] which allows the exchange of application layer data prior to connection. The GAS protocol could be used to communicate information about privacy policies as suggested in [2]. The format could follow the approach used for Location Civic Report [13] used in 802.11 [1, sec. 7.3.4.12], which presents detailed location data in XML.

Bluetooth also features a service discovery protocol that can be used to enable direct declarations. For instance, a device can advertise its presence along with a short description through the advertising packets [12, Part C, sec. 11]. Similarly, the Attribute Protocol (ATT) protocol and the Generic Attribute Profile (GATT) specifications [12, Part A, sec. 6.4] can be used by connected devices to communicate information about available services. This information is organized in profiles, which are associated with an application (e.g. health care); new profiles could be defined for privacy policies.

Wi-Fi and Bluetooth based solutions can be deployed at low cost, as wireless beacons and nano-computers can currently be purchased for around 10-20 euros apiece[3]. In some cases the device is already equipped with a Wi-Fi or Bluetooth interface (for instance Wi-Fi and Bluetooth tracking systems), this extension is thus almost costless.

B. Registry-based solutions

Another option to implement transparency is to declare collecting devices through a registry. A registry is a database accessible through the internet, storing all relevant information about data collecting devices, including *inter alia* the location of data collecting devices, their range, their privacy policy, and all information required by law.

[3]A set of 3 Estimote Proximity beacons costs 48 euros https://estimote.com/products/; A naked Raspberry-Zero featuring Bluetooth and Wi-Fi interfaces costs less than 6 euros https://www.raspberrypi.org/products/raspberry-pi-zero/

Registries can be accessible before entering an IoT area via a website or through an application. They can provide information in both machine-readable and human-readable formats.

The implementation of registries raises several challenges:

- Data subjects must be aware of all surrounding devices. Therefore inconspicuous or difficult to access registries are not acceptable.
- Registries must be properly managed, up-to-date and accurate. Managing a registry can be achieved in different ways: it can be centralized or distributed, and contributions can be restricted to authenticated parties.

The Privacy Assistant project led by the Carnegie-Mellon University (CMU) is an example of use of registries to declare and retrieve privacy policies of IoT devices [11]. A prototype has been deployed on the CMU campus, where data subjects are able to locate cameras. Combined with an assistant on a mobile phone, subjects are warned about personal data collection in their vicinity. Another example is the Wombat system, discussed in the next section, which has been demonstrated recently in Paris within an exhibition called Terra Data presented at the *Cité des Sciences et de l'Industrie*. The goal of the search engine Thingful[4] is to provide visibility and interoperability to IoT through a representation of devices in a map. Although it does not provide transparency as required by the GDPR, Thingful shows that a visual and scalable way to provide transparency is possible.

IV. Consent

After detecting the presence of a collecting device, individuals should be able to object to data collection or to express their consent for a specific purpose, data retention delay, etc. ("privacy choices"). As for data controllers declarations in the previous section, privacy choices can be communicated by data subjects either directly or through a registry. For example, the Wi-Fi Information Elements discussed in the previous section can also be used to communicate privacy choices and the registry of the CMU Privacy Assistant project can also be used to store privacy choices. More elaborated communications may also involve bidirectional exchanges of information to enable iterative negotiation of consent.

An example of registry dedicated to the declaration privacy choices is the Smart Places[5] service proposed by the Future of Privacy Forum (FPF). Smart Places is a website on which a data subject can provide his Wi-Fi or Bluetooth MAC address, which will be blacklisted from the tracking systems controlled by companies participating. These companies also commit to comply with the FPF code of conduct [4].

The Wombat system is an example of local registry recording data subjects' privacy choices. This Wi-Fi tracking system collects MAC address of Wi-Fi devices and stored them temporarily. Visitors have the possibility to opt-out from the system by using a Wi-Fi based mechanism [9]. By associating

[4]http://thingful.net/

[5]https://smart-places.org/

his device to a dedicated Wi-Fi network named "*Pas de suivi wi-fi. Do not track*", the user notifies the system his opt-out decision; the network then records the MAC address of the device and adds it to a local Do-Not-Track (DNT) list. Once added to the DNT list, all information stored on the device is erased and no further information is collected from the device.

V. Conclusion

We believe that the adoption of the measures suggested in this paper would contribute to reduce the imbalance of powers between data controllers and data subjects without introducing prohibitive costs or unacceptable constraints for data controllers. The positions advocated here are in line with the spirit of the GDPR and the opinions of the WP29 while adopting on some aspects a more ambitious interpretation of the implementation of transparency and consent. For example, the WP29 states that "appropriate measure for providing transparency information in the case of data controllers who maintain a digital/online presence, is to do so through an electronic privacy statement/ notice." However, the WP29 still finds acceptable to inform data subjects through other means such as "public signage" or "visible boards" for "real-life environments". It is doubtful whether such communication modes would pass the effectiveness testing suggested by the WP29 itself[6].

Another key issue which is alluded to in the WP29 opinions is the need to avoid "user fatigue" [14], [15], which typically leads to situations in which information is not read and consent is provided through reflex clicks by annoyed users. One way to avoid this problem would be to rely on privacy proxies or privacy agents [6], [8]. A privacy agent is defined in [8] as a software component offering two essential functionalities: (1) a user interface dedicated to the interactions with the data subject, typically to allow him to define his privacy choices and (2) a data manager controlling the disclosure of his personal data based on his choices and the declarations of the data controllers. Privacy agents can be seen as a generalized version of the Do Not Track mechanisms which makes it possible to fulfill the choices of the data subjects in a non disruptive way, without repeated requests for approval. The WP29 seems to be promoting this solution [14]. However, it is not clear whether the conditions put forward by the WP29 for the validity of consent [15] are compatible with this approach. For example, the WP29 stresses that consent should "name controllers", which would exclude a generic form of consent expressed by reference to a purpose such as, for example, counting the number of people in a store, without naming a specific data controller. The stance of the WP29 on this point needs to be clarified.

The proposals made in this paper are also very relevant to the ongoing discussions about the future ePrivacy Regulation [3]. As stated by the WP29 [17], the current draft "gives the impression that organisations may collect information emitted by terminal equipment to track the physical movements of individuals (such as WiFi-tracking or Bluetooth-tracking) without the consent of the individual concerned.". If the text were adopted with this wording, this would clearly be in contradiction with the GDPR. This would be all the more unacceptable that, as discussed in this paper, solutions can be developed to make information and consent more effective, without introducing excessive constraints neither for data controllers nor for data subjects.

[6] "Controllers can demonstrate their compliance with the transparency principle by testing the intelligibility of the information and effectiveness of user interfaces/ notices/ policies etc. through user panels." [16]

References

[1] 802.11-2012 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pages 1–2793, March 2012.

[2] John Michael Croft. *Wi-Fi service discovery over 802.11 u using non-native generic advertising services (GAS-SD)*. Master Thesis, University of Texas at Austin, 2014.

[3] European Commission. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), January 2017.

[4] Future of Privacy Forum. Mobile Location Analytics Code of Conduct. Technical report, Future of Privacy Forum, October 2013.

[5] IEEE Computer Society, LAN/MAN Standards Committee, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board. *IEEE standard for information technology telecommunications and information exchange between systems– local and metropolitan area networks– specific requirements. Part II, Amendment 9, Part II, Amendment 9,*. Institute of Electrical and Electronics Engineers, New York, 2011.

[6] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proceedings of the Ubicomp Conference*, volume 2498, pages 237–245. Springer Verlag, LNCS, 2002.

[7] Christophe Lazaro and Daniel Le Métayer. Control over personal data: true remedy or fairy tale ? In *SCRIPTed*, volume 12:1, 2015.

[8] Daniel Le Métayer. A formal privacy management framework. In *Proceedings of the Formal Aspects in Security and Trust Conference (FAST)*, volume 5491, pages 162–176. Springer Verlag, LNCS, 2009.

[9] Célestin Matte and Mathieu Cunche. Wombat: An experimental Wi-Fi tracking system. In *8e édition de l'Atelier sur la Protection de la Vie Privée (APVP)*, Correncon, France, July 2017.

[10] Official Journal of the European Union. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), May 2016.

[11] Norman Sadeh. A Privacy Assistant for the Internet of Things, 2017.

[12] Bluetooth SIG. *Specification of the Bluetooth System v5.0*. Version, December 2016.

[13] M. Thomson and J. Winterbottom. Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO). RFC 5139 (Proposed Standard), February 2008.

[14] WP29. Opinion 8/2014 on Recent Developments on the Internet of Things, 2014.

[15] WP29. Guidelines on Consent under Regulation 2016/679, November 2017.

[16] WP29. Guidelines on transparency under Regulation 2016/679, December 2017.

[17] WP29. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), December 2017.