

# Assessing Privacy Policies of IoT Services

**Sebastian Pape**

**Niklas Paul  
Welderufael Tesfay**

Chair of Mobile Business & Multilateral Security  
Goethe University Frankfurt am Main

**Dennis-Kenji Kipker  
Mattea Stelter**

Faculty of Law  
University of Bremen

1	Idea
2	Framework
3	Result
4	Conclusion and Future Work



## Privacy Statement for Nest Products and Services

Policy active as of 28 April 2017. Review previous policies [here](#). Read about our recent update [here](#).

### Legal Items

[Privacy Policy for Nest Web Sites](#)

**Privacy Statement for Nest Products and Services**

[Terms of Service](#)

[End User License Agreement](#)

[Limited Warranty](#)

### At Nest, we take your privacy seriously.

This Privacy Statement for Nest Products and Services (“Privacy Statement”) describes information that Nest Labs, Inc. and its subsidiaries and affiliates (collectively, “Nest”) collect, use, share, and store, including personal information (i.e., information that personally identifies you, such as your name, email address or billing information, or other data that can be reasonably used to infer this information).

This document focuses on information related to the operation of Nest



- Lookup Single Attributes easily for a Certain Purpose
  - e.g. Scale that does not share weight with 3<sup>rd</sup> party

- Ranking for Comparison of Privacy-Policies (within same product type)



1	Idea
2	Framework
3	Result
4	Conclusion and Future Work



# Privacy Policy Framework

- 16 Parameters
  - based on GDPR
  - (Up to 4) Questions or other Scores (e.g. Flesch Score) used



## Different Categories of Questions:

✓: Used

✗: Not used

⊕/⊖: If not present,  
rated positive/negative

👤: Only for toys

- according to the requirements to policies in the GDPR

## Normalization / Weighting

- Due to different number of questions per parameter
- User preferences for comparison possible

# Assessment: Parameters 1 to 9

#	Parameter Name	Parameter Description	T	P
1	Easily Accessible Form	1) Readability (Flesch Reading Ease Score)	✓	✓
2	Right to Object	1) Does the policy state a right to object? 2) Is an objection as easy as a consent?	✓	Ⓚ
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?	✓	⚙
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?	✓	Ⓚ
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?	✓	Ⓚ
6	Period of Storage	1) Is the storage period stated? 2) Are criteria determining the period stated?	✓	Ⓚ
7	Right of Access	1) Is the right of access stated? 2) Is a fee charged?	✓	Ⓚ
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	✓	Ⓚ
9	Right to Data Portability	1) Is the right to data portability mentioned?	✓	Ⓚ

✓: Used

✗: Not used

Ⓚ/Ⓚ: If not present,  
rated positive/negative

⚙: Only for toys



# Assessment: Parameters 10 to 16

#	Parameter Name	Parameter Description	T	P
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)?	✓	⊕
11	Data Breach Notification	1) Is a personal notification after a data breach explicitly stated? 2) Period until notification	✓	✗
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	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?	✓	✗
14	Change Notification	1) Is there a notification after policy changes?	✓	✗
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?	✓	⊕

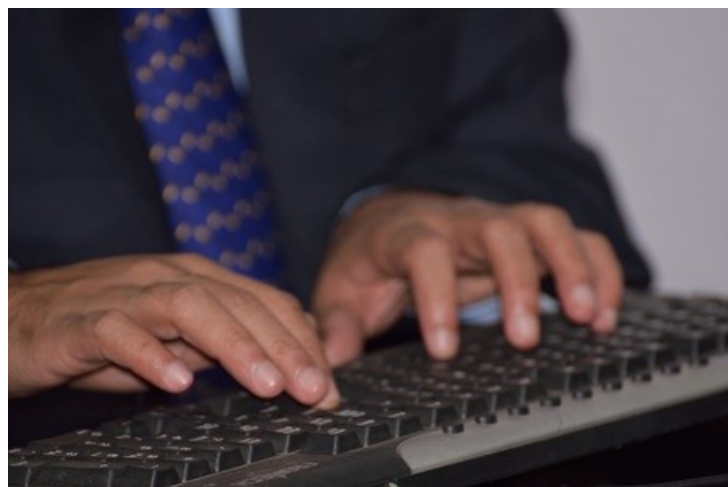
✓: Used  
 ✗: Not used  
 ⊕/⊖: If not present, rated positive/negative  
 🧸: Only for toys

# Assessment: Overall Score

Share of achieved PPS	Interpretation	Ranking
81-100%	Contents of the policy are to (nearly) whole extent user-friendly.	A
61-80%	Contents of the policy are mainly user-friendly.	B
41-60%	Some contents of the policy are questionable and not user-friendly.	C
21-40%	Contents of the policy are mainly user-unfriendly.	D
0-20%	The company does (nearly) only user-unfriendly practices.	E

- |   |                            |
|---|----------------------------|
| 1 | Idea                       |
| 2 | Framework                  |
| 3 | Result                     |
| 4 | Conclusion and Future Work |


- Processed Policies for 110 Services
  - 94 Policies
- Devices grouped to
  - Smart Home
  - Smart Health
  - Toys
- Procedure:
  - Only Products available in EU with English Policy examined
  - Inspected Website, then Terms & Conditions, Searched Website, Searched with Google, Looked at Google Playstore, Mailed to Support



# Assessment: Basic Information

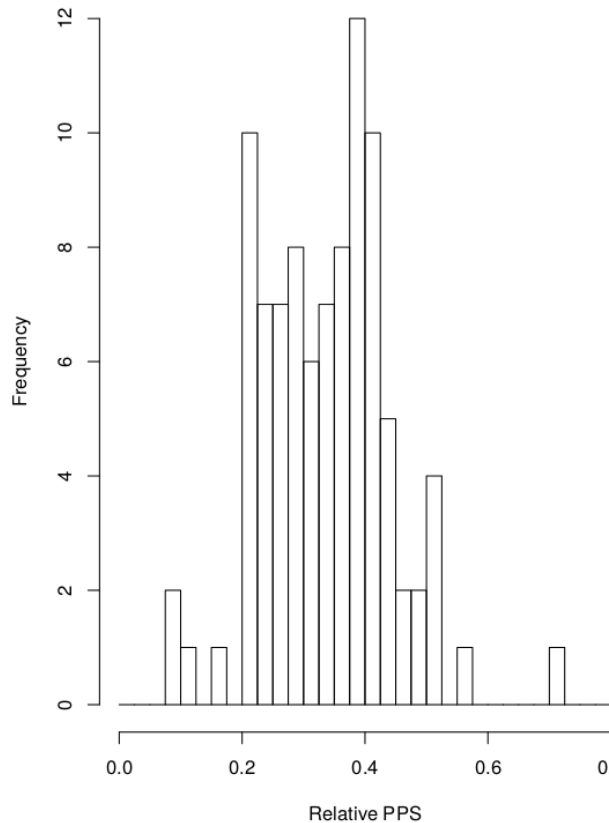
Identifier:	1
Product/Service:	Learning Thermostat™
Manufacturer:	Nest
Group:	Thermostat
Date:	01.06.2017
URL Policy:	<a href="https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/">https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/</a>
Policy Type:	1
Date:	17.04.2017
Age (days):	67
Length (number of words):	4061
Country of Origin:	US
Price:	<a href="https://store.nest.com/be/nl/product/thermostat?selectedVariantId=T3010FD">https://store.nest.com/be/nl/product/thermostat?selectedVariantId=T3010FD</a> 249,00 €

# Policy Summary Statistics

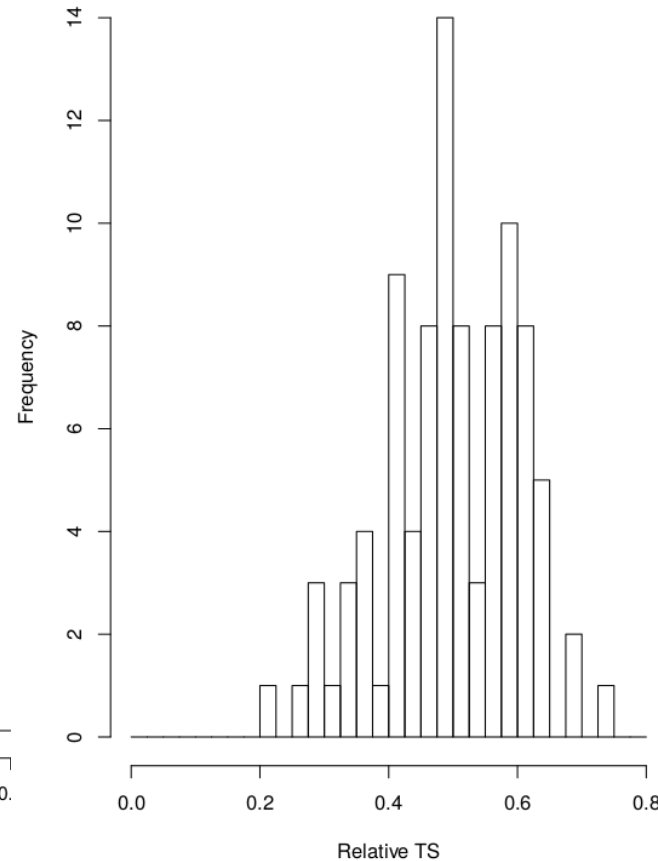
Area	Subarea	#	PPS Score					Rel. PPS (%)		Transparency					Rel. TS (%)	
			A	B	C	D	E	Mean	STD	A	B	C	D	E	Mean	STD
Smart Home	Coffee Machine	5	0	0	1	4	0	31.67	8.39	0	0	4	1	0	47.50	10.37
	Light	5	0	0	2	3	0	35.56	8.67	0	1	4	0	0	53.75	6.04
	Security	9	0	0	3	5	1	32.80	11.36	0	1	7	1	0	48.61	9.80
	Thermostat	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
$\Sigma$	Total	94	0	1	24	65	4	33.75	10.59	0	16	64	14	0	49.85	10.26



# Statistical Results - Histogram



Privacy Score



Transparency Score

Shapiro Wilk Test

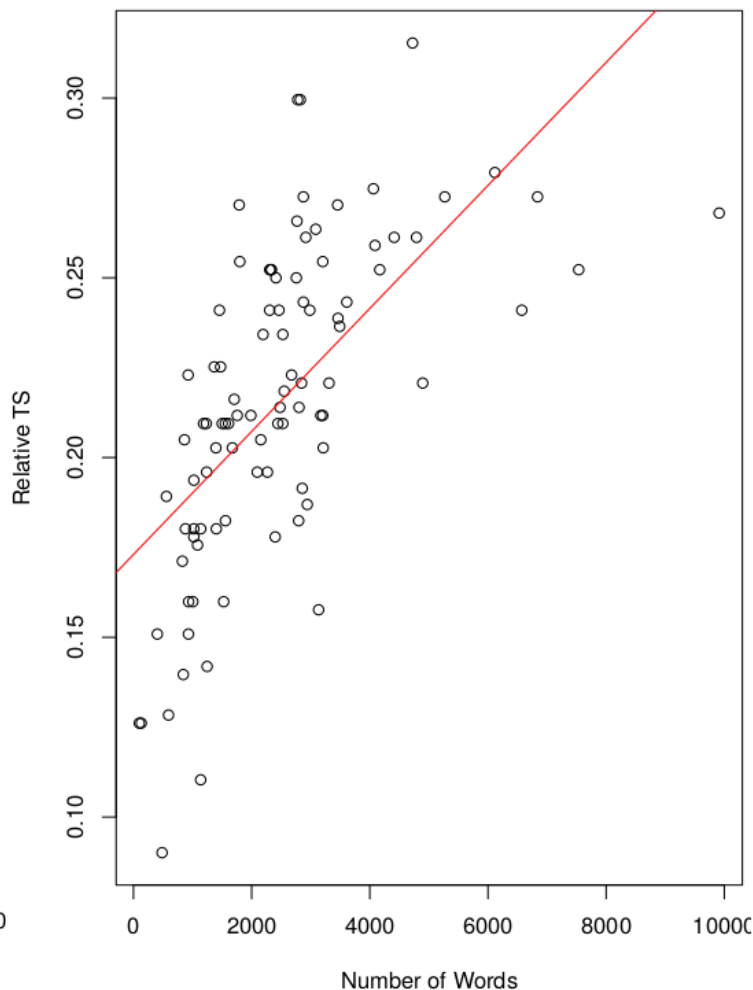
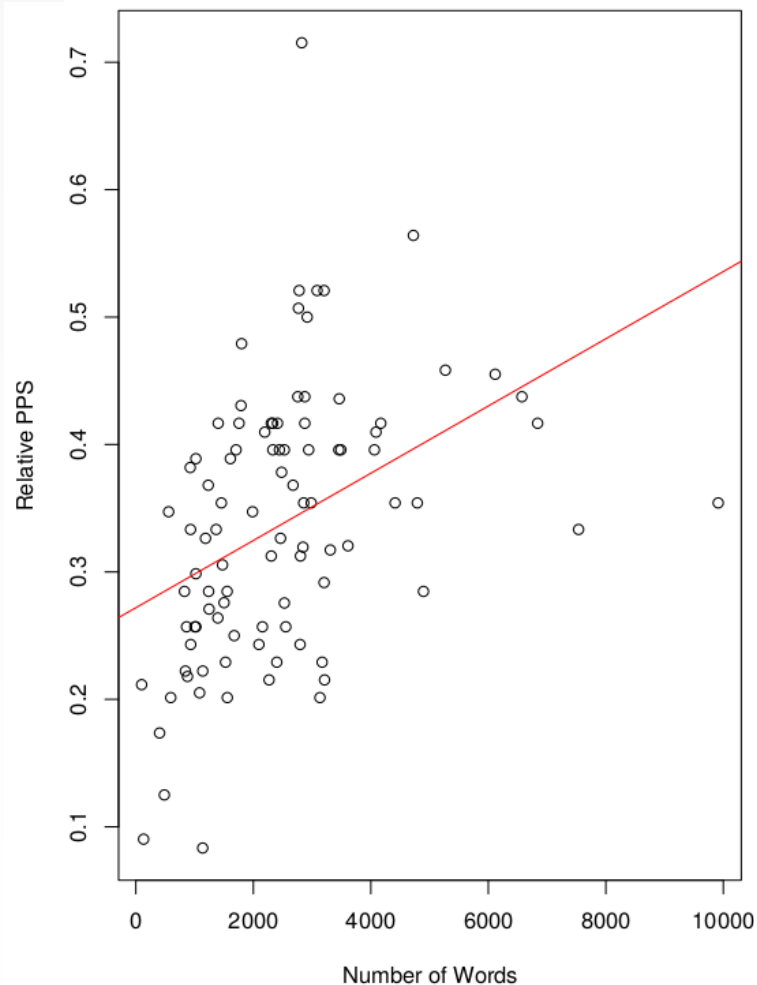
p-values:

PPS: 0.1368

TS: 0.3146

→ not normal  
distributed

# Statistical Results – Word Count



Spearman  
Correlation Test

Privacy Score:  
 $\rho \approx 0.518$   
 $p \approx 9 \times 10^{-8}$

Transparency  
Score:  
 $\rho \approx 0.723$   
 $p \approx 2 \times 10^{-16}$

- Remember: Deadlines were before GDPR went in place
- Only Privacy Policies considered  
No check what devices actually do
- Only Products available in EU with English Policy examined
- Shall we count devices or Privacy Policies for statistics?
- Data collector might get better finding privacy policies
  - We could not find a statistically significant learning effect




1	Idea
2	Framework
3	Result
4	Conclusion and Future Work

# Summary and Future Work



## IoT-Services-Privacy-Policies Framework

- 94 Policies Examined
- Designed Along GDPR
- Most Policies not “friendly”



## Lawyers' Feedback integrated

- What needs to be stated according to GDPR?



## Combination with Machine Learning

- Use Data as Training Data
- Include the more difficult parameters again (e.g. corporate merger, user not owner of the device)



## Deutsche Telekom Chair of Mobile Business & Multilateral Security

**Dr. Sebastian Pape**

Goethe University Frankfurt  
Theodor-W.-Adorno-Platz 4  
60629 Frankfurt, Germany

Phone +49 (0)69 798 34668

Fax +49 (0)69 798 35004

E-Mail: [sebastian.pape@m-chair.de](mailto:sebastian.pape@m-chair.de)

WWW: [www.m-chair.de](http://www.m-chair.de)