Privacy in the Smart Grid: End-User Concerns and Requirements

Lisa Diamond
Johann Schrammel
Peter Fröhlich
Georg Regal
AIT Austrian Institute of Technology, Center for Technology Experience
1210 Vienna, Austria
Lisa.Diamond@ait.ac.at
Johann.Schrammel@ait.ac.at
Peter.Froehlich@ait.ac.at
Georg.Regal@ait.ac.at

Manfred Tscheligi
University of Salzburg
5020 Salzburg, Austria
Manfred.Tscheligi@sbg.ac.at

AIT Austrian Institute of Technology, Center for Technology Experience
1210 Vienna, Austria

MobileHCI '18 Adjunct, September 3–6, 2018, Barcelona, Spain

ACM ISBN 978-1-4503-5941-2/18/09.
https://doi.org/10.1145/3236112.3236139

Abstract
Mobile interfaces will be central in connecting end-users to the smart grid and enabling their active participation. Services and features supporting this participation do, however, rely on high-frequency collection and transmission of energy usage data by smart meters which is privacy-sensitive. The successful communication of privacy to end-users via consumer interfaces will therefore be crucial to ensure smart meter acceptance and consequently enable participation. Current understanding of user privacy concerns in this context is not very differentiated, and user privacy requirements have received little attention. A preliminary user questionnaire study was conducted to gain a more detailed understanding of the differing perceptions of various privacy risks and the relative importance of different privacy-ensuring measures. The results underline the significance of open communication, restraint in data collection and usage, user control, transparency, communication of security measures, and a good customer relationship.

Author Keywords
Privacy; smart grid; user requirements.

ACM Classification Keywords
H.1.2 User/Machine Systems: Human Factors;

Introduction and Background

Energy demand is on the rise while the need to meet this demand in a sustainable way is becoming ever more urgent. The smart grid as the next generation of our electricity network aims to do so via the application of information and communication technologies, facilitating the integration of more volatile and distributed renewable energy resources [1,18]. At the core of a functional smart grid stands its ability to "see" (and react to) what is happening in the electricity network. Consumers have the potential to contribute in 2 important ways: Passively, via the acceptance of smart meters into their homes and by allowing a sufficiently frequent collection and transmission of energy usage data (a high rather than low data granularity); and actively, through efforts to reduce overall energy consumption via behavioral changes, load shifting to relieve the grid during peak times, and the installation of prosumer technologies such as solar panels or heat pumps [10,19]. Consumers are therefore valuable partners to the smart grid and engaging them to participate both passively and actively is crucial if the smart grid is to meet its full potential.

Smart grid consumer interfaces, connecting end-users to their smart meters and through the smart meters to the grid, will play a central role in recruiting consumers as participants: Through the provision of energy feedback based on smart meter data, giving users a clearer overview and better understanding of how they use energy in day-to-day life; through alert possibilities when a certain amount of energy has been consumed; through playful engagement strategies such as energy saving challenges; or in combination with home automation aimed at optimizing energy usage within the household and enabling automatic load shifting in connection with time-of-use tariffs or peak incidents. Mobile phones or tablets suggest themselves as ideal ways for consumers to connect with their smart meters. They have a low usage barrier as they do not require the purchase of new, costly devices, complex installation or getting used to a completely new system [13,22]. Further, they tend to be already well integrated in daily life with a large percentage of users, ensuring a relatively prompt reception of often time-sensitive information. It can therefore be assumed, that mobile devices will develop into a standard user access point to the smart grid and communication with users will centrally run through mobile applications.

To make consumer participation in the smart grid possible in the first place, a consumer has to accept the technology that connects him or her to the smart grid: The smart meter that captures and transmits the household energy usage data. Further, the transmitted data needs to be of sufficiently high granularity to enable useful energy feedback, the use of variable tariffs, alerts, and the like. Such data is, however, privacy-sensitive as it contains vast quantities of detailed information on energy used throughout day and night, potentially enabling the deduction of very sensitive information such as presence and absence patterns, which devices are used in the household and when, and, depending on data granularity, even which TV program was watched [11,20]. Not surprisingly, privacy concerns are therefore one of the most central concerns raised against smart meters and can present a substantial barrier to smart meter acceptance if they are not sufficiently addressed [6].

As a topic, privacy within the smart grid and its applications has already drawn significant attention. It has been acknowledged as a common and valid user concern [14,20] and a lot of work has been done around *privacy by design* aspects [e.g. 2,4,5] and privacy-enhancing technology (PET) development [e.g. 7,8]. End-users most commonly express a general concern about a lack of control over collected data and about its potentially revealing nature rendering them "transparent". If discussed in more detail, specific concerns include: Profiling and targeted advertising based on unauthorized data analysis revealing behavioral patterns or information on device usage; data disclosure or selling of data to third parties without consent; negative financial consequences due to data manipulation or incorrect measurements; or burglaries informed by absence patterns visible in the collected data [16,17,21] (for an extended list please see the risks included in our questionnaire and stated in tab. 1).

Most publications discussing privacy concerns did not use a quantitative approach to distinguish between different risks and were therefore not able to compare voiced concerns in terms of perceived risk. Further, discussed measures to meet and mitigate privacy concerns focus on technical and legal aspects and not on end-user perception. Even though establishing privacy from a technical and legal perspective is crucial and a prerequisite, attitudes will only be affected if end-user requirements are understood, met, and their fulfillment sufficiently communicated. An important task of interfaces connecting consumers with their smart meters and through them with the smart grid will therefore be to communicate privacy. To do so successfully it is crucial to have a clear understanding of existing privacy concerns and of what end-users need in order mitigate such concerns. The preliminary study presented below aims at providing some differentiated insights into such user concerns and requirements within the smart grid and to form a basis for more comprehensive work addressing privacy communication in theory and in practice.

Methods

A small questionnaire study with a limited sample was conducted to gain a first impression of the relative relevancy of different privacy concerns and privacy requirements from an end-user perspective. The authors' intention was to develop a tentative set of privacy communication requirements based on the results of this preliminary study. The 53 Austrian participants (51% female, age range 19 to 71 with a mean of 38.6 and *sd*=14.101) were recruited online via social networks (predominantly Facebook). Users with a high educational degree (university degree or similar) were with 44% overrepresented. Questioned concerning their prior knowledge of smart meters, 25% stated them as previously unknown to them, 32% had heard or read the term, 17% saw themselves as somewhat informed, 21% as relatively informed and 6% as very informed about them. Two participants (4%) had smart meters installed in their homes, while 81% stated that they had not and 15% were uncertain. The large majority (94%) did not have any experience with smart meter energy feedback portals.

After a short introduction to smart meters followed the first part of the questionnaire containing a list of 12 items stating potential privacy risks in the context of smart meters (as the consumer's main contact point with a smart grid), e.g. "Smart meter data reveals too

much about me". Half of the items were reversed. For each risk participants were asked to estimate the probability of occurrence along a 7-point Likert scale ranging from 1="not at all" to 7="absolutely". Additionally, respondents were offered an "I don't know" reply option in case they did not feel confident to make a risk assessment concerning a statement. In the second section of the questionnaire, participants were presented with 16 items stating potential measures to protect and communicate privacy of smart meter data (e.g. "I should be able to see which data the smart meter is transmitting to the network operator"). Respondents were asked to rate items on a 7-point Likert scale (ranging from 1="not at all important" to 7="very important"). An "I don't know" option was not offered for this part of the questionnaire as we were asking for feedback on feelings of personal relevance.

The items contained in the questionnaire addressing perceived privacy risks and requirements were developed based on an extensive literature research, considering publications around smart grid privacy and security by governmental task forces [e.g. 20], consumer research reports [e.g. 9,12,16,21], and research papers [e.g. 3,17], as well as existing general or domain-related questionnaires aiming at measuring privacy concerns [e.g. 15,23].

Further, participants where asked if data granularity (measurement every 15 minutes or daily – available options in Austria) made a difference with regards to privacy concerns (no difference / somewhat less concerned / much less concerned / not at all concerned in case of 24h rather than 15min measurement intervals). A second granularity-related question addressed if they were inclined to reject 15min and/or 24h intervals and allow only monthly measurements (effectively taking the "smart" out of the smart meter).

Results

Above average risk perception ratings ("percent agree", calculated via the percentage of score 5, 6, or 7 ratings, at 50% or more) were given for *use of data to learn about user habits*, *user has no control over data*, *risk of data theft for break-in purposes, risk of data manipulation, data reveals too much about user*, and *risk of data theft for selling purposes*. *Risk of measurement error* stood out as a risk perceived to be particularly low in comparison to all other listed risks. Participants most often (25% or more) chose to refrain from rating by selecting "I don't know" in relation to the risks of *insufficient information about data collection*, *use of data without consent*, *disclosure of data in legal matters without consent* and *selling of data without consent*. The detailed results can be found in tab. 1.

Perceived Privacy Risk	**mean**	***sd***	**% agree**	**don't know**
1. Unnecessary collection of data	4.02	2.196	36%	13%
2. Insufficient information about data collection (r)	4.25	2.109	39%	25%
3. Data reveals to much about user	4.58	1.960	51%	6%
4. Use of data to learn about user habits	4.96	1.906	60%	6%
5. User has no control over	5.02	1.961	54%	11%

data (r)				
6. Use of data without consent (r)	3.97	2.294	28%	34%
7. Selling of data without consent	3.70	2.391	29%	30%
8. Disclosure of data in legal matters without consent	4.18	2.438	38%	25%
9. Risk of data theft for break-in purposes (r)	4.91	2.130	54%	15%
10. Risk of data theft for selling purposes	4.43	2.316	51%	13%
11. Risk of measurement errors (r)	2.12	1.276	4%	19%
12. Risk of data manipulation (r)	4.80	2.075	52%	17%

Table 1: Presented privacy risks with means, *sd*'s, percent agree, and percentage of "I don't know" replies

All presented privacy requirements received average ratings above the scale mean ("percent agree", with respondents giving an importance rating of score 5, 6 or 7, at 50% or more). Particularly high ratings ("percent agree" at 90% or more) were observed for control aspects (*control over data selling or disclosure, control over use of data, control over data collection*), transparency aspects (*transparency concerning data transfer, transparency concerning occurring data access*), *information on data security measures*, *only as much data collection as necessary for agreed purpose,* and *appropriation of data for agreed purpose*. The detailed results can be found in tab. 2.

Privacy Requirement	**mean**	***sd***	**% agree**
1. Appropriation of data for agreed purpose	6.49	0.823	96%
2. Only as much data collection as necessary for agreed purpose	6.53	0.953	93%
3. Data storage only as long as necessary for agreed purpose	6.26	1.258	89%
4. Transparency concerning data transfer	6.55	0.798	97%
5. Transparency concerning occurring data access	6.36	1.111	91%
6. Information on data security measures	6.51	0.891	95%
7. Information on data privacy laws and guidelines	6.25	1.054	89%
8. Data should reveal as little as possible about users	6.15	1.420	87%
9. Control over data collection	6.13	1.468	90%
10. Control over use of data	6.26	1.163	90%
11. Control over data selling or disclosure	6.57	1.065	91%
12. Principal contact for questions around data privacy and security	5.87	1.177	85%
13. Clear communication of personal benefits	6.06	1.262	88%
14. Clear communication of societal benefits	5.77	1.423	83%

15. Supervisory body to ensure correct handling of data	6.11	1.204	83%
16. Data administration by 3rd party	4.75	1.764	57%

Table 2: Presented privacy requirements with means, *sd*'s, and percent agree

Looked at as scales, both the privacy concern items and the privacy requirement items displayed a high internal consistency with *Cronbach's alpha* at .941 and .851, respectively. Overall concern scores (*mean*=4.29 with *sd*=1.526) and overall requirement scores (*mean*=6.16 with *sd*=0.669) did not significantly correlate with each other or with prior knowledge of smart meters.

With regards to the granularity-related questions, 59% indicated that they would feel less concerned about their privacy if their smart meter would measure once daily rather than every 15 minutes (34% were "somewhat less concerned", 23% were "much less concerned" and 2% "not at all concerned" in that case). About two thirds of the participants (47%) were inclined to reject 15min measurement intervals and 32% to also reject daily measurements. Overall privacy concern scores were negatively correlated with acceptance of 15min intervals (r_{pb}=-.572 with p=.000) and positively with a rejection of daily measurements (r_{pb}=.610 with p=.000). Overall privacy requirement scores did not significantly correlate with either tendency and there was no significant correlation between perceived effect of granularity on concerns and overall privacy concern or requirement scores.

Conclusions

Study participants saw the risks of missing control over data, data security threats, and a problematic information potential of the collected data as most likely to occur. Further, they displayed uncertainty about the trustworthiness of energy distributers and providers by refraining from a risk occurrence estimation concerning a number of potential risks dependent on collector and administrator handling of data. The privacy protection measures that are perceived as most important are user control of the data (collection, access, usage), transparency about data processing (transfer, access), sufficient security measures and restraint in collection and usage (data minimization and approbation). Overall, Participants displayed a preference for a lower data granularity (24h rather than 15min intervals).

According to the results of this preliminary test, special attention should therefore be paid to the following privacy requirements when designing mobile smart grid interfaces in order to mitigate user privacy concerns:

- Acknowledge and address concerns around data control, data security and the general information potential of data
- Provide detailed information about the purpose of the data collection and data handling
- Provide and communicate end-user control over data
- Make data processes transparent
- Communicate security measures
- Communicate accountability of data collectors
- Pay special attention to customer relationship building in order to strengthen trust.

Further, it might be worth to consider if medium length measurement intervals might not be possible. An hourly measurement frequency might be sufficient to still reap close to full benefits while assuaging some of the uneasiness consumers feel with regards to the 15min interval.

As study limitations we need to acknowledge the online survey setting which relies heavily on the imaginary powers of participants and can limit result validity. Further, as a preliminary work, the scope of this study was limited to getting a first differentiated look into user concerns and requirements and our results do not provide any directly applicable guidance concerning how privacy requirements should be implemented. In a next step, the gained, preliminary understanding should be solidified with a larger sample and the question of how to communicate identified requirements to end-users should be addressed.

Acknowledgements

This research was performed within the *Smart City Demo Project Aspern* (SCDA) and financed by the *Climate and Energy Fund* of the *Austrian Research Promotion Agency*.

References

1. S. Massoud Amin and Bruce F. Wollenberg. 2005. Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine* 3, 5: 34–41.
2. Jahaivis M. Arias. 2014. Privacy in the context of Smart Home Environments: Based upon a survey of experts. Retrieved November 28, 2014 from http://www.diva-portal.org/smash/record.jsf?pid=diva2:720666
3. Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh. 2013. Social barriers to the adoption of smart homes. *Energy Policy* 63: 363–374.
4. Alvaro A. Cárdenas and Reihaneh Safavi-Naini. 2012. Security and Privacy in the Smart Grid. In *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier, 637–654.
5. Ann Cavoukian, Jules Polonetsky, and Christopher Wolf. 2010. SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society* 3, 2: 275–294. https://doi.org/10.1007/s12394-010-0046-y
6. Colette Cuijpers and Bert-Jaap Koops. 2013. *Smart Metering and Privacy in Europe: Lessons from the Dutch Case*. Social Science Research Network, Rochester, NY. Retrieved November 28, 2014 from http://papers.ssrn.com/abstract=2218553
7. Costas Efthymiou and Georgios Kalogridis. 2010. Smart Grid Privacy via Anonymization of Smart Metering Data. In *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 238–243. https://doi.org/10.1109/SMARTGRID.2010.5622050
8. Dominik Engel and Günther Eibl. 2017. Wavelet-based multiresolution smart meter privacy. *IEEE Transactions on Smart Grid* 8, 4: 1710–1721.
9. Hervais S. Fhom and Kpatcha M. Bayarou. 2011. Towards a Holistic Privacy Engineering Approach for Smart Grid Systems. In *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 234–241. https://doi.org/10.1109/TrustCom.2011.32

10. Flavia Gangale, Anna Mengolini, and Ijeoma Onyeji. 2013. Consumer engagement: An insight from smart grid projects in Europe. *Energy Policy* 60: 621–628. https://doi.org/10.1016/j.enpol.2013.05.031
11. Ulrich Greveler, Benjamin Justus, and Dennis Loehr. 2012. Multimedia content identification through smart meter power usage profiles. *Computers, Privacy and Data Protection* 1: 10.
12. Colin Griffith. 2014. *Smart and clear. Customer attitudes to communicating rights and choices on energy data privacy and access.* Consumer Futures, London, Glasgow, Cardiff, Belfast.
13. Beth Karlin, Rebecca Ford, and Cassandra Squiers. 2014. Energy feedback technology: a review and taxonomy of products and platforms. *Energy Efficiency* 7, 3: 377–399. https://doi.org/10.1007/s12053-013-9227-5
14. Eric D. Knapp and Raj Samani. 2013. Chapter 4 - Privacy Concerns with the Smart Grid. In *Applied Cyber Security and the Smart Grid*, Eric D. Knapp and Raj Samani (eds.). Syngress, Boston, 87–99.
15. Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4: 336–355. https://doi.org/10.1287/isre.1040.0032
16. O2. 2013. *Effectively engaging consumers to ensure smart meter success*. Slough. Retrieved March 14, 2015 from http://static.o2.co.uk/www/docs/enterprise/j879_smart-metering-report-a4_06_aw_hr_gs.pdf
17. Alexandra-Gwyn Paetz, Elisabeth Dütschke, and Wolf Fichtner. 2012. Smart homes as a means to sustainable energy consumption: A study of consumer perceptions. *Journal of consumer policy* 35, 1: 23–41.
18. Peter Palensky and Friederich Kupzog. 2013. Smart grids. *Annual Review of Environment and Resources* 38: 201–226.
19. Chan-Kook Park, Hyun-Jae Kim, and Yang-Soo Kim. 2014. A study of factors enhancing smart grid consumer engagement. *Energy Policy* 72: 211–218. https://doi.org/10.1016/j.enpol.2014.03.017
20. The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee. 2010. *Guidelines for Smart Grid Cyber Security. Vol. 2, Privacy and the Smart Grid (NISTIR 7628)*. Retrieved November 14, 2014 from http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
21. Michael Valocchi and John Juliano. 2012. *Knowledge is power: Driving smarter energy usage through consumer education*. IBM Global Services, Somers, NY. Retrieved December 9, 2014 from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03475USEN&attachment=GBE03475USEN.PDF#loaded
22. Markus Weiss, Claire-Michelle Loock, Thorsten Staake, Friedemann Mattern, and Elgar Fleisch. 2010. Evaluating mobile phones as energy consumption feedback devices. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, 63–77.
23. Philipp Wunderlich. 2013. *Green Information Systems in the Residential Sector: An Examination of the Determinants of Smart Meter Adoption*. Springer Science & Business Media.