Communicating Privacy: User Priorities for Privacy Requirements in Home Energy Applications

Lisa Diamond, Peter Fröhlich

Communicating Privacy: User Priorities for Privacy Requirements in Home Energy Applications

Lisa Diamond[1] and Peter Fröhlich[1]

[1] AIT Austrian Institute of Technology, Giefinggasse 2, 1210 Vienna, Austria
lisa.diamond@ait.ac.at

Abstract. Perceived privacy plays a crucial role in the acceptance of technologies that rely on sensitive data. To mitigate concerns and build trust, privacy must not only be protected, but this protection should also be successfully communicated. Residential energy consumption data are at the center of applications that facilitate improved energy management and support a more sustainable future, but such data are privacy-sensitive since they have the potential to reveal a great number of details about the daily life of users. Our study contributes to an understanding of how to communicate energy data privacy via user interfaces by looking into the relevancy and accessibility priorities of potential privacy requirements in home energy monitoring, management, and production applications. All investigated requirements showed themselves to be of relevance to users, with control aspects (access, transfer, and deletion of data) being both perceived as most important and receiving the highest accessibility priority ratings, and control of data storage joining them as top access priority requirement. Our results indicate that placing the settings and information emphasized in our results prominently in the user interface, going through extra effort to ensure easy comprehensibility, and communicating them proactively, is likely to go a long way in successfully communicating privacy. Investigation of accessibility priority differences in relation to data storage location provided less clear answers but suggests a higher importance of access to general information on data collection if data are stored centrally and of the ability to view data if stored decentrally.

Keywords: Privacy Requirements, Usable Privacy, Smart Grid

1 Introduction

Privacy is a sensitive issue for smart services and systems [1], which present a considerably larger risk for misappropriation or illegal access to personal information due to the continuous and often extensive data collection and data exchange between an ever-increasing number of connected devices [2]. Home Energy applications are prime suspects for privacy concerns because the energy usage data at their center can reveal a lot of details about the home life of end-users and can contain further user-related information such as name, billing number and account details. If users feel that their privacy is threatened when using a service or a product, they react, and acceptance suffers. This

has already affected smart meter introduction negatively, leading to a significantly delayed smart meter roll-out in Denmark [3].

There is a strong awareness of potential privacy and security risks in the smart grid community that has prompted a multitude of work to develop appropriate protection mechanisms [4, 5]. But without successful communication of such protection to end-users the risk of diminished acceptance remains. Only if end-user privacy is not just established, but also successfully communicated and consequently experienced, can adverse emotional and business consequences be avoided, and the related products and services be realized to their full potential.

Research on how to communicate (and enable management of) privacy has covered a wide range of different tools, mechanisms and features including creative user interface design solutions for individual challenges [6], methods to raise disclosure awareness [7–9], and ways to reduce the cognitive load of users [10, 11]. However, to the best of our knowledge, there has not been a user requirements investigation looking at a comprehensive compendium of potential privacy features that could be communicated by a system to its users with regards to their comparative importance to users. Such information is, however, of great value to designers of smart services as it can serve as a guide for decisions such as which privacy features should receive special attention and be placed most prominently in the interface in order to communicate the protection of privacy to its users efficiently and effectively. Since interface space as well as human attention and cognition are limited it is important to make informed choices as to which content and features should be prioritized in terms of placement and active vs. passive communication.

In this paper, we present a questionnaire study that investigates people's preferences about privacy information and features that can be integrated into the user interfaces of home energy monitoring and management applications such as smart meters or smart home technologies and discuss practical implications of the results. Our guiding research questions were: Can all identified requirements be regarded as relevant and which ones are most important (RQ1), to what extent does perceived relevancy match desired accessibility (as in easy to locate) within the interface (RQ2) and are there differences regarding accessibility preferences depending on data storage location (RQ3).

2 Background and literature review

2.1 Privacy and The Smart Grid

The smart grid is heralded as the next generation of the electricity supply network, aiming to strengthen grid reliability, and prepare it for future needs [12]. Consumers are connected to the smart grid via smart meters which record energy usage data in short intervals of typically 15 minutes to 1 hour [13]. Fed back into the grid, these consumption data can facilitate efficient network management, outage detection, mapping and restoration, asset management, load forecasting, and power quality monitoring, as well as open up opportunities of demand-side management through manual or automated load shifting [14].

Within the home of the consumer, the recorded energy usage data enables active end-user participation in several forms. Most directly, it allows home owners to monitor energy usage via smart meter portals, deepening a consumer's understanding of household energy usage patterns and facilitating their adjustment [15]. Other forms of use are within energy management systems or for prosumer technologies [16, 17]. Such uses can enable financial savings and provide an important contribution to a sustainable future - but they rely on the recording and transmission of energy consumption data.

For private consumers connected to the smart grid this means the collection, storage and transmission of vast quantities of personal data containing information on household energy usage. And with the collection of these data comes the risk of their abuse. Presence or absence of household occupants can be revealed and daily device usage and behavioral routines of users such as when somebody in a household ate and showered can be deduced [18, 19]. With sufficiently detailed consumption data and the appropriate comparison patterns it even becomes possible to derive which specific devices can be found in a household and which TV programs are watched [18–20]. Passwords, smart meter IP address, customer name and address, billing information, and bank account number are also at risk [18, 21, 22] and the opportunities for misappropriation of such information are manifold.

2.2 Energy Consumer Privacy Concerns and Needs

Not surprisingly, data privacy and security concerns are very much on the mind of users if they are asked to discuss their hopes and concerns around smart meters, their energy data, and applications relying on these data. In a large-scale study conducted by O_2 in the UK in 2013, 59% of the participants who did not want smart meters installed named privacy concerns as their most central concern [23] and the Boston Consulting Group reported 41-48% of their study participants to be concerned about privacy, security, and the disclosure of smart meter data to third parties [24]. A closer look at different aspects of such concerns show 49% to be worried about data accuracy, 38% about missing information on and control over data collection, access and use, and 36% about both illegal accessing of their data in order to use gained insights for targeted crimes, as well as the misappropriation of data obtained legally by the provider [25].

In the smart home context, perceived privacy risks are also a prevalent concern. Both Krishnamurti et al. [26] and Balta-Okzan et al. [27] list invasion of privacy and loss of control next to rising costs as the main concerns in the context of smart meters and smart homes. Paetz, Dütschke and Fichtner [16] name protection of privacy in smart homes as the most important concern of study participants independent of age.

Turning towards privacy requirements rather than concerns, being able to control one's energy consumption data oneself appears to be the most prominent requirement with study participants in a number of studies emphasizing the wish to have sole access and control of high granularity data [28], to be able to limit access and prevent the selling of data to third parties (90%), control the use of collected data (88%) and be able to access and potentially correct data (84%) [29]. Döbelt et al. [30] investigated consumer-driven energy data privacy concerns in Austria via an online survey and complementary focus groups and recommend based on their results that consumption data

be stored as decentralized as possible, clear statements on which data are collected and how they are used, and the provision of access control mechanisms to consumers.

Consumer Futures [31] developed a "Privacy Charter", a document providing consumers with the most critical information surrounding smart meters with regards to privacy. This charter includes (1) information on what the data will be used for, (2) why these data are needed and how they differ from data currently collected, (3) who will be responsible for obtaining the data and keeping it safe, (4) which choices are available to consumers, (5) which consumer benefits are connected with data collection, and (6) where more information can be found. The study concludes that providing consumers with choices how data are collected and managed is critical, as well as giving context information, information on who can access data and whether consumers have a choice with regards to this. Further, it is important to reassure end-user about data security.

3 Methods

Based on the results of the literature research and current data protection guidelines such as the privacy protection guidelines published by the Institute of Standards and Technology (NIST) [22] and the new European General Data Protection Regulation (GDPR), a set of core privacy requirements was compiled. The list was evaluated via a small preliminary questionnaire study [32] and detailed further through a number of interviews with stakeholders from the energy sector and consumer representatives, as well as through end-user feedback collected in a focus group. Through this process we identified 21 distinct requirements (see Table 1 under *4* for the full list).

In order to answer our research questions, we conducted an online questionnaire study with 312 participants recruited via a panel and approximately representative of the Austrian population. It was composed as follows: 51.6% female, 48.4% male (gender); 13.7% 16-29 years, 19.2% 30-39 years, 25.3% 40-49 year, 19.9% 50-65 years, 11.9% 66+ years (age); 9.6% completed compulsory schooling, 43.9% an apprenticeship, 21.2% a technical/trade school, 15.4% high school and 9.9% university (educational level). Participants' technological affinity and general privacy concerns, measured with 3 items each adapted from existing instruments [33, 34] on a 5-point scale, were slightly above scale-average (*m=3.44* with *sd*=0.99 and *m=3.50* with *sd=0.78*, respectively), and they had very positive attitudes towards sustainable energy production and consumption (m=4.14 with *sd=0.93*) (3 items developed by the authors).

In the first part of the questionnaire, survey participants were introduced to home energy applications and the role of their energy consumption data within them. They were asked to rate the 21 final requirements with regards to their relevance for the communication of data privacy on a 5-point Likert scale ranging from *1 = not at all important* to *5 = very important*. In the second part of the questionnaire the respondents were presented with the task of sorting the previously introduced 21 privacy requirements within 4 prioritization categories concerning accessibility and visibility within the user interface. Category 4 was described as "*High priority: As accessible as possible within the user interface*", category 3 as "*Medium priority: Easily accessible but does not have to be directly visible*", category 2 as "*Low priority: Does not have to be*

particularly accessible", and category 1 as "*Not relevant: I don't need this in the user interface at all*".

Participants were asked to sort the requirements twice under 2 different scenarios: Scenario 1 was described as a user interface for a service/product for which collected data would be stored and processed externally on a central server of the organization responsible (example: smart meter web portal). Scenario 2 was described as a user interface for a service/product for which collected data would be stored and processed locally or within a user-associated cloud storage (example: a smart home system with local data storage). Figure 1 shows a screenshot of the online card sorting task. There was no limit to the number of requirements per priority level.

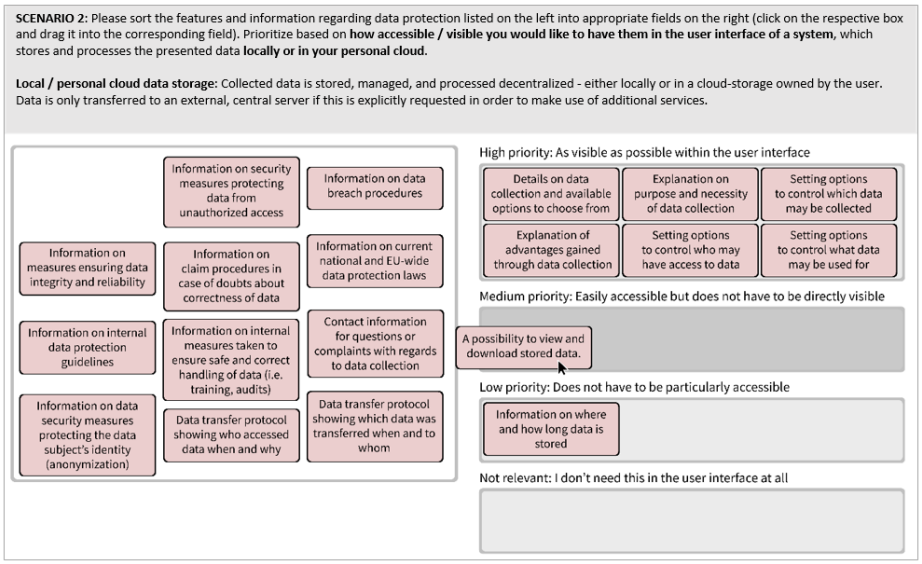

Fig. 1. Screenshot of the privacy requirement accessibility prioritization sorting task within online questionnaire; participants were asked to sort the different requirement cards according to desired accessibility in the appropriate field

4 Results

To verify internal consistency of the privacy requirements concept, Cronbach's alpha was calculated for the requirement scale and proved to be satisfying at *0.85*. To validate the relevancy of all presented requirements and answer RQ1, the percentage of participants rating a requirement as important with regards to privacy communication (rating 4 or 5 with 5 being "*very important*") was determined. All privacy requirements included in the questionnaire showed average ratings of above 50%. To determine which requirements were most important, the ones displaying a "top relevancy" with over 50% of the participants rating them with the highest score (5), were identified. Such "top requirements" are *Data Access Settings*, *Data Use Settings*, *Data Delete Settings*, and *Data Access Transparency*. All requirements showed statistically significant, very

weak to weak positive correlations with age (ranging between *0.16* and *0.3*, $p<.05$) with the ones between age and availability of *Data Storage Settings*, *Data Delete Settings*, *Benefit Information*, *Claim Procedure Info* and *Contact Info* being the strongest at $r=0.25$ or above. There were no statistically significant sex differences concerning perceived requirement relevancy.

Table 1. Privacy requirement relevancies and scenario-dependent accessibility priorities

Privacy requirement	Requirement type	Relevancy	Top-relevancy	Access priority centr.	Access priority decentr.
Data Access Settings	Control	75.0%	58.0%	high	high
Data Use Settings	Control	74.0%	52.9%	high	high
Data Delete Settings	Control	71.8%	55.1%	high	high
View Data	Transparency	70.8%	49.0%	medium	high
Data Access Transparency	Transparency	70.5%	50.0%	medium	medium
Breach Procedure Info	Security	70.2%	45.5%	medium	medium
Data Transfer Transparency	Transparency	69.9%	48.4%	medium	medium
Data Anonymization Info	Security	69.6%	49.0%	medium	medium
Data Collection Purpose Info	Info	69.2%	47.1%	medium	medium
Data Security Info	Security	68.9%	47.4%	medium	medium
Data Safety and Integrity Info	Security	68.3%	43.9%	medium	medium
Contact Info	Accountability	66.3%	43.6%	medium	medium
Claim Procedure Info	Accountability	65.1%	46.2%	medium	medium
Data Storage Settings	Control	64.1%	36.2%	high	high
Benefit Information	Information	63.8%	35.9%	medium	medium
Data Storage Transparency	Transparency	63.5%	40.7%	medium	medium
Download Data	Transparency	60.3%	37.5%	medium	medium
Data Protection Laws	Accountability	59.3%	34.9%	low	low
Internal Data Protection Guidelines	Accountability	55.1%	31.4%	low	low
General Information on Data Collection	Information	54.8%	34.6%	high	medium
Other Data Protection Measures	Security	52.2%	33.0%	low	low

In order to answer RQ2, we looked at the accessibility priorities of each requirement based on the observed median according to the sorting performed by the participants. All presented requirements received medians above 1 in both scenarios (external and local data storage) and are therefore not only perceived as relevant but participants wanted to be able to access them via the system interface. Further, in both scenarios the

control-related requirements, which were identified as top requirements via the relevancy ratings, also received top accessibility priority (md=4). There were 2 noticeable differences: Data Storage Settings, the 4th control-related requirement, which did not receive a top-relevancy rating but was in the lower half of average relevancy ratings, did, however, receive top accessibility priority in both tested scenarios. Second, General Information on Data Collection, which displayed the 2nd-lowest average relevancy, was seen to be of high accessibility priority under centralized data storage conditions and medium priority under decentralized storage conditions. Further, Data Access Transparency was, despite its top relevancy ratings, not a top accessibility priority in either scenario.

Answering RQ3 required a detailed look at rating differences between the 2 storage scenarios. Differences concerning top accessibility priority with regards to storage location were observed in 2 requirements: *General Information on Data Collection* received a top accessibility priority sorting when data was stated as stored centrally but not when it was stated as stored locally. The *View Data* requirement showed the opposite. In a last step, we looked at statistically significant differences concerning top accessibility depending on storage location. Wilcoxon signed rank tests indicated significant sorting differences for 4 requirements (the familywise error rate was controlled with the Bonferroni-Holm correction): *Benefit information* (*Z=-2.61; p=.009* with *alpha=.013*), *Data Transfer Transparency* (*Z=-2.92; p=.003* with *alpha=0.017*), *View Data* (*Z=-3.83; p=.000* with *alpha=0.05*) and *Download Data* (*Z=-3.41; p=.001* with *alpha=0.025*) all were sorted into a higher accessibility priority category more often, when data storage was described as decentralized / local. The detailed results of the findings reported above can be found above in Table 1.

5 Discussion and Conclusions

The results of this study give readers an insight into user priorities with regards to privacy features in Internet of Things applications processing energy usage data. Our results provide a systematic and formal confirmation of the relevancy of privacy aspects typically included in privacy protection plans – control, transparency, security, information and accountability – from an end-user perspective. They further show control related requirements to be most important for end-user privacy experience both in terms of perceived relevancy and required accessibility within the interface. To successfully communicate privacy, control-related information and setting options should therefore receive special attention by placing them more prominently in the user interface of energy management applications than is practice nowadays, assuring excellent usability use via user-centered design approaches, and communicating them more proactively.

Looking at the applicability of these findings, our results suggest that user interface designers for home energy management applications consider the following recommendations:

- Place the information and settings that received top accessibility (as in easy to locate) priority ratings – data storage, data access, data use and delete settings, as well as general information on energy data collection and a possibility to view data – in

highly visible and accessible spots and stress their existence, e.g. via a privacy-related wizard or other approaches to inform end-users proactively. They should receive special attention during the developmental phase in order to ensure that they are comprehensible to end-users and that their implications are clear. They should be linked to all related spots and potentially proactively provided in relevant moments e.g. via "Just-In-Time-Click-Through Agreements" [47].

- Functions with medium prioritization such as information on security measures or breach procedures do not require quite as prominent spots – they should be easy to access but do not need to be actively "pushed" and, although comprehensibility is still important, do not need as many iterations and feedback-rounds. We would suggest placing them such that they can be easily located through a "further information and settings" link and inform end-users about them proactively once. Regarding transparency related requirements, visual data privacy diagrams [23] that allow access to more detailed information might be an attractive approach.
- Functions with low prioritization such as general and internal data protection guidelines should be accessible but do not need to be promoted to users – they just need to be "there" if someone is actively looking for them. It is also of less importance to optimize their comprehensibility as they are less likely to be perused in detail.

The differences in requirement prioritization between the two presented data storage scenarios were minimal, indicating that data storage location does not greatly affect which privacy requirements are deemed most important regarding accessibility. There does, however, seem to be a somewhat higher interest in transparency-related requirement accessibility under local data storage conditions. We interpreted this as increased interest in the data, potentially motivated through a stronger sense of "ownership" and suggest underlining data ownership through wording and visual cues that add a sense of confirmation in this regard to increase the privacy comfort levels of home owners.

Finally, we want to emphasize the importance of simplicity, efficiency and effort minimization in privacy communication. Our days are full and busy, there is already an overwhelming amount of information to constantly process and control is a "finite resource". Our data are processed everywhere – it is impossible to control all details and there comes a point where control becomes meaningless. We will need to find a middle road – a way to enable users to control their data without overwhelming them to a degree that they click through checkboxes without reading just to cope with the sheer amount of them. Tackling this challenge will be an interesting task for future research in this field and we hope that our findings can provide a contribution by clarifying what needs highlighting and what simply needs to be available if searched for, so that privacy can be communicated sufficiently without taxing end-user attention unnecessarily.

Acknowledgements. The work presented in this paper has received funding from the Austrian Research Promotion Agency FFG under grant agreement n° 848811 (RASSA).

References

1. Hong, J.: The privacy landscape of pervasive computing. IEEE Pervasive Computing. 16, 40–48 (2017).
2. Chow, R.: The last mile for IoT privacy. IEEE Security & Privacy. 15, 73–76 (2017).
3. Cuijpers, C., Koops, B.-J.: Smart Metering and Privacy in Europe: Lessons from the Dutch Case. Social Science Research Network, Rochester, NY (2013).
4. Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L.: A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities and Society. 38, 806–835 (2018).
5. Uludag, S., Zeadally, S., Badra, M.: Techniques, taxonomy, and challenges of privacy protection in the smart grid. In: Privacy in a Digital, Networked World. pp. 343–390. Springer (2015).
6. Jackson, C.B., Wang, Y.: Addressing The Privacy Paradox through Personalized Privacy Notifications. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2, 68 (2018).
7. Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M.: Nudges for privacy and security: understanding and assisting users' choices online. ACM Computing Surveys (CSUR). 50, 44 (2017).
8. Patrick, A.S., Kenny, S.: From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In: Privacy Enhancing Technologies. pp. 107–124. Springer (2003).
9. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a GDPR-compliant and usable privacy dashboard. In: IFIP International Summer School on Privacy and Identity Management. pp. 221–236. Springer (2017).
10. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A nutrition label for privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security. p. 4. ACM (2009).
11. Fox, G., Tonge, C., Lynn, T., Mooney, J.: Communicating compliance: developing a GDPR privacy label. (2018).
12. Tuballa, M.L., Abundo, M.L.: A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews. 59, 710–725 (2016). https://doi.org/10.1016/j.rser.2016.01.011.
13. McKenna, E., Richardson, I., Thomson, M.: Smart meter data: Balancing consumer privacy concerns with legitimate applications. Energy Policy. 41, 807–814 (2012). https://doi.org/10.1016/j.enpol.2011.11.049.
14. Dütschke, E., Paetz, A.-G.: Dynamic electricity pricing—Which programs do consumers prefer? Energy Policy. 59, 226–234 (2013). https://doi.org/10.1016/j.enpol.2013.03.025.
15. Karlin, B., Zinger, J.F., Ford, R.: The effects of feedback on energy conservation: A meta-analysis. Psychological Bulletin. 141, 1205–1227 (2015). https://doi.org/10.1037/a0039650.
16. Paetz, A.-G., Dütschke, E., Fichtner, W.: Smart homes as a means to sustainable energy consumption: A study of consumer perceptions. Journal of consumer policy. 35, 23–41 (2012).
17. Zafar, R., Mahmood, A., Razzaq, S., Ali, W., Naeem, U., Shehzad, K.: Prosumer based energy management and sharing in smart grid. Renewable and Sustainable Energy Reviews. 82, 1675–1684 (2018). https://doi.org/10.1016/j.rser.2017.07.018.
18. Cho, H.S., Yamazaki, T., Hahn, M.: AERO: extraction of user's activities from electric power consumption data. IEEE Transactions on Consumer Electronics. 56, 2011–2018 (2010). https://doi.org/10.1109/TCE.2010.5606359.

19. McDaniel, P., McLaughlin, S.: Security and Privacy Challenges in the Smart Grid. IEEE Security Privacy. 7, 75–77 (2009). https://doi.org/10.1109/MSP.2009.76.
20. Cárdenas, A.A., Safavi-Naini, R.: Security and Privacy in the Smart Grid. In: Handbook on Securing Cyber-Physical Critical Infrastructure. pp. 637–654. Elsevier (2012).
21. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private Memoirs of a Smart Meter. In: Proceedings of the 2Nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building. pp. 61–66. ACM, New York, NY, USA (2010). https://doi.org/10.1145/1878431.1878446.
22. National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Guidelines for Smart Grid Cyber Security. Vol. 2, Privacy and the Smart Grid (NISTIR 7628r1). National Institute of Standard and Technology (NIST), U.S. Department of Commerce (2014).
23. O2: Effectively engaging consumers to ensure smart meter success. (2013).
24. Seshadri, P., Barton, C., Manfred, K.: Capturing the Value of Smart Meters, www.bcgperspectives.com, (2010).
25. Valocchi, M., Juliano, J.: Knowledge is power: Driving smarter energy usage through consumer education. IBM Institute for Business (2012).
26. Krishnamurti, T., Schwartz, D., Davis, A., Fischhoff, B., de Bruin, W.B., Lave, L., Wang, J.: Preparing for smart grid technologies: A behavioral decision research approach to understanding consumer expectations about smart meters. Energy Policy. 41, 790–797 (2012). https://doi.org/10.1016/j.enpol.2011.11.047.
27. Balta-Ozkan, N., Davidson, R., Bicket, M., Whitmarsh, L.: Social barriers to the adoption of smart homes. Energy Policy. 63, 363–374 (2013).
28. Wimberly, J.: Separating Smart Grid from Smart Meters? Consumer Perceptions and Expectations of Smart Grid. EcoAlign (2010).
29. Lundin, B.V.: Breaking down consumer privacy barriers, http://www.smartgridnews.com/story/breaking-down-consumer-privacy-barriers/2015-03-10, last accessed 2015/03/14.
30. Döbelt, S., Jung, M., Busch, M., Tscheligi, M.: Consumers' privacy concerns and implications for a privacy preserving Smart Grid architecture—Results of an Austrian study. Energy Research & Social Science. 9, 137–145 (2015). https://doi.org/10.1016/j.erss.2015.08.022.
31. Consumer Futures, R.: Smart and clear. Customer attitudes to communicating rights and choices on energy data privacy and access. (2014).
32. Diamond, L., Schrammel, J., Fröhlich, P., Regal, G., Tscheligi, M.: Privacy in the smart grid: end-user concerns and requirements. In: Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct. pp. 189–196 (2018).
33. Smith, H.J., Milberg, S.J., Burke, S.J.: Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly. 20, 167 (1996). https://doi.org/10.2307/249477.
34. Karrer, K., Glaser, C., Clemens, C., Bruder, C.: Technikaffinität erfassen–der Fragebogen TA-EG. Der Mensch im Mittelpunkt technischer Systeme. 8, 196–201 (2009).