Assessing Privacy Policies of Internet of Things Services

Niklas Paul, Welderufael B. Tesfay, Dennis-Kenji Kipker, Mattea Stelter, Sebastian Pape

Assessing Privacy Policies of Internet of Things Services

Niklas Paul[1 [0000−0001−8283−4751]], Welderufael B. Tesfay[1 [0000−0002−1087−2019]], Dennis-Kenji Kipker[2 [0000−0003−1454−591X]], Mattea Stelter[2 [0000−0002−3627−8990]], and Sebastian Pape[1 (✉) [0000−0002−0893−7856]]

[1] Goethe-University, Frankfurt, Germany
[2] University of Bremen, Bremen, Germany

Abstract. This paper provides an assessment framework for privacy policies of Internet of Things Services which is based on particular GDPR requirements. The objective of the framework is to serve as supportive tool for users to take privacy-related informed decisions. For example when buying a new fitness tracker, users could compare different models in respect to privacy friendliness or more particular aspects of the framework such as if data is given to a third party. The framework consists of 16 parameters with one to four yes-or-no-questions each and allows the users to bring in their own weights for the different parameters. We assessed 110 devices which had 94 different policies. Furthermore, we did a legal assessment for the parameters to deal with the case that there is no statement at all regarding a certain parameter. The results of this comparative study show that most of the examined privacy policies of IoT devices/services are insufficient to address particular GDPR requirements and beyond. We also found a correlation between the length of the policy and the privacy transparency score, respectively.

Keywords: Internet of Things, Privacy Policies, General Data Protection Regulation, GDPR, ePrivacy Regulation, ePR

1 Introduction

Privacy is a big but early stage research topic in the Internet of Things (IoT), where many questions are still inadequately addressed [1]. Studies indicate that "six in ten Internet of Things devices dont properly tell customers how their personal information is being used" [2] and "nearly all areas (of Internet of Things) miss applicable mechanisms in privacy" [3]. This collection and processing of personal, sometimes sensitive, information has raised privacy concerns of users. A survey in 2016 revealed that 53% of 797 IT professionals are very concerned about privacy in IoT, it already seems relevant in professional circles [4]. With the increasing complexity of products users have to deal with, it is likely that this raises concerns of non-professional users as well.

Thus, regulators require service providers to publish their data processing practices. As such, terms and conditions and privacy policies are used to inform

users about the purpose of data collection and processing. However, only a small proportion of users read these documents [5, 6], mainly due to the length of the texts, and being written in difficult legal jargon. Therefore, it is widely accepted to confirm a policy without reading it, even if users in general should read them [7]. As a consequence, users are not aware that a large number of policies elude domestic justice, contains user unfriendly parts or suspect purpose of private data use e.g. to collect information and to use it as "a new source of revenue" by selling the information or for advertising purposes [8].

To give a methodological assessment of this problem, in this work, we introduce a framework for privacy policies of Internet of Things (IoT) devices evaluation based on General Data Protection Regulation (GDPR) aspects as assessment criteria. The framework gives an overview of the contents of certain policies and further ranks them based on their scores pertinent to these criteria. The objective of the framework is not to provide binding legal guidance, but to serve as supportive tool for users to take privacy-related informed decisions. For example when buying a new fitness tracker, users could compare different models in respect to privacy friendliness or more particular aspects of the framework such as if data is given to a third party.

The remainder of the paper is structured as follows: Sect. 2 briefly introduces the regulatory background on which our framework is based. After that, in section 3, related work is presented and how this work differs from them. In section 4 we present our research methodology and in section 5, the assessment framework is introduced. In section 6 we present the results of a first assessment and statistical analyses. In section 7, we discuss results and limitations of the framework and suggest future work. We conclude in section 8.

2 Background

Internet of Things (IoT) refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence [9]. Usually users can extend the control of IoT devices by using an application on their phone, tablet or computer. Since IoT-Services require a certain amount of personal information to determine user behaviour and they process electronic data automatically, they are regulated by the General Data Protection Regulation (GDPR) [10] and the ePrivacy Regulation (ePR) [11]. In this section, we give a brief overview on the GDPR and ePR with a focus how to utilize them as foundation for the privacy policy assessment framework.

2.1 General Data Protection Regulation

The General Data Protection Regulation, adopted by the European Parliament on 14 April 2016 and becoming effective as from 25 May 2018, will replace the Data Protection Directive (1995/46/EC). The regulation is the result of the EU's objective to harmonize the several data protection provisions existing at European

and national level and thereby to strengthen data protection throughout the EU[3]. Unlike the previous directive, the new regulation does not require transposition into national laws and will be directly applicable in all Member States. Henceforth, national legislation that diverges from the GDPR provisions will be allowed only within various opening clauses contained in the regulation. Since the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data" [10, Article 1 para. 1], it is also addressed to suppliers of IoT products. According to Article 3 of the regulation, the GDPR thereby does not only apply for EU-based producers of IoT devices, but also for all enterprises established outside the EU that offer their products on the European market. Therefore, the provisions of the GDPR can serve as uniform assessment criteria for the comparison of the level of data protection ensured for IoT devices whose producers are located across the world.

Of particular importance for the evaluation of privacy policies is Article 13 GDPR, which specifies the information to be provided where personal data are collected from a data subject. These information obligations follow from the transparency principle laid down in Article 5 GDPR. The mandatory information includes, inter alia, identity and contact details of the product provider as well as full details on the purposes of the data processing, the storage period, the various rights of the data subject under Articles 12-23 GDPR, or, where applicable, the disclosure of data to a third party and the transfer of data to third countries.

2.2 ePrivacy Regulation

However, the legislative process on the harmonisation of European data protection law is not yet completed. Apart from the GDPR, the ePrivacy Regulation is intended to replace the outdated Privacy and Electronic Communications Directive (2002/58/EC) and to supplement the GDPR as regards the electronic communication sector. Although the ePrivacy Regulation initially had been expected to become effective at the same time as the GDPR on 25 May 2018, it is currently still at the stage of draft [11]. While trilogue negotiations between the Parliament, the Commission and the Council are about to take place, the high level of data protection provided in the proposal is strongly criticised by media and advertising industries[4]. The exact scope of the ePrivacy Regulation and its relation to the GDPR remain controversial, too [13]. Thus, it does not appear to be appropriate to include the current draft regulation into this assessment framework the discrepancies that have to be resolved prior to the adoption of a final version are too fundamental. However, in the future, legal requirements for IoT devices will be significantly determined not only by the GDPR, but also by the ePrivacy Regulation: Recital 12 of the proposed regulation explicitly states that the scope of the regulation also covers the transmission of machine-to-machine communications, which is the essential characteristic of the Internet of Things. The regulations entry into force is not expected before 2019 [14].

[3] See, inter alia, Recitals 6, 7, 9, 10 of the GDPR.
[4] See, for example, the campaign by several industry associations [12]

3 Related Work

Even though information privacy is a concern for users and IoT operators, so far, it seems to be addressed inadequately. However, there are still some promising efforts, which we summarize below. Stankovic [1] proposed a new language for privacy policies in IoT to address emerging problems of privacy. Ziegeldorf et al. stated seven categories of privacy threats in the Internet of Things, introducing four new categories of privacy threats especially in the Internet of Things [15]. The threat of life-cycle transition (changes of control spheres e.g. through selling) is considered in this framework as well.

Smith, Milberg and Burke found five central dimensions of concerns about privacy practices namely, collection of personal information, internal unauthorized secondary use of personal information, external unauthorized secondary use of personal information and finally errors and improper access [16]. All these previously mentioned dimensions should be addressed in a privacy policy and are also, to some extent, part of the requirements for the assessment framework and can be considered as the basis to develop the framework.

Previous studies examined the existence of policies rather than assessing the content [17]. Previous work that took the content into account, mainly dealt with privacy policies of websites, but not of IoT services and respectively, apps to control them [18, 17, 19]. For Example some of them used the Fair Information Practices (FIPs) for the content and the Flesch grade level [20] for assessing the readability with the result that the examined policies were difficult to read and required a higher education level. The Flesch Score is based on the average lenth of a sentence and the average word length within syllables, the higher it is the easier a text is to read. Over time more mathematical approaches which calculated scores were established but also rankings based on a crowdsourcing approach [19]. In 2017, the project "Ranking Digital Rights" evaluated a set of companies based on 35 parameters in three groups namely governance, freedom of expression and privacy [21]. The privacy category was by far the largest, consisting of 18 parameters. It examined a broad variety of characteristics reaching from simple and easy policy access to the supply of information about potential cyber risks. Noteworthy is, they assessed not only one service of the company but a service portfolio. The project "Terms of Service; Didn't read" uses a less mathematical approach [22]. Based on crowdsourcing they present summaries and a rating of terms of 8 services that are assessed by other users on their website. The problem with this and other crowdsourcing solutions is that the scope is highly dependent on participation [23]. To overcome this, the project "Privee" uses a combination of crowdsourcing and automated classification [23]. Despite most previous work dealing with website privacy policies, there are also works assessing privacy aspects of apps [24].

4 Methodology

This section briefly describes how the framework was designed, how the assessed policies were selected, and how the assessment procedure was.

4.1 Framework Development

The main goal of this work is to create an assessment framework for privacy policies to assess a large variety of IoT devices. Therefore, applicable parameters are needed. The framework is strongly inspired by the GDPR (cf. Sect. 2), but we also considered the categories of privacy threats from Ziegeldorf et al. [15] and the dimensions of concerns about privacy practices from Smith, at al. [16] (cf. Sect. 3). For each of the parameters we identified relevant yes-or-no questions. For all categories, we did a legal assessment to check how we should cope with a non existing statement. We explain this in more detail in Sect. 5.1.

We identified two important dimensions for the framework: (i) Content-Dimension (Privacy Score) and (ii) Transparency-Dimension (Transparency Score). They differ in so far that the transparency-dimension rather checks whether the policy makes a statement or not and the content-dimension rather checks what statement the policy makes.

4.2 Policy Selection

To get an overview of the available products on the market, two websites[5] were used. Since many listed devices didnt exist anymore, we searched in web shops (e.g. Amazon) for similar products. As the framework is built on the GDPR and the GDRP applies only to services provided to EU citizens, the product must be available on the European market. Criteria defining what products are available in terms of the GDPR can be found in Recital 23 [10] and were checked by searching the manufacturers website and web shops. We did not assess policies where we couldn't find the IoT device available to the European market.

Another condition was that the policy needed to be available in English language. If no general EU-English policy was available, an English version applicable in Germany was looked for or otherwise the UK one was chosen. Sometimes, e.g. US policies are slightly different from EU-language policies. If there was an US and an EU policy available, the EU one was chosen. If some parts of the policy were applicable to specific countries, the descriptions for Germany or otherwise another EU-country were preferred. If there was no distinction of EU/Non-EU or no declaration of where the policies apply, it was assumed that it is a global policy, which is also permitted in the framework.

To find the policies we searched the website of the manufacturer in the first place and after that we searched for the policy in the Google Playstore and in the last instance we contacted them via E-Mail to send us the according policy.

4.3 Assessment Procedure

The assessment was done manually by reading the policies and applying all parameters to them. The number of words and the Flesch Score were calculated automatically by an Online Tool [25], the remaining questions are yes-or-no

[5] `http://IoTLineup.com` and `http://IoTList.co`

questions. To record the results of the assessment, a table-workbook with several sheets was created containing an overview of all policies and one sheet for every assessment. The assessment scorecard is a table with general information (e.g. name, ID, category) in the header and all parameters beneath. For both Privacy Score and Transparency Score there are columns where the answer and the corresponding points were saved. We also stored the segment of the privacy policy which was relevant for the scoring to allow using this data as a training set for a machine learning algorithm later.

5 Assessment Framework for Privacy Policies

The framework consists of 16 parameters with all besides the first of them having up to four yes-no-questions. As already discussed, parameters are assessed towards a privacy score and a transparency score. The answer to each question is assessed and the awarded points sum up to a score in this parameter. Every parameter has a separate score. To balance the different number of each question, the score for each parameter is then normalized to be between 0 and 1. For questions that cannot be answered with yes or no (e.g. clicks needed) there was a table which assigned the clicks to points within this interval. Since convergence to the privacy-protective condition of the parameter raises the score, the score can be interpreted as "the higher the score, the better the privacy practices". Analogous, the transparency can be interpreted.

Agrawal et al. (2007) weighted their categories with an importance factor, which is the case on the parameter level in this framework as well. Users can set a weighting factor for each parameter to operationalize their personal preferences. If the user is not able to come up with weights easily, the framework can also be used as a basis for an Analytic Hierarchy Process (AHP) like approach [26]. Hereby, the importance of every parameter is compared pairwise to each other and the result is a parameter importance ranking. However, with an increasing number of parameters, respondents might perceive this approach as exhaustive. For the remainder of this work the weighting factor was set to 1.

To make it easy for the user to see where a policy is positioned within the range of 100%, letters are assigned to relative scores. Therefore, we divided the range of possible scores into five quintiles such that a relative Privacy Policy Score (PPS) and respectively a relative Transparency Score (TS) with more than 80% get the best "A"-Ranking and the rankings with 20% and less get an "E"-Ranking which is the worst.

5.1 Parameters

The 16 parameters of the framework (cf. Tab. 1) cover different categories like accessibility, readability, the right to object, access, erasure and data portability. Whether the policy considers special treatment of children data and utilization of special data categories (Health, Race, Sex, ...) is covered as well. Also for the involvement of a third party, notification for changes or data breaches and notes

on utilization for advertisement there are separate parameters. Due to space limitations, we are not able to describe each parameter and reasoning in detail, but for transparency each related GDPR article is noted in column § of Tab. 1.

5.2 Transparency Score

As shown in Tab. 1, all parameters are considered for the transparency score. Since it is modeled if the policy makes a statement, the value of a parameter question is 1 if the policy answered the question (irrespective how it was answered) and 0 if the question is not or contradictory answered.

Relative Transparency Score The transparency score is based on the sum of the 16 parameters that each have a value between 0 and 1. The score for service i is calculated by formula 1 where $T_{i,j} \in \{0, 1\}$ represents the corresponding value of the parameters, and w_j is the weighting factor for parameter j. With $T_j^* = 1$ as the best possible score of parameter j, we get:

$$\text{Relative TS}_i = \frac{\sum_{j=1}^{n} w_j T_{i,j}}{\sum_{j=1}^{n} w_j T_j^*} = \frac{\sum_{j=1}^{n} w_j T_{i,j}}{\sum_{j=1}^{n} w_j} \tag{1}$$

5.3 Privacy Score

The privacy score needs a more distinct view on the parameters. Some parameters like the Flesch Reading Ease Score or if the policy is a multi-device policy can be assessed for all policies (cf. Tab. 1, sign: ✓). We did not consider the parameters marked with ✗ in Tab. 1, because some of them are not referring to the content of the policy, e.g. how easy it is to find the policy. Others do not necessarily need to be provided, e.g. the GDPR already states when a notification of policy changes needs to be provided. Gluck et al. [27] found contradicting signs: Despite that shorter notices are typically expected to be more effective, removing expected privacy practices from privacy policies sometimes led to less awareness of those practices, without improving awareness of the remaining practices. Thus, we decided not to consider these parameters for the privacy score.

However, there are also parameters which need to be stated (cf. Tab. 1, sign: 🔍), e.g. the right of data portability, where we considered their absence negative for the privacy friendliness. In contrast, parameters which are in general not expected, but required if the service provider follows a certain practice (cf. Tab. 1, sign: 🔍), e.g. transfer of data to third parties. Therefore, if no statement was given, we considered them to be positive for the privacy friendliness.

The parameter marked with 🧍 should only apply to devices which are used by children. Since for many devices there is no clear statement of the target audience, we considered it only for toys.

Table 1. The Framework's Parameters with their Questions and how the Parameters are Considered for Transparency (T) and the Privacy Friendliness of the Policy (P).

#	Parameter Name	Parameter Description	T	P	§
1	Easily Acc. Form	1) Readability (Flesch Reading Ease Score)	✓	✓	12
2	Right to Object	1) Does the policy state a right to object? 2) Is an objection as easy as a consent?	✓	🔍	6, 7, 13, 21
3	Children	1) Is a binding age limit to use the service stated? 2) Is there a special policy for children? 3) Is there a mechanism to ensure that parents agree with the processing? 4) Does the policy state the procedure if children data has been processed unintentionally?	✓	🧍	8
4	Processing of Special Categories of Personal Data	1) Are special personal data categories processed? 2) Is it required contentwise for using the service? 3) Is there an explicit consent?	✓	🔍	9, 13
5	Necessary Information	1) Are identity and contact details of the controller stated? 2) Is a data protection officer stated? 3) Are the purposes of the processing for which the personal data are intended stated?	✓	🔍	13
6	Period of Storage	1) Is the storage period stated? 2) Are criteria determining the period stated?	✓	🔍	13
7	Right of Access	1) Is the right of access stated? 2) Is a fee charged?	✓	🔍	12, 13, 15
8	Right to Erasure	1) Is the right to erasure stated? 2) Is the time to fulfil the erasure request stated? 3) Period until fulfilment	✓	🔍	12, 13, 17
9	Data Portability	1) Is the right to data portability mentioned?	✓	🔍	13, 20
10	Third Countries	1) Is data processed in third countries? 2) Does the policy state these countries? 3) Is data transferred to countries with adequate level of protection (e.g. EU-U.S. Privacy shield)?	✓	🔍	45, 46, 47, 49
11	Data Breach Notification	1) Is a personal notification after a data breach explicitly stated? 2) Period until notification	✓	✗	34
12	Third Parties	1) Is a third party involved by design? 2) Does the policy state who the third party is? 3) Does the policy explicitly state the purpose? 4) Is the scope of the transferred data stated?	✓	🔍	13
13	Search for the Policy	1) Is there a link on the homepage that leads to the policy for the device quickly? 2) How many clicks are needed from the homepage to find the link to the policy?	✓	✗	12, 13
14	Change Notificat.	1) Is there a notification after policy changes?	✓	✗	13
15	Special Device Policy	1) Is the present policy a multi-policy? 2) Is it clear, the policy is for the IoT product?	✓	✓	
16	Lifecycle	1) Can information stored on the device be deleted?	✓	🔍	

✓: Used, ✗: Not used, 🔍/🔍: If not present, rated positive/negative, 🧍: Only for toys

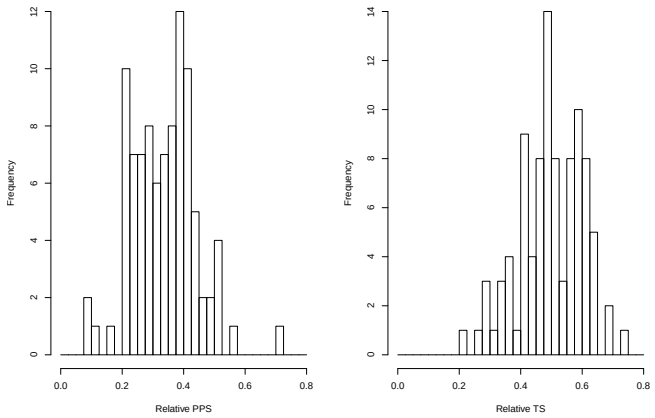

Fig. 1. Histogram of PPS and TS of Examined Policies

Relative Privacy Policy Score The value which enables comparisons along different policies is called relative Privacy Policy Score (relative PPS). The relative PPS for service i is calculated by formula 2 where j is the parameter id, x_j is the weighting factor for parameter j, $P_{j,i}$ is the score of parameter j for Service i and with $P_j^* = 1$ as the best possible score of parameter j, we get:

$$\text{Relative PPS}_i = \frac{\sum_{j=1}^{n} x_j P_{i,j}}{\sum_{j=1}^{n} x_j P_j^*} = \frac{\sum_{j=1}^{n} x_j P_{i,j}}{\sum_{j=1}^{n} x_j} \tag{2}$$

6 Results

A set of 113 IoT devices was created, but while collecting policies we found three products without a policy which would be ranked with 0% in both dimensions. For legibility reasons we removed these ones and ended up with 110 products to assess. They were divided into three umbrella categories Smart Home, Smart Health and Toys, which are subdivided in groups e.g. Thermostat, Light, Washer, etc. Some privacy policies covered multiple devices or they were a privacy policy for all of the company's services. According to the assessment framework in Sect. 4.3, privacy policies were assessed and ranked based on their achieved privacy and transparency scores. In the end, we assessed 94 policies: 14 policies covered 30 devices and 80 policies were for a single IoT device. Two devices changed their policy during the assessment period.

6.1 Ranking Results

Table 2 shows the results of the privacy and transparency scores grouped into the respective subgroups. Figure 1 presents histograms for the relative privacy policy respectively transparency score.

Table 2. Summary Statistics of Examined Policies

Area	Subarea	#	PPS Score					Rel. PPS (%)		Transparency					Rel. TS (%)	
			A	B	C	D	E	Mean	STD	A	B	C	D	E	Mean	STD
Smart Home	Coffee Machine	5	0	0	1	4	0	31.67	8.39	0	0	4	1	0	47.50	10.37
	Light	5	0	0	2	3	0	35.56	8.67	0	1	4	0	0	53.75	6.04
	Security	9	0	0	3	5	1	32.80	11.36	0	1	7	1	0	48.61	9.80
	Thermostat	6	0	0	3	3	0	36.69	11.10	0	1	4	1	0	50.43	11.35
	Washer	5	0	1	2	2	0	37.91	20.83	0	1	3	1	0	54.17	12.68
	Others	28	0	0	7	21	0	34.71	8.95	0	5	20	3	0	50.52	8.99
	Total	58	0	1	17	38	2	34.70	10.50	0	9	42	7	0	50.55	9.37
Health	Fitness Tracker	7	0	0	2	5	0	36.11	6.39	0	1	6	0	0	53.72	4.91
	Scale	15	0	0	1	12	2	28.75	11.56	0	3	6	6	0	43.89	12.93
	Others	5	0	0	1	4	0	33.89	8.22	0	1	4	0	0	52.29	6.93
	Total	27	0	0	4	21	2	31.61	10.14	0	5	16	6	1	47.99	11.18
	Toy	9	0	0	3	6	0	34.05	12.66	0	2	6	1	0	50.92	13.18
$\sum$	Total	94	0	1	24	65	4	33.75	10.59	0	16	64	14	0	49.85	10.26

6.2 Statistics on the Privacy Policies

The results do not appear to have similarities with a normal distribution. We conducted a Shapiro-Wilk-Test [28] to confirm or reject this hypothesis. It is a high-quality test for normal distribution that can be applied on relatively small samples. The p-value predicts how likely it is to get such results from a normal distribution. With a p-value of 0.1368 for the relative PPS and p-value of 0.3146 for the relative TS, we assume that the distribution of the privacy scores and the distribution for the transparency score are not close to a normal distribution.

Due to the results of Gluck et al. [27], we were also interested in the relationship between the length and the privacy respectively transparency score of the privacy policies. Since the plots (cf. Fig. 2) show some clusters, we conducted Spearman correlation tests [29]. For the correlation between the number of words in the policy and the privacy score we found a moderate effect size ($\rho_{PPS} \approx 0.518$ with p-value $\approx 8.8 \cdot 10^{-8}$). Analogous, for the correlation between the number of words in the policy and the transparency score we found a strong effect size ($\rho_{TS} \approx 0.723$ with p-value $\approx 2.2 \cdot 10^{-16}$. Both correlations are statistically highly significant and allow us to conclude that there is a relationship between the length of the policy and the privacy respectively transparency score.

7 Discussion

The ranking of the both scores within the quintiles shows that none could get an A-rating. This might improve when the GDPR is put in place in May 2018. However, being compliant to the GDPR could also mean to inform about certain privacy practices without them being more privacy friendly. Difficulties in finding the right policy raises also the question whether companies use privacy policies to inform the users or if they just use them as a legal cover.

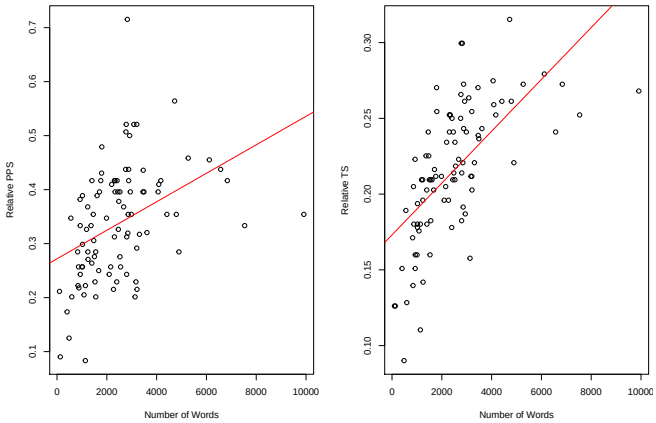

Fig. 2. Relationship between Length and Relative PPS/TS

The result of the correlation between scores and length should not be misunderstood as a motivation to provide longer policies because longer policies seem to be better. More likely, the result is due to the fact that in longer policies more topics can be covered. We expect a certain length where this effect will invert.

7.1 Limitations and Threats to Validity

Despite all care, the assessment framework cannot replace the detailed analysis of a lawyer. Although, the questions are Additionally, it was not possible to test the implementation of the policy. All assessment is based on the written policy and it is not guaranteed that companies follow their own rules. Future research should crosscheck contents and execution of the policy. Labels like TRUSTe, which the FTC approach took into account for a measure of enforcement [18], can be an indicator that their policies indeed reflect their practices. Nevertheless, even for labels like TRUSTe, there is reason for critique e.g. in meaningfulness [30].

We only examined English privacy policies. We can not exclude that the policies' contents differ between the different language versions. According to Article 12 of the GDPR the policy must be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". The availability of a language other than English is not explicitly mentioned in the GDPR but the line of argument could be that this supports the requirements.

A weak point of parameter 13 (Search for the Policy) is that the effort to find a policy is not a reliable measure because it is dependent on who looks for it. Some companies use the same policy for their products as for their websites and some companies don't declare the range of application which makes it difficult to ensure that the present policy is the right one for the IoT product. However, we could statistically show that there was no learning effect when searching for the policy since the number of steps was not significantly lower at the last investigated policies.

7.2 Future Extension of the Framework

One design goal of this framework was its openness to extensions. New parameters can be easily added, the utilization of a relative score instead of an absolute score makes allowance for this, because it allows a step-wise re-assessment. One can easily think of further requirements for a good privacy policy/practice which is not considered in this framework yet, but future work could create new parameters to operationalize them. We list some of the additional parameters, we also considered, assessed but not included in the final version of the framework. Procedure of data sharing after a *corporate merge or bankruptcy*. Has the parent company access to personal information after a merge? We didn't include this parameter in the final framework, because we couldn't find a statement how reliable this declaration would be if there would really be a merge or bankruptcy. A parameter considering the data processing if *the user is not the owner*, but e.g. a guest in a smart home where microphones listen for commands and listen to the guests, who have not given consent [31]. Is the scenario of an incidental use considered? Are there mechanisms to protect against an incidental use? Since as of today, this seems to be a non resolved issue, we also did not consider this parameter in our framework. For the same reason, we did not consider *interacting systems*, where each system has its own privacy policy and there is a chance of inconsistencies arising when systems work together.

8 Conclusion and Future Work

This paper presents an extendable assessment framework for privacy policies consisting of 16 parameters. We collected 94 privacy policies covering 110 devices. Users can look up certain topics or compare devices according to their own preferences.

The results of this comparative study show that most of the examined privacy policies of IoT devices/services are insufficient to address the GDPR requirements and beyond. Many topics are currently not addressed in privacy policies but will need to be covered until May 2018, when the GDPR comes into effect.

Difficulties in finding the right policy raises the question whether the purpose of privacy policies is to inform the users and make them conscious of the data processing or if it is just a legal cover, which deserves further research. The transparency dimension tried to operationalize this aspect but further development and improvement of this dimension is required.

During the analysis of this work it also seemed as though that products on the European market have fewer functionalities than US products. Some devices are not even available for EU citizens, perhaps due to the higher requirements of European law. Future work could check this impression. Additionally, there might be differences in the cont the same policies in different languages and future research should include a comparison.

To make people more aware about the shortcomings of privacy policies, a public ranking website should be designed. Based on the current framework users

could set the privacy preferences and a personalized score could be calculated. Awareness for privacy topics might help to force companies to reform their practices. To avoid manually processing a larger number of policies, an automatic assessment tool could be designed and developed, e.g. based on a machine learning approach. In particular, we aim at extending the framework by using the assessed privacy policies as corpus and building predictive models using machine learning and natural language techniques. Furthermore, considering semantic features of privacy policies could result in analyzing and bench-marking IoT privacy policies with high accuracy. Such automatic and adaptive models coupled with usable and informative user interfaces can be helpful to support users in analyzing and retracing the data processing practices of IoT services they intend to subscribe.

Acknowledgments

This research was partly funded by the German Federal Ministry of Education and Research (BMBF) with grant number: 16KIS0371.

References

1. Stankovic, J.A.: Research Directions for the Internet of Things. IEEE Internet of Things Journal **1**(1) (2014) 3–9
2. Information Commissioner's Office: Privacy regulators study finds Internet of Things shortfalls (2016)
3. Mayer, C.P.: Security and Privacy Challenges in the Internet of Things. In: Electronic Communications of the EASST. Volume 17. (2009)
4. DZone: The DZone guide to Internet of Things (2016)
5. Milne, G.R., Culnan, M.J.: Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing **18**(3) (2004) 15–29
6. European Commission: Special Eurobarometer 431: Data Protection Report (2015)
7. Jensen, C., Potts, C., Jensen, C.: Privacy practices of internet users: Self-reports versus observed behavior. International Journal of Human-Computer Studies **63**(1-2) (2005) 203–227
8. Casadesus-Masanell, R., Hervas-Drane, A.: Competing with Privacy. Management Science **61**(1) (2015) 229–246
9. Xia, F., Yang, L.T., Wang, L., Vinel, A.: Internet of Things. International Journal of Communication Systems **25**(9) (2012) 1101–1102
10. European Parliament, Council of The European Union: Regulation (EU) 2016/679 General Data Protection Regulation (GDPR). `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679` (2016)
11. European Commission: Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010` (2017)

12. European Interactive Digital Advertising Alliance (EDAA): The e-privacy regulation – good or bad for european consumers? http://www.likeabadmovie.eu/ (2018)
13. Engeler, M., Felber, W.: Draft of the ePrivacy Regulation from the perspective of the regulatory practice. http://rsw.beck.de/rsw/upload/ZD/ZD_Sonderver\"offentlichung_Engeleer_Felber_engl..pdf (2017)
14. Pellikan, L.: Bundesregierung: ePrivacy-Verordnung kommt erst 2019. W&V of 22 November 2017, https://www.wuv.de/digital/bundesregierung_eprivacy_verordnung_kommt_erst_2019 (2017)
15. Ziegeldorf, J.H., Morchon, O.G., Wehrle, K.: Privacy in the Internet of Things: threats and challenges. Security and Communication Networks **7**(12) (2014) 2728–2742
16. Smith, H.J., Milberg, S.J., Burke, S.J.: Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly **20**(2) (1996) 167
17. Milne, G.R., Culnan, M.J.: Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 u.s. web surveys. The Information Society **18**(5) (2002) 345–359
18. Peslak, A.R.: Internet Privacy Policies. Information Resources Management Journal **18**(1) (2005) 29–41
19. Agrawal, R., Grosky, W.I., Fotouhi, F.: Ranking Privacy Policy. In: IEEE 23rd Intern. Conference on Data Engineering Workshop. (2007) 192–197
20. Flesch, R.: A new readability yardstick. Journal of Applied Psychology **32**(3) (1948) 221–233
21. Ranking Digital Rights: 2017 Corporate Accountability Index (2017)
22. Terms of Service; Didn't Read project: Website. https://tosdr.org/ (2017)
23. Zimmeck, S., Bellovin, S.M.: Privee: An architecture for automatically analyzing web privacy policies. In: Proceedings of the 23rd USENIX Security Symposium. August 20–22, 2014, USENIX Association (2003)
24. Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Liu, B., Schaub, F., Wilson, S., Sadeh, N., Bellovin, S.M., Reidenberg, J.: Automated Analysis of Privacy Requirements for Mobile Apps: Ndss'17: Network and Distributed System Security Symposium (2017)
25. WebpageFX: Readability Test Tool. https://www.webpagefx.com/tools/read-able/
26. Saaty, T.L.: What is the analytic hierarchy process? In: Mathematical models for decision support. Springer (1988) 109–121
27. Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L.F., Agarwal, Y.: How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In: Symposium on Usable Privacy and Security (SOUPS). (2016)
28. D'Agostino, R.B., Stephens, M.A., eds.: Goodness-of-fit techniques. 5. print edn. Volume 68 of Statistics. Dekker, New York, NY (1986)
29. Hollander, M., Wolfe, D.A.: Nonparametric Statistical Methods. (1999)
30. McCarthy, J.: TRUSTe Decides Its Own Fate Today - Slashdot (1999)
31. v. Leitner, F.: Das IoT-Problem. https://ptrace.fefe.de/iot (2017)

All websites have been last accessed on Jan. 15th, 2018.