Let there be LITE: Design and Evaluation of a Label for IoT Transparency Enhancement

Alexandr Railean
Unabhängiges Landeszentrum für Datenschutz
Kiel, Germany

Institute of Computer Science
Georg-August-Universität Göttingen
Göttingen, Germany
arailean@datenschutzzentrum.de

Delphine Reinhardt
Institute of Computer Science
Georg-August-Universität Göttingen
Göttingen, Germany
reinhardt@cs.uni-goettingen.de

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

Copyright held by the owner/author(s).
MobileHCI '18 Adjunct, September 3–6, 2018, Barcelona, Spain
ACM 978-1-4503-5941-2/18/09.
https://doi.org/10.1145/3236112.3236126

Abstract
We present a "privacy facts" label, which aims at helping non-experts understand how an Internet of Things (IoT) device collects and handles data. We describe our design methodology, and detail the results of our user study involving 31 participants, assessing the efficacy of the label. The results suggest that the label was perceived positively by the participants, and is a promising solution to help users in making informed decisions.

Author Keywords
Internet of Things; IoT; privacy; usability; label.

ACM Classification Keywords
H.5.m [Information interfaces and presentation]: Miscellaneous; K.4.1 [Computers and society]: Public policy issues

Introduction
The IoT is composed of *devices, sensors or actuators, that connect, communicate or transmit information with or between each other through the Internet* [10]. Ubiquitous use of such technology can have major privacy implications for its users, as well as non-users, who may be unaware of IoT devices in their environment [1, 4]. For example, TV content can be identified from smart energy meter data [7]. Another problem is that users have little awareness of how the data collected by IoT devices are handled [11].

Figure 1: "Privacy facts" label for IoT devices.

```
customer number = 481-AHR-1831
temperature = 22 C
humidity = 34%
device Internet address =
93.184.216.34
```

Listing 1: QR code contents.

The *General Data Protection Regulation* (GDPR) aims to address some of these risks. It applies to entities that handle personal data of EU citizens, and requires organizations that legally control the data to "take appropriate measures to provide any information [..] relating to processing to the data subject in a *concise, transparent, intelligible and easily accessible form, using clear and plain language* [..]" [5]. In this paper, we map these requirements to a *Label for IoT Transparency Enhancement* (LITE), as shown in Fig. 1, that can be distributed with an IoT device, to assist potential buyers in protecting their privacy *before* acquiring the device. This is the earliest point in time, where important privacy-preserving decisions can be made [10]. The main contributions of our work are the label design and the conclusions of the user study we conducted to assess its clarity.

Requirements and Design Space Analysis

The primary goal for the label is to be informative, and answer these questions:

- *What* data are collected? (referred to as Q_{what})
- *What is the purpose* of collection? ($Q_{purpose}$)
- *Where* are the data stored? (Q_{where})
- *How long* are they kept? ($Q_{duration}$)
- *Who* has access to the data? (Q_{who})

The list is based on the GDPR and the transparency recommendations [2] of the *Article 29 Working Party* (WP29), an advisory group of representatives from European *Data Protection Authorities* (DPA). We then extend it with questions derived from autoethnographic observations:

- What do the data look like? (Q_{sample})
- How to access the data? (Q_{access})
- How frequently are the data sent? (Q_{freq})
- Which communications are protected? (Q_{sec})
- What paths do the data follow? (Q_{path})
- What information does the device receive from other sources? (Q_{rcv})

In addition, we set these usability requirements: facilitate side-by-side comparison, be compatible with printed and digital media, maintain utility even when shown in gray-scale, be short and simple. Finally, the label has to be future-proof, rather than over-fitted to a particular class of devices.

Label Design Methodology

We structure the design as follows: the *information area* on top is grouped by the questions Q_{what}, Q_{where}, $Q_{duration}$, Q_{who}, $Q_{purpose}$. It features a sample of collected data, in the form of a *Quick Response* (QR) code. The QR answers Q_{sample}, by illustrating a *concrete* set of values, which can improve understanding. For example, a "customer number" can look like "481-AHR-1831", but it could also take forms that reveal more information, e.g., an email address. To keep the label self-contained, the QR holds human-readable text, as seen in List. 1, rather than a link to a site.

The lower part is a *trace view* [6] of the data flows involving the IoT device, it answers Q_{sec}, Q_{path} and Q_{rcv}. It aims at helping users understand if they operate the IoT device directly, or if it relies on systems outside of their control.

We follow the visual guidelines compiled in List. 2. To make the text accessible to non-experts, we have avoided specialized terms, e.g., "Internet address" instead of "IP address". We choose words that have a more generic meaning, e.g., "software" instead of "firmware". We follow the *progressive disclosure* principle and omit low-level information. For instance, we use the padlock icons as security indicators, instead of mentioning algorithms and key lengths. This reduces clutter and removes terms that might not be clear to a novice. Another choice in favour of simplicity is to refrain from listing all the sensors, actuators and connec-

Listing 2: Visual design guidelines

- group related elements [9],
- use indentation to express hierarchy,
- facilitate quick scanning by using bullet points in lists
- and by emphasizing section titles,
- provide redundant encoding of information via icons,
- use gray-scale, to ensure that LITE is print-friendly and that color-blindness does not hinder readability,
- use additional emphasis to facilitate side-by-side comparison of key parameters,
- keep the number of elements at each level of abstraction below Miller's "magic number 7 ± 2" [8], to reduce the cognitive load when comparing devices.

tivity interfaces. Some devices may integrate mechanisms that are not exposed to users, e.g., noise-cancelling headphones may use microphones to improve noise suppression, possibly contradicting one's mental model of "headphones produce sound, they do not record it".

Further simplifications are achieved by focusing on *collected*, rather than transmitted data. The GDPR holds organizations accountable for the data they have, rather than the data which may be, in principle, extracted from the metadata of communication protocols, or derived via post-processing. This also guards against cases where an IoT device is privacy-friendly, while its accompanying smartphone application is not, as it may collect other data using the phone. Given that the data from the device and the smartphone end up on the same online service, they all become "collected data". As such, it would take a greater effort to conceal potentially abusive privacy practices.

The "purpose" section of the label guards against *purpose creep*, which occurs when collected data are used in ways other than originally declared. When this information is stated upfront, users can decide for themselves if the data are applicable to the purpose.

Evaluation

To test the clarity and readability of LITE, we have designed a study that elicits answers to questions about how a mock-up IoT product handles data.

Recruitment

In February 2018, 31 participants were recruited among the students and staff of the University of Karlstad, Sweden. To get a better approximation of non-expert consumers, we have focused our recruitment efforts on areas outside the computer science department. The invitation referred to an "evaluation of a privacy label for IoT (Internet of Things) products" and announced that 6 coupons for the university cafeteria worth 8.5 EUR (10.5 USD), would be randomly distributed after the study. No ethical committee approval was necessary according to the university's regulations.

Demographics

52% of the participants are female, 48% are male. 58% of the participants are between 18 and 26 years, followed by 27 and 35 years (35%). We measure their *self-reported* technical competence in Q_{12} (see Appendix A: Questionnaire), by assigning points to each skill, according to Tab. 1. The skill category is determined by the sum of points. As in [10], we have categorized participants with a total number of points below 8 as *novice*, between 8 and 20 as *medium*, and greater than 20 as expert. In our sample, 29% are classified as medium and 23% as novice, the rest are expert.

Experiment Settings

We first gave the participants a consent form, that explains how the information collected during the experiment will be used. Then, we provided a mock-up IoT device and a $128mm \times 40mm$ "privacy facts" label with these instructions: *"You are holding a prototype device produced by* Tesami GmbH*, it is called "Hausio" and it keeps track of the temperature and humidity in your house. The accompanying "privacy facts" label summarizes how the data are collected and handled. Take as much time as you want to examine the device and the label. When ready, please proceed to the questionnaire".* We then asked participants to examine the items and fill out our questionnaire, available in Appendix A. Participants were then left alone, having LITE with them all the time. When done, they notified the examiner, who asked follow-up questions and recorded the interview (average duration was 7 minutes).

A mock-up device is used to make the experiment more realistic and link LITE to a tangible item. We have used two

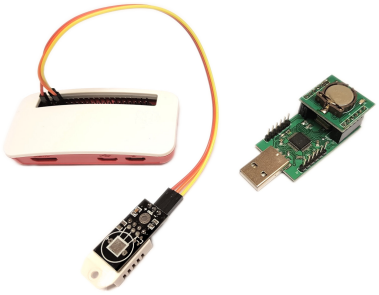


Figure 2: Mock-ups used: RasPi Zero with a DHT-22 sensor **(left)**, custom board **(right)**.

Points	Skills
2	play video games
2	browse the Internet and send emails
2	view photos and watch videos
2	use a word-processor to type documents
5	set up email sorting filters
5	type complex documents in word processors (e.g., macros, automatic indexes, dynamic fields)
10	assemble computers or other electronics from components
15	I know at least one programming language

Table 1: Distribution of points for each computer-related skill (Q_{12}).

mock-ups (Fig. 2), to check if there is any difference in responses depending on the device. Half of the participants were given a RasPi Zero, the other half got a custom board. We have chosen not to distribute the items in a product box, because it could potentially distract participants from the label, which is the focus of the study.

The transcripts were independently coded by two researchers, who counted the references to label sections, and tagged the participants' interpretation of the "product improvement" purpose listed on the label, as "suspicious" (e.g., intentionally vague, potentially abusive) or "not suspicious".

Results

For a quantifiable evaluation, we count the number of errors in the completed questionnaires, compiled in Fig. 3. The score treats any deviation from the correct answer as a separate error. For example, in Q_1 "what purpose are the data collected for?", the expected answer is to check "my personal use" and "scientific research", and to write "targeted ads" and "product improvement" in the custom fields. The following deviations would amount to 4 errors: checking another box (1 error), not checking one of the correct ones (1 error) and not filling out correct values in both custom fields (2 errors). The maximum number of errors one can make is 23. Note that Q_5 and Q_6 do not count towards this total, as they are open to interpretation and are exploratory.

We consider the following types of errors: *check incorrect* (i.e., a wrong box is checked), *uncheck correct* (i.e., a correct box is not checked), *custom missing* (i.e., a custom entry field was left empty), *custom incorrect* (i.e., a custom entry field contains an incorrect value).

Q_1 *What purpose are the data collected for?*
This entry has the largest number of errors, 87% of the participants made at least one. 54% of these errors are of the *custom missing* type, while none of the other questions have had such errors in their responses.

This could be an artifact of our questionnaire, as most participants have correctly checked the right options from the list, but did not fill in the custom ones, thus taking a penalty of 2 errors. It is also possible that the participants considered that the empty fields were optional, and that it was sufficient to check the correct items that were explicitly listed. Note that questions, which did not require hand-written options besides listed ones, were not subject to this effect.

It is also possible that participants interpreted "marketing offers" (listed) as "targeted advertisements" (had to be written by hand). 26% of the participants have done so, thus taking a penalty of 2 errors. One of the highest error rates was attained by P13, who has forgotten their glasses and used a smart-phone camera as a lens to read the materials.

These "traps" were deliberately placed into the questionnaire, while they increased the error rate, they suggest that LITE works better when used as a *reference*. This also emphasizes the importance of a well-defined vocabulary of terms, as minor inconsistencies lead to errors.

Q_2 *If the data were collected in the year 2045, what will be the last year in which they are still available?*
84% of the participants correctly answered "2048". We expected many off-by-one errors, however only one participant answered "2047". Another incorrect answer was "2042", which can be caused by a misinterpretation of the question. In this case, the participant subtracted the given interval, instead of adding it.

Q_3 *What information is collected?*
Although the complexity of Q_3 is comparable to Q_1, the error rate was substantially lower. 65% of the participants

have made no errors when answering it. There could be several reasons that explain the difference: the list of collected data features icons, while the list of purposes does not. However, the questionnaire itself did not include the icons, hence participants *could not have* relied on the graphics to identify the correct entries. Another possibility is that the correct answer required less effort, as there is no need to write custom texts, one simply had to check a subset of the listed options. Finally, the listed options were worded as on the label, thus reducing interpretation issues.

Q_4 *Which country are the data stored in?*
P13 skipped this question, while others have correctly written "France" in the custom field. It is worth noting that Q_4 did not provide options to choose from, there was only an empty field to write text in. This can explain the high number of "custom missing" errors for Q_1 and their absence in Q_4. Another possibility is that "France" on the label is highlighted, making it easier to see.

Q_5 *Who in Tesami GmbH can access the collected data?*
Since there is no such information on the label, this question has no exact answer. We use it to see how participants react, expecting no consensus. 36% chose "I don't know", 13% ticked all the available options, while 10% answered "not sure", "everyone?" or "it doesn't say". 45% of the participants chose various combinations of the listed options. During the interviews, they would come up with plausible explanations based on the purpose of collection, e.g., "but seeing product improvement and targeted advertisement, you can say it is the marketing staff that will get it" (P2).

Q_6 *Who can access the data while they are transmitted to Tesami?*
This question is open to interpretation, because the answer depends on one's assumptions about the system (e.g., type of encryption, network protocols in use). 61% indicated that Tesami can access the data while they are in transit, 16% stated that others in the household can do it, 10% chose "I don't know". Contrary to our expectations, only 6% considered that the government can access the data.

Q_7 *How many organizations can access the data after they were collected?*
The expected answer is "10", comprising Tesami and 9 affiliates. The answers were "9" (42%), "10" (19%), "9..10" or "9 affiliates" (16%), "I don't know" (10%), while 10% wrote "1", "1-2" or "1?". P16 skipped the question.

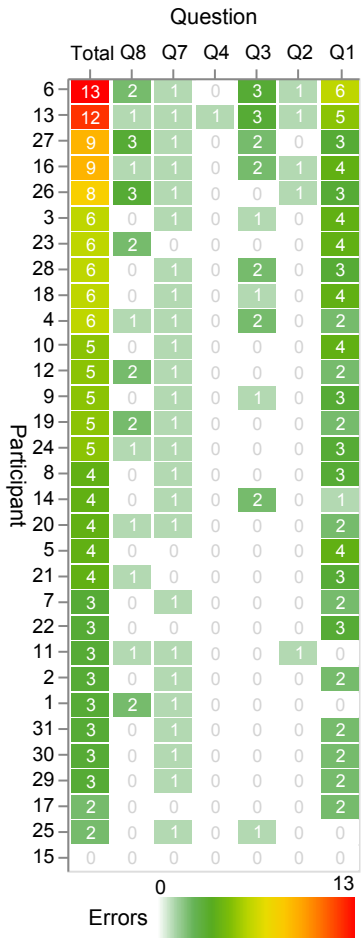
It is possible that the answer "9" is an off-by-one error. However, there was only one instance in Q_2, which could mean that something else has caused this discrepancy. It is also possible that some answered "9" because it is highlighted on the label, so they simply referred to that value.

Some participants have explicitly commented that "it depends on whether you count Tesami or not", it indicates that they understand the context, but the phrasing of the question made it difficult to settle on one interpretation. Some participants could have made a distinction between "organization" and "affiliate", hence answering "1", because the question asked about organizations, not affiliates.

Q_8 *Which of the following data transmissions are* not *protected?*
This question relies on the interpretation of padlock icons in the trace view. 55% of the participants answered correctly, 23% made one error, 7% chose "I don't know". Our analysis rules out the possibility that some participants did not notice the negation in the question, as we have not found answers that are the exact opposite of the correct one.

If participants understand the meaning of the padlock icon, they ought to answer the question correctly, otherwise they would make two errors, one for each use of the icon. The fact that 23% made only one error suggests that they did

Figure 3: The number of errors per participant per question.



not understand the principle, or that they understood it, but did not notice the other icon. It is worth noting that a participant who said they usually ignored icons, answered the question correctly (P22). Another one has realized during the interview that they made a mistake in the form (P23).

Other participants' comments indicate a clear understanding of the role of these icons, e.g., "it's my own data, and it's coming to me with some privacy, but my data is going to 9 affiliates without any privacy; isn't it odd?" (P30).

What do you think of when you read "product improvement"? Contrary to our expectations, this vague purpose statement did not raise suspicions among the participants. All the interpretations were positive, focusing on the product in general, e.g., "making the product better in the future" (P18), or on software updates: "I guess bug-fixes" (P24). One participant has emphasized that they are not concerned by this: "it makes me think of updates for the device perhaps [..] *I don't think that would be something that would feel like a concern to me*" (P20). P22 pointed out that there can be different interpretations: "Probably they would associate your preference with your customer number [..] I suppose, I have no idea at this point, this is speculation. It's quite rough... general, so it depends".

In their answers to Q_{13}, about the advantages and disadvantages of such labels, 68% of the participants consider that the label benefits consumers, e.g., "Yes. I think it is important to be very clear about what information will be gathered, how and by whom it will be used!" (P7), "I do think such kind of labels are essential" (P28). Two participants expressed concerns: "[..] it only informs me, but I cannot control the data or limit it" (P1) and "[..] if you only went of the label you might not find loopholes or other things a company could use/abuse" (P2).

In Q_{14} we have asked whether participants like or dislike to have such labels. 77% of them answered affirmatively: "I don't usually look at labels when I buy stuff, but I'd like to have this label" (P8), "Yes, I would like to see as much facts and descriptions as possible, so that I can make a better choice" (P23). None of the surveyed persons disliked the idea of having such labels.

Throughout the interviews, participants expressed satisfaction with the structure of the label and appreciated its contribution to transparency: "it feels like it is more open and more explanatory, they kind of show you their hand, like in poker almost. They don't try to hide it, they put an emphasis on it so you know about it. I think that is good for the customer" (P2). Others would point out that such information is hard to find: "usually this type of information is buried under a lot of paper" (P7). Some stated that they liked the brevity of the label: "privacy facts should be short, [..] I get so much data just by looking at that, [..] if you make it longer, I will probably not read it" (P10). A common theme was the desire to obtain more information about how the data are used, participants wanted to know who the affiliates were, and what parts of data they were getting. P19 suggested a folding label, like the ones used in medical products, which would allow more information to be provided "under the fold". Three participants questioned the authenticity of the label: "I need to feel that I trust the label itself" (P17), "labels can lie" (P9). Although such remarks were infrequent, contrary to our expectations, we believe that it is important to support LITE, e.g., via government-endorsed programmes [3]. Two participants expressed preference for a larger label, e.g., "it's pretty clear, but I would like it bigger" (P5). Some participants stated that they understand the label, but not the full implications: "I believe it is my IP address they're taking. But I don't really know how that affects me" (P18).

Section	Most interesting	Least interesting
Who	12	1
What	9	2
Trace	8	1
Purpose	7	0
Duration	1	3
QR	0	2
Where	0	2

Table 2: Most and least interesting sections of the label.

We have asked participants to point out which parts of the label were most and least interesting to them, mapping each response to an element of the label. A total of 37 "most interesting" mentions were made, and 11 "least interesting" ones (Tab. 2).

The answers to our follow-up questions reveal that all of the participants have noticed the QR code, however 10% did not know what it was, while 84% did not scan it, nor intended to. 77% noticed the rectangles that emphasize some parts of the label. In terms of interpretation, all participants stated that they understood the icons, 77% had no difficulties with the text. Although 16% did not know the word "affiliate", they understood it when the word "partner" was suggested.

Discussion

Participants wanted to know more details about the way the data are used by each affiliate. The folding label proposed by P19 is an elegant solution, as it keeps the label usable without relying on gadgets or online services.

The results suggest that efficiency can be improved through the use of standardized terms and icons. This would also make the labels consistent across vendors, making comparisons easier, and improve usability, by habituating consumers to these terms.

The fact that none of the participants had suspicions when interpreting "product improvement" (in the "purpose" section) indicates that additional measures are needed to protect consumers. This may be resolved by the introduction of consistent terminology and by legal means.

When it comes to the authenticity of the label itself, our results suggest that most of the participants trusted the information or did not voice their concerns about it.

Statistical analysis of the results did not reveal any correlations between error rates and age, gender, skill level or the mock-up used.

The various errors we measured have a different impact on transparency. For example, the belief that the data are accessed by 9 companies instead of 10 is inaccurate, but still good enough for practical purposes.

For LITE to stay relevant as products evolve, vendors should decouple security and privacy from feature updates. Thus, IoT devices stay current without breaking the terms shown on the label. If users choose to install an update that modifies data collection practices, an updated label can be shown and consent has to be requested again, per GDPR.

Conclusions

We have presented a "privacy facts" label for IoT devices and held 31 interviews to test it in practice. This is one out of many possible designs that meet the requirements, in this study we aimed for simplicity. The results are encouraging and they offer pointers for future work. For example, it is clear the creation of a standardized vocabulary and a common set of graphical primitives are important in the long term. Although we have found that participants tend to trust the information in the label, even in the absence of indicators of endorsement by regulators, we believe that such support will improve the viability of LITE.

Acknowledgments

This research has received funding from the H2020 Marie Sklodowska-Curie EU project "Privacy&Us" under the grant agreement No 675730. We thank the survey participants, Patrick Murmann for helping us analyze the transcripts, Harald Zwingelberg and the anonymous peer reviewers for their helpful comments.

Appendix A: Questionnaire

Please fill out this questionnaire. Feel free to go back to the label at any time. You can take notes and *use any tools and gadgets* at your disposal. This is not an exam, and there are no wrong answers or grades.

1. What purpose are the data collected for? (multiple choice possible)

☐ marketing offers
☐ home automation
☐ automatic billing
☐ my personal use
☐ scientific research
☐ _____
☐ _____
☐ I don't know

2. If the data were collected in the year 2045, what will be the last year in which they are still available?

○ _____ ○ I don't know

3. What information is collected? (multiple choice possible)

☐ current time
☐ device Internet address
☐ my customer number
☐ temperature
☐ my name
☐ number of computers in my home
☐ humidity
☐ my phone number
☐ _____
☐ I don't know

4. Which country are the data stored in?

○ _____ ○ I don't know

5. Who in Tesami GmbH can access the collected data? (multiple choice possible)

☐ software engineers
☐ hardware engineers
☐ research & development dept.
☐ marketing staff
☐ company director
☐ _____
☐ _____
☐ I don't know

6. Who can access the data while they are transmitted to Tesami GmbH? (multiple choice possible)

☐ others in my home
☐ my neighbors
☐ Tesami GmbH
☐ my Internet provider
☐ the IoT device
☐ the government
☐ _____
☐ _____
☐ I don't know

7. How many organizations can access the data after they were collected?

○ _____ ○ I don't know

8. Which of the following data transmissions are ***not*** protected? (multiple choice possible)

☐ data sent from device to Tesami
☐ updates sent from Tesami to the device
☐ data sent from Tesami to you
☐ data sent from Tesami to affiliates
☐ I don't know

9. Do you have a QR-scanner program in your smartphone?

○ yes ○ no
○ I don't have a smartphone
○ I don't know
○ prefer not to say

10. What is your age?

○ 18..26 ○ 45..53
○ 27..35 ○ 54 and above
○ 36..44 ○ prefer not to say

11. What is your gender?

○ male ○ other
○ female ○ prefer not to say

12. Please specify the computer-related skills you have

☐ play video games
☐ view photos and watch videos
☐ browse the Internet and send emails
☐ use a word-processor to type documents
☐ set up email sorting filters
☐ type complex documents in word processors (e.g., macros, automatic indexes, dynamic fields)
☐ assemble computers or other electronics from components
☐ I know at least one programming language

13. Do you see advantages/disadvantages in having such labels on products in the future?

14. Would you like/dislike to have such product labels in the future?

These questions are asked to elicit qualitative data after the survey is filled out:

- Have you encountered any difficulties in understanding the information on the label? If yes, which ones?
- Have you encountered any difficulties in understanding the icons on the label? If yes, which ones?
- Which content has been particularly interesting/not interesting to you?
- What do you understand when reading "personal use" and "product improvement"?
- Have you seen that some of the elements of the label are highlighted? How have you interpreted that emphasis?
- How do you interpret the image in the hand of the human figure?
- Do you know what this figure [QR] is, and what can be done with it?
- What other comments have you got about the "privacy facts" label?

References

1. Noura Aleisa and Karen Renaud. "Privacy of the Internet of Things: A Systematic Literature Review". In: *Proc. of HICSS* (2017).
2. Article 29 Working Party. *Guidelines on Transparency Under Regulation 2016/679*.
3. Abhijit Banerjee and Barry D. Solomon. "Eco-Labeling for Energy Efficiency and Sustainability: A Meta-Evaluation of US Programs". In: *Energy Policy* (2003), pp. 109–123.
4. David De Cremer, Bang Nguyen, and Lyndon Simkin. "The Integrity Challenge of the Internet-of-Things (IoT): on Understanding its Dark Side". In: *Journal of Marketing Management* (2017), pp. 145–158.
5. European Parliament and Council of European Union. "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". In: *Official Journal of the European Union* (2016), pp. 1–88.
6. Simone Fischer-Hübner et al. "Transparency, Privacy and Trust–Technology for Tracking and Controlling My Data Disclosures: Does This Work?" In: *Proc. of IFIP TM*. 2016, pp. 3–14.
7. Ulrich Greveler et al. "Multimedia Content Identification Through Smart Meter Power Usage Profiles". In: *Proc. of IKE*. 2012, p. 1.
8. George A Miller. "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information". In: *Psychological review* (1956), p. 81.
9. Patrick Moore and Chad Fitz. "Gestalt Theory and Instructional Design". In: *Journal of Technical Writing and Communication* (1993), pp. 137–157.
10. Alexandr Railean and Delphine Reinhardt. "Life-Long Privacy in the IoT? Measuring Privacy Attitudes Throughout the Life-Cycle of IoT Devices". In: *IFIP International Summer School on Privacy and Identity Management*. 2017, pp. 132–149.
11. Jessica Vitak et al. "Privacy Attitudes and Data Valuation Among Fitness Tracker Users". In: *iConference*. 2018, pp. 229–239.