ANALYZING THE PRIVACY AND SECURITY IMPLICATIONS OF HOUSEHOLD CLEANING DEVICES THROUGH THE ARCHITECTURE OF IOT

Sabine Prossnegg / Veronika Beimrohr / Gerhard Seuchter / Klaus Gebeshuber

Senior Lecturer, FH JOANNEUM University of Applied Sciences, Department of Applied Computer Sciences
Werk-VI-Straße 46, 8605 Kapfenberg, Sabine.Prossnegg@fh-joanneum.at

Legal Advisor, FH JOANNEUM University of Applied Sciences, Personnel and Legal Services
Alte Poststraße 147, 8020 Graz, Veronika.Beimrohr@fh-joanneum.at

Senior Lecturer, FH JOANNEUM University of Applied Sciences, Department of Applied Computer Sciences
Werk-VI-Straße 46, 8605 Kapfenberg, Gerhard.Seuchter@fh-joanneum.at

Associate Professor (FH) for IT-Security, FH JOANNEUM University of Applied Science,
Institute of Internet Technologies Applications
Werk-VI Straße 46, 8605 Kapfenberg, Klaus.Gebeshuber@fh-joanneum.at

Keywords: ***Internet of Things, IoT, privacy by design, data architecture, perception layer, networking layer, middleware layer, application layer, privacy, personal data, GDPR***

Abstract: *The Internet of Things (IoT) connects countless objects to the Internet. In a typical IoT system data is usually collected by end devices, transmitted through communication networks, processed by servers and finally provided to various applications. Thus personal data flows through a multi-layered, complex architecture. In order to protect the privacy of the persons using the IoT system protection is needed at every layer. Under the GDPR framework both privacy and security need to be ensured not only when processing personal data but already at an earlier stage, which means when products and services are designed. From that point of view privacy by architecture is first and foremost an engineering issue.*

1. Introduction

The Internet of Things is one manifestation of recent developments in information and communication technologies (ICT) that is closely linked to others like cloud computing, big data and even block chain technologies. Instead of going into theory about data protection and IoT, this contribution will approach the issue via a case study. This means that the complexity of the Internet of Things is analyzed through the lens of a specific and rather simple product that many people consider nevertheless vital in their household, a room cleaning device.

IoT connects countless physical objects to the Internet and not only will this number increase dramatically in the next years but humans will be included in this system as well. However, for the purpose of this paper we will focus just on the Internet of Things, the classical IoT. In such a typical Internet of Things system data is usually collected by an end device, transmitted through communication networks, processed by servers and finally provided to various, often mobile applications. Thus data flows through a multi-layered, complex

architecture. In this paper we will argue that using an IoT System in our homes requires protection at every single layer of the system.[1]

In the first part, which is the technical part of the paper, the architecture and structure as well as the design process of such a device will be described, which is necessary to be able to start from a common point and to find the weak spots and possible threats that lie within such a system and its products/services. In the second part that is dedicated to legal aspects, some of the areas of concern will be examined more closely with a focus on the legal and factual implications. However, apart from compliancy issues, the overwhelming power of the economic aspects will be taken into account. For the purpose of this paper we will chose as an example the rather basic product of a vacuum cleaner that is part of the IoT system of a smart home.

2. Technical Aspect of the IoT household vacuum cleaner

In an IoT system data is usually collected by end devices, transmitted through communication networks, processed by local/remote servers and finally provided to various applications. Moreover, the general design of IoT components evolves more and more into the use of – usually cheaper – modular systems using generic components with extensive functionality that, again, might be unknown not only to the owner but also to the producer(s) themselves.

Thus, private personal data flows through multiple layers of the architecture stack and it needs privacy protection at all layers. In general, the number of layers proposed for the architecture of IoT varies, here a four-layer architecture as the reference IoT architecture is adopted for the purpose of this paper which consists of a perception layer, a networking layer, a middleware layer and an application layer.[2]

IoT Architecture in layers	**Exemplification**
Application layer	Vacuum cleaner app, smart home, smart phone, tablet, smart watch
Middleware layer	«Brain», transforms the received data, stores it, inserts it into databases
Networking layer	ZigBee, Bluetooth, Z-Wave, Wi-Fi HaLow and 5th generation mobile networks
Perception layer	vacuum cleaner with sensors for the space, time, workload /dirtinessController, identification, actuator

Table 1 Structure of an IoT system (Adapted from: Li/Palansiamy, IEEE Internet of Things Journal 2018, 4).

As the lowest layer of the architecture (see table 1), the perception layer works as the base of the entire Internet of Things. It bridges the gap between the physical world and the digital world by making innumerable physical entities identifiable like RFIDs (radio-frequency identifications), perceptibles like sensors and finally controllables like actuators. These devices (identifiable, perceptibles and controllables) enable the interaction between the physical and digital worlds. The networking layer plays a main role, linking the perception layer and middleware layer so that sensed data and corresponding commands can be transmitted seamlessly between the two layers. The vast number of heterogeneous power-limited devices in the perception layer and the various applications in the application layer create a vital need for communication technologies that support low energy consumption, low latency, high data rate and high capacity. Main technologies supporting the IoT networking layer include ZigBee, Bluetooth, Z-Wave, Wi-Fi HaLow and 5th generation mobile networks. The middleware

[1] Noto La Diega/Walden, Contracting for the «Internet of Things»: Looking into the Nest, European Journal of Law and Technology, Vol 7, No 2, 2016, pp. 1-38.

[2] Li/Palansiamy, Privacy in Internet of Things: from Principles to Technologies, IEEE Internet of Things Journal 2018, p. 4.

layer works as the «brain» of IoT to process the amount of data received from lower layers. To cope with the interoperability of the heterogeneous physical devices, the device abstraction component semantically describes the resources with a consistent language such as the Extensible Markup Language (XML), Resource Description Framework (RDF) or Web Ontology Language (OWL). Based on that, resources are made discoverable through the resource discovery component by using Semantic Annotations for WSDL (web service description language) and XML Schemes, also called Semantic Annotations for WSDL and XML Schema (SAWSDL) or simply key words. Then, if needed, multiple resources can be composed by means of the composition component to enhance their functionality. After that, received data could be stored (storage component) in either databases or using cloud services and kept available to be queried. Different computational and analytical units can be combined to form the processing component. Although the individual components have a manageable functionality the overall system can be complex. High complexity can influence the testability of the system and thus influence the quality and also the security. Here, security of data, namely its confidentiality, integrity, availability, and nonrepudiation should be well protected. If data can make its owner either identified or identifiable, privacy enhancement technologies (PETs) are necessary to protect privacy so that privacy principles required by the laws can be satisfied. As the highest layer of the architecture, the application layer contains various IoT applications.[3]

3. A vacuum cleaner for every budget

In our example, the IoT vacuum cleaner consists of a cleaning body that is augmented by sensors in order to determine the size and layout of the rooms to be cleaned, the location of stairs or holes and the makeup of the ground, such as carpets or hardwood floors. Besides, the vacuum cleaner also contains one device (a system on a chip) in order to offer communication options via WiFi, Bluetooth or Z-Wave, positioning using GPS and WiFi and also a microphone as an audio input option for voice activation. Finally, it can also communicate via servers which are in a public cloud.

Additionally, our vacuum cleaning device offers an app to be able to steer it, to program it and to control the device. As the manufacturer's advertisements enthusiastically describe: «*Everything only for your comfort – so that you can do it all with your smartphone or tablet from wherever you choose*.» The app works on operating systems like Android as well as iOS and offers the following features: regular updates, a push notification when the vacuum cleaner finishes its work or is in trouble, a tool to monitor the progress of the cleaning constantly. The user is also able to get a protocol from the vacuum cleaner that takes the form of a map and of a timetable in order to monitor the cleaning on a regular basis. The app tells the user where the dirtiest spots in their house are as well as processing statistical information about the cleanings it has carried out in the past. Users need to provide an e-mail address and a name to gain access to the apps' functions. The app also offers the (optional) function to connect the device to a digital assistant of a third party, such as Amazon's Alexa, Apple's Siri or Google's OK Google.

The following entities are involved in designing, manufacturing and running the hard- and software of the IoT vacuum cleaner: the manufacturer of the vacuum cleaner itself, the developer of the app and its operating software, including the setup of the cloud.[4] This IoT-enabled vacuum cleaner does not boast a recognizable brand name but is affordable for nearly every budget. When discussing low-budget IoT devices special considerations have to be made in regard to the quality of both software and hardware. While using cheaper hardware components and building to a lower manufacturing standard are often the most visible cost cutting measure, the implications of developing software in such a budget-constrained environment can often have much graver

[3] Gartner, http://www.gartner.com/newsroom/id/3598917, November 2018; Kurz/Rieger, Die Datenfresser (2011).

[4] This is a very simplified scenario for illustration purpose. For a real life example of the complexities of an IoT system see Noto La Diega/Walden, Contracting for the «Internet of Things»: Looking into the Nest, European Journal of Law and Technology, Vol 7, No 2, 2016, pp. 1-38.

consequences. In order to cut down on both the development costs and the development time reuse of already established codes is key. This can be done in multiple ways, for example through the use of so-called libraries. These libraries can be seen as pre-made building blocks for solving common and often recurring problems, especially in the middleware layer such as secure communication via «Transport Layer Security» (TLS). Another way of reducing the development costs is by reusing already existing codes for example a previous iteration of the vacuum cleaner or a similar product, such as an IoT lawn mower. Although both the usage of software libraries and overall code reuse is considered good practice in the discipline of software engineering they still have consequences in regards to the overall stability and security of the finished product.

If a security vulnerability in a widely used software library is found, every application that embeds the said library is also at risk. Even if the flaw is fixed in the library later on, a new version of the software must be released which includes the new version of the library. In the past, flaws in widely used libraries such as the «Heartbleed bug»,[5] which was a security flaw in the widely used cryptographic library OpenSSL (which is used for TLS connections such as HTTPS) have had long lasting consequences even though the flaw itself had been fixed in a matter of days. Therefore, it is not only enough to simply the use of these libraries but also to track their versions and stay up to date on their security status. It is not uncommon for software development projects to use up to a 100 of these libraries and therefore correctly tracking versions and vulnerabilities is not a trivial task. Even if a supplier of a software library provides an update, this does not mean that all the devices used in the library are automatically updated with the new version. The manufacturer of the IoT device has to guarantee that any side effects due to the update must be excluded and the functionality of the device will not be affected by the update. This is one of the reasons why IoT devices usually do not offer an automatic update mechanism and run the same software or firmware version over their lifetime.

The practice of reusing codes that are more mature (in other words: older) or from similar products can also lead to unintended consequences. Codes that were written for a specific product in mind might not perform exactly as intended in the newer or a different product. A popular example for the unintended consequences of code reuse is the «Ariane 5» rocket incident, which lead to the destruction of the rocket during take-off. Investigations later on found out that the cause was a software error which was in part triggered by a code that was used for Ariane 4 and which was not adapted for the new performance characteristics of the newer rocket.[6] While code reuse in IoT appliances is unlikely to lead to such catastrophic incidents the same problems in principle still remain applicable. For example, old codes from previous appliances which were not intended to be used in a network environment can have a myriad of security and privacy flaws once exposed to the Internet.

Developing software intended for interconnected devices such as an IoT-enabled vacuum cleaner therefore requires a well-defined and well planned software development process. These methodologies do already exist, for example Microsoft developed and published the «Secure Development Lifecycle» (SDL).[7]However, when faced with both short development times and understaffed project teams, nonfunctional requirements such as security are the first to be neglected. This has also been the case in our example: Our vacuum cleaner reuses various older codes meant for other devices, not all the libraries incorporated are up to date and the cloud storage of the data is especially at risk of loss of confidentiality due to these lax practices. The manufacturer, however, is not aware of these risks, not being knowledgeable or experienced in the software development trade. The manufacturer has thus outsourced the software development to a series of contractors located outside of the European Union.

5 For more information about the Heartbleed Bug see http://heartbleed.com/.

6 Lions, Jacques-Lois, et al. «Ariane 5 flight 501 : failure report by the inquiry board.» (1996).

7 see https://www.microsoft.com/en-us/securityengineering/sdl/.

4. Data protection law aspects

The vacuum cleaner and the corresponding app collect and process the following data about its user: contact details (name, e-mail address), location data (GPS coordinates), connectivity details (such as IP address, SSID, password), size and layout of the living space, amount of dirt collected, times of use, use patterns, and any audio data collected by the microphone. Based on the data processed the identity of the user of the vacuum cleaning device can be determined, therefore personal data of the user is being processed within the meaning of Article 4 (1) GDPR.[8] It goes without saying that even more personal data can be gained if the cleaner is just one part in a whole smart house.

The various obligations of the GDPR address first and foremost the data controller as defined in Article 4 (7) GDPR. Article 24 GDPR determines the responsibilities of the controller for the processing of personal data but even before that, as early as at the design stage, Article 25 GDPR ensures that data protection issues are considered. Therefore, the controller has to implement appropriate technical and organizational measures to ensure that processing is carried out in accordance with the GDPR. However, most obligations address the controller, not (at least not directly) its processors or other entities such as data recipients.[9] In our case of the vacuum cleaner it is difficult to ascertain who exactly has determined the means and purposes of the processing. Was it the manufacturer or the software developers or even the users who made the decision to use and how to use the cleaner, to collect data and to connect everything to the internet?[10]

As a matter of fact in our case the manufacturer determined the purpose of the vacuum cleaner when deciding that the IoT vacuum cleaner should be at least connectable to the Internet and by that be able to navigate the cleaning space on its own. The developers of the software determine the means of the processing when deciding the architecture of the device, e.g. which code parts and libraries to use, and which kind of cloud and which cloud operator to use, especially since in our case they received no input from the manufacturer regarding these issues. Therefore, the manufacturer and the software developers could be regarded as joint controllers in accordance with Article 26 GDPR, for the data processing carried out when using the IoT vacuum cleaner. This conclusion seems to be supported by the most recent ECJ ruling on controllership. The ECJ states «[…] *that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.*» [11] In that case, the data subject can turn to each of the controllers to exercise their rights as secured in Article 26 par 3 GDPR.

The level of responsibilities is described in Articles 25 and 32 of the GDPR, which state that controllers must implement appropriate technical and organizational measures in order to protect the rights of data subjects and ensure a level of security depending on the risk for the rights and freedom of the data subject. Although Article 32 addresses the controller and processor alike, the obligations for controllers are more prominent. In the case of our IoT vacuum cleaning device the manufacturer should not have collaborated in a joint controllership with

---

8 Regulation (EU) 2016/679 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), OJ L 2016/119, p. 1.

9 Hötzendorfer/Kastelitz/Tschohl, Der DatKomm, Art 24 (7. Lieferung), para. 13; Article 29 WP 169, opinion 1/2010 on the concept of «controller» and «processor».

10 Whether the data subject can also inhabit the role of controller in relation to its own data is disputed at the moment and cannot be definitely answered by this contribution, see Fritz, Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DSGVO, in Schweighofer/Kummer/Saarenpää/Schafer (Ed), Data Protection/Legal Tech, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018 (2018), p. 24, with further references.

11 ECJ 5.6.2018 C210/16 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), para. 43; this ruling was made regarding the interpretation of Article 2 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 2018/1995, 31; however, the authors consider it still applicable to Article 4 (7) since the wording of both provisions is almost the same.

a company that does not ensure the compliance with the GDPR. Even if in the case of outsourced software development our controller had made an processing contract, it must not have chosen a processor that is not capable of ensuring an appropriate level of security and privacy as states Article 28 GDPR.[12] Although the processor is not addressed as often as the controller in the GDPR, he or she has nevertheless to take into account and to implement privacy enhancing techniques as well as the state of the art when including outdated versions of libraries and re-purposing code parts. In our case here, as stated, there is a joint controllership meaning that all controllers are jointly responsible for the processing of data.

5. Practical solutions for practical problems

However, this joint controllership for our cleaning device isn't worth that much neither to the data subjects nor to the supervisory authorities if the entities responsible remain obscure. In this case two principles of the GDPR might help to find a solution: first, the obligation for data controllers to be transparent about their data processing activities and to provide information and second, that the rights of the subject have to be enforceable.

Transparency and information are on top of the requirements of the GDPR, see Articles 12 ff GDPR. Article 13 and 14 GDPR require data controllers to identify themselves and to make contact details available. Any processing activity devoid of such basic information is obviously a violation of the GDPR. Besides, problems with transparency and information cannot just arise when they are not given at all but also when too much or confusing information is given to data subjects. Even if terms of service do exist they often use vague wording, incorporate a variety of technical terms and tend to reproduce the wording of US sources as well as through the multilayered structure of the device make it necessary to apply several contracts / general terms and conditions / privacy statements and service agreements at the same time and thus may not clearly identify the controller.[13] In both cases, that means that no or confusing / unclear data are given, data subjects wishing to know who is responsible for the processing activities of their IoT vacuum cleaner can turn to their local data protection authority under Article 77 of the GDPR and launch a complaint. In our scenario the manufacturer of the vacuum cleaner would be the first point of reference for an inquiry – especially since responsibility for the processing cannot be so easily denied, having your brand on the product.

With regard to the second important point for our case, that the GDPR wants to ensure that data protection is enforced, the ECJ has previously held that « [...] *the objective [...] is to ensure, through a broad definition of the concept of «controller», effective and complete protection of the persons concerned*.»[14]

In case that the design flaws mentioned above did lead to actual negative effects, such as security breaches, identity theft or disclosure of personal data, the data subject also has the right to an effective judicial remedy against a controller as laid down in Article 79 of the GDPR. Article 26 par 3 GDPR was already mentioned, so the data subject and the data authority can turn to either, the vacuum cleaner's manufacturer or the software developers. Thus information and transparency might help to increase awareness of users on how to protect their own personal data wherever they can, and at the same time the liability of a controller even if there are more than one, will ensure that they will make their particular roles clearer in the future. This would also be in the interest of data processors, to ensure their role and to secure a good contract.

In our opinion the GDPR could offer through its intertwining of transparency obligations and extensive enforcement measures a very practical way of cutting through the complexities of IoT systems in order to find at least one responsible controller to turn to in case of breach or damage. This will in the end increase the motivation of controllers to ensure privacy either especially by carrying out anonymization, perturbation and encryption in order to protect personal data either themselves or by their careful choice of their processors or

---

12 Hötzendorfer/Kastelitz/Tschohl, Der DatKomm, Art 25 (7. Lieferung), para. 17 f.

13 Noto La Diega/Walden, European Journal of Law and Technology, Vol 7, No 2, 2016, 3.

14 ECJ 5.6.2018 C210/16 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), para. 28; see also Article 29 WP 100, Opinion 10/2004 on More Harmonized Information Provisions.

joint controllers, especially when having the enormous penalty payments or additional damage payments that can arise in mind.[15]

6. Conclusion

The GDPR and other legal documents want to ensure the protection of personal data of natural persons so that no disadvantage should come to these persons through unlawful processing activities. The question arises whether the current legal instruments offered by the legal system in general and by the GDPR in particular are good enough for such an interconnected IoT world and can ensure the concept of privacy as we know it.[16] We think that it probably can if used in a very practical sense. We even assume that there is more to it given the new possibilities for law enforcement via these new technological possibilities. As Noto la Diega puts it with regard to information: «If the imposition of obligations for «data protection by design and by default» tells us anything, it is that a new frontier of law enforcement is technology. One could also envisage «consent by design» or «awareness by design» where, to give an example, it would be feasible to disable the feature enabling the user to confirm that «I have read» the applicable terms when he could not have read them, e.g. an algorithm could measure the time spent on the page and scrolling through the text.» [17]

Apart from that technical and organisational measures can ensure maybe not a very tight but nevertheless a reasonably secure curtain that hides our personal and private data collected by our cleaner or the smart house from the world, namely the internet. The complexity of the IoT system shows that the products and services have to be designed in a way that personal data does not even leave the house and by that create that privacy data curtain we will need. That means that the data collected by the perception layer have to be transformed to non-personal data as early as possible, probably at the latest at the middle ware layer.

The way to ensure all the discussed issues above will be carried out is probably through a combination of an active responsible authorities and attentive natural persons who enforce their rights from manufacturers / importers or software developers who may be liable as sole or joint controllers. That may come with higher prices that we should be prepared to pay in exchange for a better protection of our personal data.

7. References

Article 29 WP 100, Opinion 10/2004 on More Harmonized Information Provisions.

Article 29 WP 169, opinion 1/2010 on the concept of «controller» and «processor».

Article 29 WP 173, Opinion 3/2010 on the principle of accountability.

Article 29 WP 216, Opinion 05/2014 on Anonymisation Techniques.

Feiler, Lukas / Forgó, Nikolaus, EU-DSGVO, EU-Datenschutzgrundverordnung, Verlag Österreich, Wien, 2017.

Fritz, Gernot, Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, in Schweighofer/Kummer/Saarenpää/Schafer (Ed), Data Protection/Legal Tech, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018 (2018), 24.

Gartner, http://www.gartner.com/newsroom/id/3598917, Nov 2018.

Knyrim, Rainer (Hg), Der DatKomm, Praxiskommentar zum Datenschutzrecht – DSGVO und DSG, Wien 2018.

Kurz, Constanze / Rieger, Frank, Die Datenfresser, Fischer Taschenbuchverlag, Frankfurt, 2011.

[15] See also Article 29 WP 173, Opinion 3/2010 on the principle of accountability and Article 29 WP 216, Opinion 05/2014 on Anonymization Techniques.

[16] Rabl, Künstliche Intelligenz oder künstliche Aufregung: drei Thesen zur Digitalisierung, ecolex 2018 (222-224); Rebhahn, Effektivität des Rechts, ÖJZ 2018/7 (54-61).

[17] La Diega/Walden, European Journal of Law and Technology, Vol 7, No 2, 2016, 4.

Li, Chao / Palanisamy, Balaji, Privacy and IoT, DOI 10.1109/JIOT.2018.2864168, IEEE Internet of Things Journal, pp. 1-18.

Noto La Diega, Guido / Walden, Ian, European Journal of Law and Technology, Vol 7, No 2, 2016, pp. 1-38.

RABL, Thomas, Künstliche Intelligenz oder künstliche Aufregung: drei Thesen zur Digitalisierung, ecolex 2018, pp. 222-224.

Rebhahn, Robert, Effektivität des Rechts, ÖJZ 2018/7, pp. 54-61.