



Ramokapane, M., Bird, C. M., Rashid, A., & Chitchyan, R. (2022). Privacy Design Strategies for Home Energy Management Systems (HEMS). In *CHI '22: CHI Conference on Human Factors in Computing Systems* (pp. 1-15). [405] Association for Computing Machinery (ACM). <https://doi.org/10.1145/3491102.3517515>

Peer reviewed version

Link to published version (if available):
[10.1145/3491102.3517515](https://doi.org/10.1145/3491102.3517515)

[Link to publication record in Explore Bristol Research](#)
PDF-document

This is the accepted author manuscript (AAM). The final published version (version of record) is available online via ACM at <https://doi.org/10.1145/3491102.3517515>. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: <http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

Privacy Design Strategies for Home Energy Management Systems (HEMS)

Kopo M. Ramokapane , Caroline Bird , Awais Rashid , Ruzanna Chitchyan 
{marvin.ramokapane,caroline.bird,awais.rashid,ruzanna.chitchyan}@bristol.ac.uk

University of Bristol
Bristol, United Kingdom





ABSTRACT

Home energy management systems (HEMS) offer control and the ability to manage energy, generating and collecting energy consumption data at the most detailed level. However, data at this level poses various privacy concerns, including, for instance, profiling consumer behaviors and large-scale surveillance. The question of how utility providers can get value from such data without infringing consumers' privacy has remained under-investigated. We address this gap by exploring the pro-sharing attitudes and privacy perceptions of 30 HEMS users and non-users through an interview study. While participants are concerned about data misuse and stigmatization, our analysis also reveals that incentives, altruism, trust, security and privacy, transparency and accountability encourage data sharing. From this analysis, we derive privacy design strategies for HEMS that can both improve privacy and engender adoption.

KEYWORDS

Energy Data, Smart Home Energy Management Systems, User Perceptions, User Privacy, Smart Home, Security, Data Privacy

Authors

Kopo M. Ramokapane , Caroline Bird , Awais Rashid , Ruzanna Chitchyan 
. 2022. Privacy Design Strategies for Home Energy Management Systems (HEMS). 15 pages.

1 INTRODUCTION

The need to manage energy better, use it efficiently, and address complex demand and supply issues has led to the advent of home energy management systems. HEMS aim to manage energy consumption, automate activities, and provide detailed energy usage feedback, critical for behavior change, and managing demand and supply. Unlike traditional aggregated energy data at the household level, HEMS collect (including user-generated) and generate consumption data at a very fine granular level (e.g., time and duration an appliance is in use) [6]. At a fine granular level, users can see how much energy each appliance uses in real-time and this helps them manage their energy. For utility companies, this data can be used for accurate billing and providing tailored services (e.g., demand and supply management) [25]. For other new market players, this data could be useful for developing new technologies and services that provide better comfort for users and support more sustainable living.

Corresponding author: Kopo M. Ramokapane, marvin.ramokapane@bristol.ac.uk.

Energy data is different from other collected data from smart home devices because, at some level, it is *required* for the provision of the service (e.g., billing purposes); without such data, utility companies may not be able to offer any service at all or require users to pay more. For instance, in Spain, failing to provide such data means billing is carried out applying an average consumption profile to the actual reading [30] (where the average profile is determined by Red Electrica Espanola ¹, grid manager, and transmission agent). Moreover, a stable and continuous energy supply is a critical requirement for modern society, and to ensure uninterrupted supply in a renewable-based environment, energy data sharing may soon become a mandatory requirement [24]. However, given the HEMS data granularity, it poses various privacy concerns. For instance, from such data one can infer home occupancy, sleeping patterns, household routine (e.g., shower times), or the number of people in the house. There is also a potential threat of suppliers having excessive control over users' activities through controlling energy consumption patterns. Thus, the issue of how energy data should be collected, shared, stored, and protected is timely.

The existing literature lacks a comprehensive understanding of how utility providers can get value from collecting and processing users' data without violating their privacy. Prior efforts [2, 12, 13, 17, 24, 25, 32, 34, 34, 39, 43, 48, 49] have focused on understanding consumers' perceptions and concerns around energy data and how best energy data can be used to influence behavior. The question as to how utility providers can get value from collecting and processing users' HEMS data without violating their privacy remains open. Moreover, there is a need for approaches to realize privacy and remedy users' concerns because relying on policy alone may not provide a sufficient level of privacy [16, 18, 25, 28]. As previously argued, privacy needs to be baked into system design [7, 29]. The existing literature makes it unclear how privacy by design can be achieved in HEMS to alleviate users' concerns and promote energy data collection and sharing. Thus, the gap between privacy requirements and measures that utility providers and HEMS designers can adopt foster participation in data sharing remains unaddressed.

To address this gap, we interviewed two groups of participants, consumers taking part in an energy conservation project and those who are not, to identify their concerns around energy data and the factors that may encourage them to share such data. Using these findings and Hoepman's privacy strategy framework [22], we derive privacy design strategies for HEMS, which utility companies can implement to mitigate privacy concerns and promote data sharing and adoption of HEMS. Identifying pro-data sharing attitudes and concrete measures (i.e., privacy design strategies) that may help

¹<https://www.ree.es/en>: Red Electrica Espanola is partly state-owned and public limited Spanish corporation which operates the national electricity grid in Spain.

practitioners address HEMS privacy issues and inform policy needs at early development stages, which may be more effective than privacy controls imposed after deployment. The main contributions of this paper are as follows:

- Identification of key attitudes towards mandatory and voluntary energy data collection and sharing.
- Discussion of how key energy data collection and sharing issues can be addressed and translated into systems requirements—Privacy Design Strategies for HEMS.
- Practical design measures that are better aligned with consumers' privacy expectations around energy data collection and sharing that utility providers can adopt.

Our study is not only important to research with regards to security and privacy of energy consumption data but also regarding the promotion of technologies that might help people reduce energy demand and climate change. Our paper uses the following terms:

Energy consumption data: – detailed energy data that shows how much energy each device or appliance used, the details of the appliance (e.g., model), the time and duration it used energy, and the source of energy (e.g., main grid, battery, solar).

Mandatory Data collection: – Energy data that the supplier wants to collect in order to provide a service. For example, the amount of energy a user consumes during peak-time.

Optional Data sharing: – Energy data that the user may choose to share but not obligated to share. For example, the number of appliances that consume between 100 and 250 watts daily.

2 BACKGROUND AND RELATED WORK

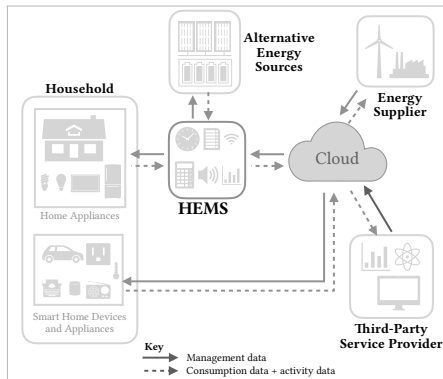


Figure 1: HEMS Data Ecosystem: HEMS collect and generate data from different sources. This data can be shared with various stakeholders including utility companies and other third-parties.

HEMS Features and Functionalities

Home energy management systems are part of the smart grid and smart home technologies. They are a platform that consumers can install in their homes to help monitor, manage, and automate energy around their households [26, 27, 31]. The HEMS ecosystem (shown in Fig. 1) includes various devices and appliances: sensors, smart plugs, energy supplier controllers, smart devices, and gateway—to communicate with the internet. The HEMS is required to monitor

and communicate with all these components to optimize energy use around the smart house. The main functionalities of HEMS include logging, monitoring, control, signaling, and management. Unlike smart meters, HEMS can manage and regulate energy from various energy sources such as solar panels and the main grid. HEMS can also automate/control other appliances; turn them *ON* and *OFF* during specific times. Moreover, HEMS can link with other devices (e.g., smart assistants) through Bluetooth and the internet (i.e., cloud), giving consumers more interfaces to manage and control energy flow within their household.

Literature around the design and development of HEMS is new and shaping up. Mikkelsen and Jacobsen [33] investigated HEMS and identified various threats to HEMS data, and key data flows that could happen between various stakeholders. Saha et al. [40] identified possible attacks and their countermeasures. Related to energy data flow, Rahman et al. [37] developed a HEMS privacy policy manager architecture which was aimed at allowing users to manage how data should flow between their households and utility companies. Prior works lack insights on what designers should implement to engender trust and adoption of HEMS, particularly concerning security and data privacy.

Energy Consumption Data

Traditionally each household had an electricity meter to periodically measure the aggregated electricity consumption. This data is non-specific: it does not show how many appliances were used or how much energy each appliance consumed, etc. [44]. To pay electricity bills, users must provide their meter readings to their local electricity supplier or allow the supplier to collect such readings. The supplier holds the right to this data and does not state to users how long it will be held or how it will further be used. Since this data is required to pay energy bills, users cannot opt-out of such data collection. Failure to provide such readings may result in one losing power or being disconnected from the main grid. HEMS-generated data, on the other hand, not only shows the total amount of energy used but provides rich, detailed information about the type and number of used appliances and other household devices as well as timings of their operation [6].

Most research on energy data has focused on smart meters². While it has been shown that detailed data can be useful, e.g., as providing users with tailored feedback helps to increase users' awareness on energy use and encourages behavior change [2, 32, 34, 43]. However, highly accurate and granular energy data may also pose various threats to consumer privacy [24, 41]. Moreover, as data is shared over smart grids and data networks, it can be a target for multiple reasons, for example, falsification of consumption data for financial gain [23, 50]. Furthermore, the current literature [12, 13, 17, 24, 34, 39, 43, 48, 49] suggests mixed opinions on users' perceptions of energy data. For instance, Wunderlich et al. [49] found that privacy was not the main factor for participants when they were contemplating owning smart meters, but perceived usefulness and behavioral control were highly considered. Moreover, users were more concerned about the credibility of the data rather than privacy [17]. However, 92% of participants either changed their privacy settings

²Smart meters provide some (not all) of the HEMS functionalities, for example, detailed consumption feedback.

or canceled their service subscription after being shown the risks associated with their subscribed service [24]. Schwartz et al. [42] found that users are not comfortable sharing their consumption data because they fear being misrepresented. Also, they classified energy data as personal goods, therefore were concerned about losing ownership. Concerning the sensitivity of energy data, most participants in a Swedish field study [34] concerning HEMS believed that energy data is harmless and poses no threat to their privacy. Another study [39], notes that the participants expressed little concern about the nature of the data collected and analyzed. However, they were concerned about how companies might exploit their consumption data. Schwartz et al. [42] also found that participants wanted to discuss energy data as relates to collective consumption rather than its fine-grain details. Our study provides users' perceptions of energy data with regards to their privacy and factors that may influence them to share such data.

Privacy in Development of Green Technologies

While data privacy concerns continue to grow, only a limited set of studies has considered users' concerns and perceptions to inform development of green technologies. For example, Jakkobi et al. [24] used participants' concerns and risks to develop a mobile application to mimic the smart meters' privacy management system. Our work too investigates perceptions and attitudes to inform the design of HEMS. However, unlike [24], we specifically examine users' perceptions and attitudes towards collecting and sharing data, as users have varying attitudes towards *collecting* and *sharing* their data. Also, prior studies [46, 47] argue that the interplay between energy consumption data and personal habits is the key to stimulating energy-efficient behavior. This notion suggests that adoption or acceptance would depend mainly on users' attitudes, but such insights are missing concerning HEMS.

Two other studies closely related to our work were conducted by Gürses et al. [21] and Ukil et al. [45]. Gürses et al. [21] identified and discussed data minimization strategies (privacy design strategy to avoid excessive data collection) and used smart meter data as an example to show how these strategies can be applied. Ukil et al. [45], on the other hand, proposed a dynamic privacy analyzer scheme to minimize privacy leakage in smart meters. While both studies aim to achieve energy data privacy, they : (a) are limited to smart meters, (b) neglect issues of data sharing between the system and other entities, (c) disregard users' perceptions and attitudes. Moreover, Gürses et al. focuses only on data minimization and neglects other privacy design strategies (as discussed in the sub-section below). Other efforts [12, 38, 42] on design recommendations for energy data systems mainly focus on changing behavior and conserving energy. However, none of these studies consider specific recommendations for preserving privacy in the same systems. Our study provides clear guidelines and recommendations on how utility providers may clarify privacy implications, minimize risks, and engender trust in HEMS.

Privacy by Design (PbD)

To promote privacy consideration during the development process, a Privacy by Design (PbD) [7, 29] philosophy has been proposed. PbD's main goal is to guide the design of privacy-preserving systems.

However, PbD principles are not concrete enough to provide ways to address privacy issues during the design and implementation phases of a system. They also lack a clear way to translate or map legal data privacy requirements (or policies) into system requirements during the early stages of development, i.e., analysis and requirements engineering phases. To address these limitations, design strategies, privacy patterns, and Privacy Enhancing Technologies (PETs) have been proposed. Privacy design strategies [4, 22] form the first part of the development phase, and they aim to model a way in which designers can formulate system requirements that address privacy issues outlined by data-protection laws or policies. In contrast, privacy patterns [14, 20] are designed to provide concrete guidelines for solving recurring privacy problems during the design and implementation stages. PETs, on the other hand, provide ways in which privacy patterns can be implemented.

Privacy design strategies are a set of fundamental strategic approaches derived from data protection laws and frameworks to achieve certain levels of privacy protection [22]. They are goal-oriented; they aim to identify privacy features that must be satisfied to ensure privacy [35]. These strategies are intended to support engineers and designers' decision-making regarding fulfilling privacy requirements because they specify an architectural goal that, when implemented, ensures some privacy [1]. Thus, for each privacy design strategy, a suitable privacy pattern and the underlying PETs can be identified to implement a privacy protection feature. There are eight (8) privacy design strategies defined by Hoepman: *MINIMIZE*, *SEPARATE*, *AGGREGATE*, *HIDE*, *INFORM*, *CONTROL*, *ENFORCE* and *DEMONSTRATE*. Our study provides privacy design strategies for HEMS derived from users' perceptions about energy data and their pro-data collection and sharing attitudes, thus moving privacy considerations beyond specification in policies and regulations.

3 METHODOLOGY

Our study was approved by our Institutional Review Board (IRB) before any investigations could proceed. We obtained informed written consent from all participants concerning taking part in the study and having the session audio recorded.

Recruitment and Sampling

Our recruitment focused on two groups of people, those who were already part of an energy-saving project and those who were not in any project concerning energy or climate change. Other than for broad representation of perspectives, the idea behind recruitment was to investigate and compare the differences (if present) between the two groups. And, whether people who were already taking part in the energy conservation project might be more willing to have data collected and shared than those who were not.

The Energy saving project

Renaissance of PLaces with Innovative Citizenship And TEchnologies (REPLICATE^a) is a European research and development project that aims to deploy integrated energy, mobility, and ICT solutions in city districts. This research relates solely to the 'Smart Homes' element of domestic energy management. During 2018, 150 households in Bristol were recruited and supplied with smart appliances (e.g., Washing Machines, Dishwashers, and Dryers) connected to apps and data collection devices. The Smart Homes project aims to explore how energy demand

might be better managed and shifted to assist in smoothing grid demand, avoiding times of peak energy use and potentially taking advantage of renewable generation or advantageous off-peak tariffs using automated home energy management systems.

^a<https://replicate-project.eu/about/overview/>

To recruit participants from the local energy saving project, an email explaining the focus of the study was sent to participants who were asked to respond if they were interested. Participants not involved in the energy saving project were recruited through the university newsletter and by word-of-mouth.

Table 1: Summary: Study Demographics.

	Energy Project	No Energy Project
Gender		
Male	6	4
Female	12	8
Other	-	-
Did not disclose	-	-
Age		
18 - 24	-	1
25 - 34	4	3
35 - 44	5	5
45 - 54	-	-
55 - 64	9	3
65+	-	-
Did not disclose	-	-
Education		
High school/College	4	3
FE - Diploma	5	-
Bachelors	7	3
Masters	2	3
PhD	-	3
Did not disclose	-	-
Employment status		
Unemployed	-	1
Full time	13	9
Self Employment	1	1
Student	-	1
Retired	4	-
Did not disclose	-	-
Env. Org. Affiliation		
Affiliated	5	5
No affiliation	13	7
Did not disclose	-	-
Interest in Env issues		
1 - 2 (Not at all)	-	-
3 (sometimes)	6	-
4 - 5 (Very much)	12	9
Did not disclose	-	3

In the end, we recruited 30 adults: 18 from the energy-saving project (including 2 couples) and 12 from outside the project. For the energy project (6 males, 12 females), 13 people had full-time employment, 4 retired and 1 self-employed, while for the no-energy project (4 males, 8 females) 9 had full-time employment, 3 were either unemployed, self-employed, or student. Table 1 summarizes the demographics of our participants. The majority of our sample was involved in an energy conservation project, and they have a keen interest in environmental issues, especially towards the promotion of renewable energy sources. Thus, their attitudes may be more inclined towards sharing energy data than their counterparts since they are familiar with the uses and benefits of energy data. However, we view this as an advantage because they have more understanding of energy data in general, they also own energy-saving devices, and they know organizations which might find their energy data useful. Thus, their perceptions are likely to be more informed.

Interview Procedure

One researcher led the interviews, and each interview began by administering the information sheet, which explained the purpose of the study. Participants were encouraged to ask questions concerning any information that was not clear. Then, we obtained consent for the study and the use of a voice recorder for the interview sessions. After the participants had given consent, we asked them to complete the demographics form before answering the main questions. On average, most interviews took between 30 and 40 minutes. Participants volunteered to take part in the study and were compensated (\$27.00) for their time.

Interview Script

Our interview script started by asking participants about their general use of energy, then their feelings about automating of appliances, motivations and lastly about energy consumption data:

Energy Use. The first part of our script focused on energy use to encourage participants to think about their current energy practices. As part of this, we asked them about their daily routines around energy use and how frequently they used appliances such as washing machines and ovens.

HEMS Features and capabilities. The next set of questions focused on the features of HEMS (e.g., automation). We asked participants about the appliances they would automate using HEMS (i.e., when energy demand and costs are high). Our rationale behind these questions is supported by research [9] that suggests that HEMS can help people reduce the demand on the main grid by automating some appliances to reduce demand during peak times. To establish a baseline understanding of HEMS, as some participants noted they had neither encountered nor used HEMS before, we explained what HEMS were, its ecosystem—features, and capabilities. Our reason behind this explanation was to make sure all participants understood what HEMS were in the context of our study as some studies only consider specific parts of the HEMS ecosystem, like smart metering and automation, but neglecting the data that is collected and generated.

Data Collection and Sharing. The last set of questions focused on the collection and sharing of energy consumption data. We asked participants how they felt about the collection of consumption data, and it being accessible to energy suppliers through HEMS. We also inquired about their sentiments concerning such data being shared by different stakeholders such as researchers. While we were interested in understanding their perception of energy consumption data, we did not explicitly ask them how they viewed such data. We hoped this would come from the discussions during the interview as opposed to being primed by the questions. However, to avoid missing out on this, as the last question, we asked participants how this data compares with other data that is currently being collected from consumers such as social media and supermarket loyalty cards. We chose to ask questions concerning data and privacy at the end, giving participants the opportunity to raise concerns about HEMS and data they collect without being primed.

For the purpose of this study, we only analyzed questions about data collection and sharing. The interview script is shown in Appendix A.

Data Analysis

We transcribed and then qualitatively analyzed our interview scripts using thematic analysis [5, 36]. The lead researcher coded the first two scripts producing their own codebook before the second coder randomly selected two scripts to code independently. Then, the two coders discussed the codes and jointly produced a single codebook. In situations where coders had different codes, the researchers resolved the different by reading and discussing the disputed part of the text and clarifying the coding definition. Our calculated *Cohen's Kappa*, a coefficient for inter-rater reliability in thematic analysis, was 0.83 (showing a high degree of agreement). After the final code book was established, the lead researcher coded the remaining scripts. Relationships between the codes were established to produce themes and factors affecting data collection and sharing.

Threats to Validity

Our study is qualitative and was limited to local residents whose energy uses and practices are shaped by local guidelines. Thus, our findings may not generalize to other populations which may use different energy management systems, and where energy data may be regulated differently, which leads to different perceptions. Nevertheless, this is the first study towards understanding users' perceptions and concerns regarding privacy and how suppliers can effectively address these to promote the use of HEMS and hence a more sustainable living agenda across their customers.

Most of our participants did not own an energy management system and those who owned one did not own the same system, so there is a possibility that their answers were based on the smart energy management system they owned. However, we were cognizant of this, accordingly we provided explanations and examples of HEMS during our interviews to mitigate this.

4 PRO-DATA COLLECTION AND PRO-SHARING ATTITUDES

We next present our findings around factors that influence data collection and sharing. In summary, our findings show that participants' data sharing choices are influenced by incentives, altruism, trust, transparency, and data protection assurances. Fig. 2 presents an overview of our results.

To aid with the discussion of our results, we use EP1 – EP18 (EP – Energy Project) to denote **participants** from the energy conservation project and NP1 – NP12 (NP- No Project) for participants not participating in any energy-saving project. Moreover, after discussing each theme, we discuss the design implication of the associated theme. **Design implications** are denoted as DI-x, x is the design implication number.

4.1 Incentives

The first theme described the reward or gains of allowing data collection and sharing. Participants stated that their willingness to allow data collection and sharing would be motivated by what they will personally gain or benefit from such action. When data collection is compulsory, participants are more accepting of the idea of paying the correct amount than receiving discounts—prioritizing price over consumption details. They would allow collection so that the utility company does not gain from them.

"I'm alright with it. I give monthly readings to [company name] on their app, and that just makes sure that I pay in the right amount of money 'cause you don't wanna get stung if you do it once or twice 'cause you end up owing them money." EP5

However, with regards to data sharing, they only want to share data to know how much they are spending. Participants (n=12) particularly those part of the energy conservation project, stated that they would also be willing to share their data if they would benefit materially from such activity. These participants were given appliances to use as part of the energy conservation project. Other participants stated that they would allow data sharing if it resulted in a positive change in their lives (e.g., good behavior).

DI-1 Design Implications for HEMS: Participants want to share data to ensure that they are **not overpaying**; **mandatory** data collection should only focus on the data that is **essential for bills and grid management**.

4.2 Altruism

The second key factor impacting data collection and sharing concerns people and the environment. Participants were content with data being collected to ensure that everyone has a supply of energy and save the environment, highlighting the environmental concerns and energy security (i.e., load balancing). Participants reasoned that compulsory energy data collection was crucial for saving the planet and promoting green energy.

"From an environmental perspective, it's definitely beneficial if it reduces the load on the grid." NP4

When data sharing is optional, participants stated they would be willing to share data with relevant entities, particularly local projects, to promote energy conservation. Other respondents (n=11) explained that they would be willing to share data locally to compare their energy usage with other local people as a way of reducing their energy use. Participants also said they would share data to improve green technologies (e.g., vanguards).

"Yes and I think if you had the data you're talking about [usage data], you know the sort of peak that comes, it would be interesting to compare [with other] people... acting in a more community level." NP11

DI-2 Design Implications for HEMS: Participants' desire to live sustainable lives may lead to data sharing; **the purpose of data collection, particularly for promoting sustainable living or improving green technologies, should be communicated clearly to users**. For instance, the expected environmental impact of sharing such data. Users should be able to distinguish between the purpose of *mandatory* and *optional* data. The purpose of *mandatory* data collection could be made **part of the setup process** since it may not change, while *optional* data collection purposes could be included in **other settings**

4.3 Trust.

Our third theme identified issues around trust. Participants talked about how they consider the data collector and receiver's trustworthiness when deciding whether they should allow data collection and sharing. Among the numerous data collectors, participants reasoned

Major Themes	Data Collection Pro-attitudes	Data Sharing Pro-Attitudes
Incentives	<ul style="list-style-type: none"> Financial benefits Paying the correct fees 	<ul style="list-style-type: none"> Financial incentives Change of behaviour
Altruism	<ul style="list-style-type: none"> Load balancing Environmental purposes Promotion of green energy 	<ul style="list-style-type: none"> Normative beliefs Development of new technologies
Trust	<ul style="list-style-type: none"> Trust in data collector Energy companies Trusting a single entity 	<ul style="list-style-type: none"> Credible companies Local authorities Well known data receivers
Accountability & Transparency	<ul style="list-style-type: none"> Clear explanations Type of data 	<ul style="list-style-type: none"> Choice and Consent Data Control Data use charges Data ownership
Data Protection Assurances	<ul style="list-style-type: none"> Data security assurances 	<ul style="list-style-type: none"> Anonymity

Figure 2: Key findings: Schematic depiction of the codebook. Our analysis leads to the discovery of various attitudes towards data collection and sharing. These attitudes span five main themes which include incentives, altruism, trust, transparency and accountability, and data protection assurances. However, participants’ concerns about data collection and sharing can be categorized into three groups: data security, misuse, and power relations.

that trust in the data collector (i.e., HEMS manufacturer, local authorities, utility companies, and other third parties) was important when deciding to allow data collection and sharing. They stated that there were some companies that they would more easily trust than others. Participants also discussed the importance of trust in HEMS, and that data will be kept securely.

Regarding mandatory data collection, we found that participants (n=13) preferred local green energy companies or community networks for data collection over large companies. They explained that large companies are primarily fossil-based while small local companies are environmentally conscious and focused on renewable energy. Others (n=8) believed large companies had multinational ownership and profited at the expense of customers, while local companies invested in the local area and were considered more ethical and customer-focused.

“I’m with [local utility company], so I trust them. If I was with one of the big six³, I might be a bit reluctant to let them have it. Yeah it probably depends who’s supplying my energy.” EP11

“Ultimately these energy providers are owned by massively wealthy people who have lots of influence in lots of other areas as well and connections with other people. I don’t like it.” EP3

Some participants (n=18) expressed their desire to have only energy companies collecting their data. They explained that they trust that energy companies would use their data for energy-related purposes rather than other reasons which may not align with their preferences. Participants believed that non-energy companies are

more likely to misuse their data if given access since they are about making money from other avenues, and they may have other interests outside energy which may not align with their preferences.

“I wouldn’t want any company or any business to be able to provide me with some kind of idea of service improvement. It would have to be something that would come from the supplier itself.” EP1

“I wouldn’t really like that because from your energy company that makes sense but for other third parties I don’t think [it would make sense].” EP10

When given a choice to share data, participants (n=17) stated that the data receiver should be credible, with a track record of honest data use (i.e., using data as promised) whose interests are not only to make a profit—stressing that it should be a company/organization that they know well. Some respondents (n=6) also stated they would voluntarily share their energy data with a trusted municipality or researchers promoting green energy.

“As long as it was credible ones that are on board with energy, rather than these cold-calling types and people that haven’t really got the community or the person’s interests, you know.” EP14

“if there was some form of intermediary which would be trusted, so possibly something set up at a municipal local authority or local government level that might act as an aggregator. So for the common good, not for the private benefit.” EP1

DI-3 Design Implications for HEMS: Given participants’ lack of trust towards big energy companies, mandatory data could be

³“Big six” are the six largest suppliers of gas and electricity in the UK.

collected only by the **utility providers**, while *optional* data sharing could be made available to **other parties chosen by the user**. This could be facilitated by mechanisms that allow users to **choose data recipients** to support their needs—list of choices should be made explicit. To engender trust, utility providers could also ensure that **privacy policy agreed by users is enforced** and users have the **mechanisms to verify**.

4.4 Accountability and Transparency.

This theme is concerned with data practices by those who collect and receive data. Our results highlight that participants want to have a clear understanding of what data is collected, how it will be used, and who it will be shared with, suggesting their efforts to guard against giving away data that is not relevant to the energy sector or being passed to non-energy sectors whose practices they do not want to be associated with.

When participants are obligated to allow data collection, they prioritize getting clear information about what data is being collected and its purpose. They explained that the current communication mode does not make it easy for them to understand what data is being collected.

“it’s like with all these data forms, they’ve got to be user friendly as well for the public to understand, because sometimes you just tick, tick, tick. There have got to be clear explanations, I think, before any [data collection] was to happen.” NP10

Other participants (n=26) explained that having a clear understanding of what data is being collected will help them decide whether such data is necessary for the purpose it is being collected. Moreover, since they believe the energy supplier will be the issuer of the energy system, they suggested that the supplier should also provide a document (e.g., “disclosure document”) with the system.

“I guess it would need to disclose to you what the profile of information looks like, so you can understand what you’re giving away... You might get a disclosure document from an energy company to say “this is this type of information that we’re collecting.” NP2

Our analysis suggests that participants seek these explanations for two reasons, 1) participants’ limited understanding of how energy data can be used, and 2) the prevalence of data misuse cases in other domains. Responses suggest that some participants did not fully understand how energy data can be used, so they wanted more information about what data is collected to have a better understanding. Regarding data misuse, participants (n=11) explained that companies collect more data than they need and then use it against users in other domains, so they wanted to ensure that it is not the same case concerning energy data. EP12 explained why they needed an explanation:

“What worries me is if they have data [about] me, and that, being passed on or whatever. That does worry me those sorts of things” NP12

Regarding voluntary data sharing, participants stated that they were willing to share their data if the data sharing is transparent; reasons clearly communicated, choice to opt-in or out of it, and retained control of how energy data could be used, including after the original purpose has changed. Participants highlighted that most

data sharing activities are not transparent and take place without their knowledge or control. However, our analysis suggests that these desires are based on data practices from other domains not the current HEMS or other energy systems.

After acknowledging that the energy data ecosystem may include new other stakeholders which traditionally were not part of the energy ecosystem (e.g., third parties using energy data to offer other services), some participants (n=12) explained that they would share data if they had control over what data they could share or who gets to receive it.

“I think as long as I have a choice to opt-in, who gets it and what it’s about then fine.” EP7

Others (n=4) expressed the desire to get updated about data use changes. For instance, if the data receiver finds a new purpose for the data, they should reach out to the data owners. Regarding sharing energy data with the local council, EP9 explained:

“... as long as the council are really open, as long as it was very open and transparent and not being used – if they were ever going to use it for other purposes they would have to consult people and tell everybody... we’re going to start using this for some other reason.”

Two of our participants expressed the desire to remain the full owners of the data after it has been shared. They explained that it would be ideal for them to control who should have access to their data. NP1 explained:

“I would want to have full control over my data... if we’re talking about energy consumption data, I would want to be the holder of that data. Whereas currently [ownership] lies with the supplier, I would want to take ownership of that data in the future.”

DI-4 Design Implications for HEMS: In addition to **clearly outlining** what data is being collected and the purpose for such collection, there is a need for **control mechanisms (e.g., consensual mechanisms) for users to choose how data should be handled (i.e., data recipients, data use, retention options) especially optional data**. For instance, users could be allowed to delete *optional* data completely.

4.5 Data Protection Assurance

Our final theme is concerned with data protection assurances. Participants (n=14) expressed the need to have security measures in place for them to be confident to allow data collection and sharing.

Participants explained that data protection is necessary when data collection is compulsory since they do not have the choice to opt-out of the collection. The data collector should ensure that data is not easily accessible to unauthorized parties.

“...my suppliers know how much energy I use, I would hope that their knowledge of my demand curves and data would be kept quite securely.” NP1

When given a choice to share data, participants (n=11) want assurances over anonymity. They expressed the desire to have data shared in an anonymized format. They were specifically concerned about other entities knowing their identity. NP7 noted

“That would be okay, I guess, if it’s [anonymized]. But it’s [not ok] when it’s like they can pinpoint which house and which room and what you look like.”

DI-5 Design Implications for HEMS: Participants highlighted the need for data protection especially for *mandatory* data. Designers could ensure that data is always protected during collection, transit, and at rest. *Optional* data could be anonymized by default while ensuring that both *mandatory* and *optional* data are not easily accessible but by only authorized parties. Designers could also demonstrate protection (e.g., system uses secure standards) and compliance.

5 USERS’ ENERGY DATA CONCERNS

Despite some participants being willing to allow data collection and sharing, we identified three major concerns that may impede data collection and sharing: (1) Security, (2) Data misuse, and (3) Power relations.

5.1 Security

Participants expressed their concerns over the safety and security of energy data; they transferred their experience from other domains where data collection is more established to create new threat models in HEMS.

System security. Some participants (n=6) were concerned about the security of the device itself. They explained that the number of data breaches worldwide had increased significantly, and HEMS would not be an exception; they may get hacked, giving attackers access to mandatory data. EP2 explained:

“No matter how much someone might tell you that their systems aren’t hackable and everything, you know, nothing is unhackable so ultimately once that stuff has all been tracked.”

Data security. Some participants (n=5) expressed concerns over sharing energy data with other technologies or services (e.g., smart home devices), and highlighted that some of these end up stealing their data for other purposes.

“[sharing data with my energy supplier] doesn’t worry me. What worries me is the sort of the interactive technologies that potentially can steal your data.” NP3

Other participants explained that energy data would bring a new dimension to the data that companies already have about them, thus attracting new threats. EP3 explained why data needed protection.

“There have been loads of breaches, whether it’s banking or Facebook or whatever, and I just feel in this modern age, that’s where the crime and stuff is happening, it’s in data.” EP3

DI-6 Design Implications for HEMS: Given that participants were concerned about the HEMS security, designers could ensure HEMS is well **secured with industry-recognized security standards (e.g., Advanced Encryption Standard (AES))**. Designers could implement trigger action mechanisms [8, 19] that allow users to implement their own rules to **control who or what devices can access their energy data**. Moreover, designers could use the privacy label framework [15] to develop privacy labels for HEMS to **raise awareness of what data is collected, stored, and shared with other devices and parties**.

5.2 Data Misuse

This theme is concerned with data being used for other purposes not stated initially. Since fine-grain activities such as when a household eats, sleep, and their type of entertainment can be implied from energy use, energy data could reveal personal habits, preferences, and lifestyles. Most participants raised concerns over misusing this learned information, e.g., for nefarious purposes or supporting causes that do not align with their ethos. This section discusses energy-specific issues around energy data.

Profit making. One point of consensus from our participants (n=25) was the disapproval of data being used or shared for monetizing or profitable purposes. Participants expressed their resentment towards companies that collect energy data for monetization for targeted advertising. Participants associated profit-making with big energy companies. NP9 said:

“most of the time that gets done, it’s done for commercial advantage for companies that I don’t have a particular sympathy with and probably are not making the world a better place. That’s my general assumption on people gathering that kind of data”

Profiling concerns. Participants (n=10) also reported that their data might be used to profile them. They explained that energy data collection would be an extension of the information that companies already know about them. For instance, companies could study their usage patterns and infer other information about them for targeted advertisements.

“Yes there’s enough data out there about me to profile me and do horrible things to me if they really wanted to so, yes, it would just be another data source.” EP2

“Already all the big companies know everything about what we’re doing, where we’re going on holiday, what our daily plans are because they’re tracking us on our phones. . . , so I suppose it’s just another way of finding out what we’re doing when we’re not on our phones and we’re doing our household chores, and now they’re going to know that too. That is a worry.” EP3

Penalizing people. Participants (n=10) expressed concerns over their energy data being used to penalize them. They explained that data at a fine-grained level would reveal the appliances customers are using and their energy consumption to the utility provider. If a customer uses a particular appliance or consumes too much energy from the main grid at certain times (e.g., peak times), they may be disconnected, charged more, or be restricted to some amount of energy at such times.

“I suppose further down the road it could be, people might say, well you can only use so much energy, they might monitor how much people are using, maybe there might be a cutoff. They say, right you’ve had your quota for the day and then, shoosh, everything goes off.” EP9

“How do you feel about something or somebody – if you want to do that, just meter electricity. Limit it or give people 1,000 watts a week and that’s it. You can

do what you want with it, but that's all you're getting, mate." EP15

Surveillance purposes. Other participants (n=5) expressed the risk of data collectors and receivers being able to know the whereabouts of an individual.

"I suppose there might be a whole domain about privacy, somehow. Concerns that, you know, given the other kind of constellation of devices people have now with consoles and smart TVs and everything, it's one more thing that they're using to track. 'Oh, well, now I know that they're in the kitchen because they're boiling the kettle.' 'Oh, now they've moved to the front room because...' I mean, it sounds silly, but, yeah, it irritates me a little bit to think, you know, corporations sucking up so much data about your daily habits as it is." EP2

Energy stigmatization. (Discrimination) Participants (n=10) also discussed the issue of being marginalized because of energy usage. They reported that other people (i.e., neighbors and friends) knowing how much energy they are using might judge and treat them differently. They also cited this as a reason why they would not share their energy data locally or with people they know. EP3 explained:

"I wouldn't want my information being shared, not that I have anything to hide, but I just wouldn't want people to know my daily routine of how much I wash. I wouldn't want that being shared with the community."

Unnecessary data collection and sharing. Some participants (n=12) discussed how some companies collect or share data that is unnecessary for delivering services to them. Moreover, they discussed how unnecessary collection and sharing might lead to data misuse. For example, data collectors may find value in their data and share it with other parties that traditionally would not want or find such data useful. NP9 expressed that they would be unhappy if they would find out that the data collection is unnecessary:

"I'd certainly be unhappy if they were gathering that information except as far as it's absolutely essential in order to do the [distribution] they need to do."

Unsolicited communication. Some participants (n=8) raised concerns over unwanted contact with data collectors and receivers. They stated that they would not be comfortable with people contacting them because they have shared data with them. Most participants expressed this concern when discussing sharing data with researchers and advertising companies.

"[referencing contact] I think that's probably where I feel a bit iffy about it. I wouldn't want a lot of unsolicited contact." EP7

DI-7 Design Implications for HEMS: To address surveillance and energy stigmatization concerns, designers could ensure that HEMS share **optional data intended to improve the technology anonymously**.

DI-8 Design Implications for HEMS: To address unsolicited communication issues, designers could provide mechanisms that allow users to **choose which parties** they would want to **communicate** with regarding their energy and use. This could include **appropriate and usable communication channels**.

5.3 Power Relations.

Our final theme concerns losing control over data that has been collected and shared.

Loss of control. Most participants (n=16) shared concerns over not having control over their energy data after it has been collected or shared with other parties. They expressed the inability to opt-out from further processing or knowing who has access to their data. For instance, NP3 suggested it would be better if they could still opt-out of some data processing schemes:

"I think as long as one can opt-out of any of the irritating stuff that might come thereafter."

Power shift. Some participants (n=9) discussed the issue of the utility provider having more power and control over consumers because of the information they can get from the data. They stated that sharing data with the utility provider will take power away from them and it may lead to the provider dictating how they should use energy.

"The dictatorship, you cannot use this, well I am going to use it." NP10

DI-9 Design Implications for HEMS: To balance the power between utility providers and consumers, designers could provide **various mechanisms** to allow users to **manage and delete** their data. For example, consumers could choose the *optional* data they want to share with utility providers.

6 PRIVACY DESIGN STRATEGIES FOR HEMS

As energy systems continues to evolve, collection and sharing of energy consumption data will be critical. It is already a law in some countries to have green technologies installed in new buildings [30, 51] because it is seen as a cost reduction and disruptive way for increasing efficiency. Therefore, energy data is useful for reducing costs and enabling other functions such as demand response programs. HEMS offer an interesting case to explore, especially in countries (e.g., in Europe) where there is a considerable variation in policy contexts encouraging the adoption and deployment of green technologies [3, 10, 11], and little on how data generated by these systems should be handled.

As shown by our findings, security and privacy concerns around energy data may impede such efforts. However, our findings suggest that HEMS users may be willing to participate in data sharing if these concerns are addressed. As a result, we used our findings to derive privacy design strategies to address the issues raised by participants in our study to inform the development of HEMS. We use these strategies to identify what measures the utility providers and HEMS designers should satisfy to realize privacy in HEMS, particularly around collecting and sharing energy data. We adopted this framework because they are abstract and not system-specific, enabling us to map and define each strategy specific to HEMS. We derived these strategies by first eliciting design recommendations from the themes we identified during coding. Then, we map each design recommendation to the relevant privacy design strategy. By doing this, we are ensuring that each privacy design strategy is no longer abstract but specific to HEMS. In Table 2, we present privacy design strategies for HEMS. We show Hoepman's privacy design strategies and the design recommendations that informs them.

Table 2: Summary: Adaptation of Hoepman Privacy Design Strategies for HEMS.

Strategy	Hoepman [22]	Design Implications informing the strategy	HEMS - Collection and Sharing
Minimize	Suggests that personal data processing should be minimal, and collection should only focus on the data that is needed for processing.	DI-1, DI-2	Mandatory data should represent data that is required for processing bills, service provision, and grid management purposes. Mandatory data collection and sharing should focus only on these data.
Hide	Indicates that collected and processed data should not be in plain sight.	DI-5, DI-7	Mandatory and optional data should not be shared or stored in plain view or kept when it is no longer needed.
Separate	Suggests that data should be distributed or isolated, whether during storage or processing stage.	DI-1, DI-3	Mandatory data should be separated from optional data before sharing to make correlation difficult while data is at rest or during processing. Moreover, optional data could be separated from personal identification information where possible.
Aggregate	States that personal data should be stored or processed at the highest possible aggregation level.	DI-1, DI-3	Mandatory data should be combined before sharing and processing, and where necessary optional data should be aggregated.
Inform	Suggests that data subject should be informed timely whenever personal data is processed.	DI-2, DI-4, DI-7	Energy consumers should be informed about data collection and sharing. This information should explain what constitutes data to be mandatory or optional, how it is collected, stored, used, whom it is shared with and how long it is retained.
Control	Implies that data subjects should be in control over data collection, storage and processing.	DI-3, DI-4, DI-6, DI-7, DI-9	Consumers should be in control over their energy data. They should be able to choose who should have access to their mandatory data other than the utility provider and how it should be used beyond the provision of the service. Consumers should have control over what optional data is collected, shared and for what purpose.
Enforce	Suggests that contractual and legal policies (i.e., privacy policy) that is compatible with legal requirements should in place and enforced.	DI-3	Any contractual agreed or privacy policy that is presented to the consumer should be respected and enforced.
Demonstrate	Requires that the data controller should be ready to demonstrate compliance.	DI-5	The HEMS manufacturer should be able to demonstrate that the system complies with industry security standards technically. Moreover, the utility provider should technically demonstrate that the privacy policy presented and agreed upon by the user is enforced.

Formulating and mapping design strategies to users' concerns are vital because it addresses two problems: (1) lack of empirical evidence on privacy concerns that are pressing for users and may hinder adoption, and (2) the absence of tools that are based on perceptions and attitudes for developers to use when designing HEMS. We are providing designers with approaches that they can follow to identify relevant PETs for developing HEMS, which is missing in the literature. Privacy protection is a quality attribution; therefore, addressing its concerns at the development stage using empirical evidence is vital for engendering trust and developing systems that appeal to users' variety of motivations, social and environmental issues without invading their privacy.

HEMS Privacy Design Strategies Mapping

In Fig. 3, we map participants' concerns we previously presented in Section 5 to our newly derived design strategies. This mapping identifies specific strategies for addressing each concern. By doing this, we are providing the designers of HEMS and parties with interest in energy data with a foundation to identify relevant privacy patterns and PETs for addressing users' concerns. These strategies are not restrictive; the designers can choose from a wide range of privacy patterns and PETs to address the specified issues. Moreover, this will give utility providers a chance to see how mature their approach is by seeing which strategies they are deploying and if such strategies lead to positive engagement from users and give them assurances.

Users' concerns around the system and data security could be addressed by demonstrating and minimizing the impact of a data breach on individuals. Less data could be collected (*Minimization*), *separated*, *hidden*, and in some cases aggregated to minimize impact. Addressing data misuse concerns will require consideration of all the privacy strategies, ensuring that consumers' trust is established, especially with mechanisms to verify that the data collector or processor is doing exactly what was stipulated in the agreement. Power relations could be alleviated by giving the user a degree of some control. A satisfactory amount of understanding of what the user can do (e.g., consent and control) is vital. *Control*, *Enforcement*, *Demonstration*, and *Minimization* are critical in addressing issues of power mismatch.

7 DISCUSSION

How do the two groups compare?

Contrasting the two groups, participants from the energy group showed more willingness to share data than their counterparts. The energy project participants' altruism to be environmentally friendly, and the desire to share energy seemed to outweigh reasons not to share data. This suggests that users may be willing to share data if the purpose is clearly outlined to users. While both sets of participants highlighted that trust in the data collector to be a significant factor in sharing data, no energy project participants were firmly against sharing data with local authorities. We also found that energy project respondents had strong knowledge about energy data usages and discussed well-informed threat models. We posit this may be due to

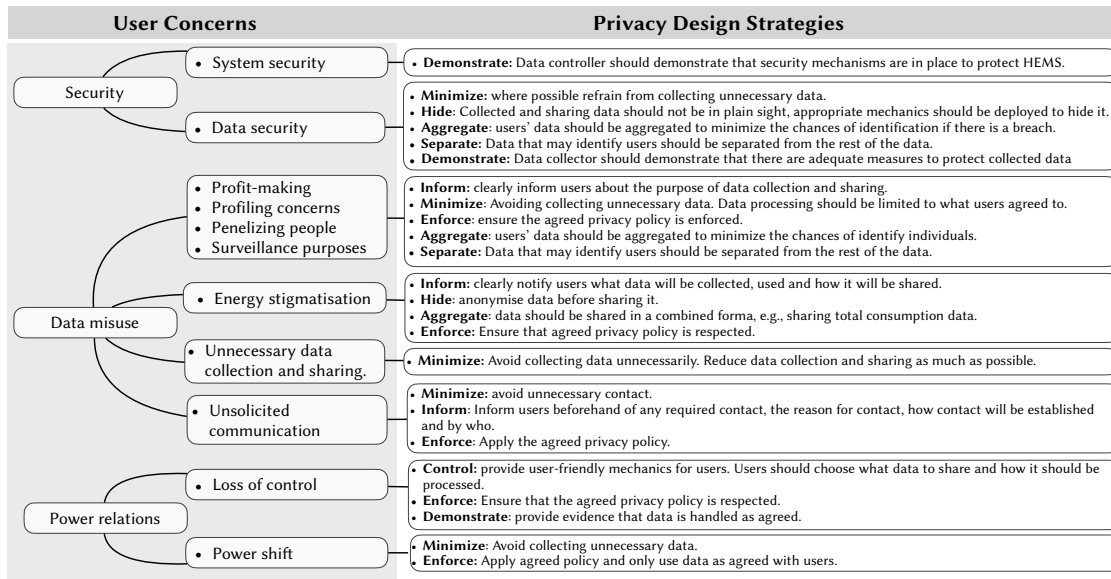


Figure 3: Summary: Mapping user concerns and privacy design strategies. This is to show how each user concern may be addressed by our derived privacy design strategies.

Themes	Energy Project	No - Energy Project
Incentives	<ul style="list-style-type: none"> • Change of behaviour. • Benefit materially (e.g., better appliances for free) 	<ul style="list-style-type: none"> • Share data to save money • Protection from over paying
Altruism	<ul style="list-style-type: none"> • Promote green technology • Support local energy companies 	<ul style="list-style-type: none"> • Save the environment • Energy security (i.e., Load balancing) • Improve technology
Trust	<ul style="list-style-type: none"> • Trust in green energy companies • Local and small energy companies 	<ul style="list-style-type: none"> • Trustworthy data collectors • Known company or municipal • Data sharing with energy companies • Less likely to share with local authorities
Accountability & Transparency		<ul style="list-style-type: none"> • Clear data handling practices. • Type of data being collected. • Choice to opt in and out. • Control over use and recipients. • Data ownership • Concerned about unnecessary data collection and sharing.
Data Protection Assurances		<ul style="list-style-type: none"> • Security over data • Concerned about data misuse than being hacked. • Data annoymization • Fewer participants were worried about utility companies having more control.
Security		<ul style="list-style-type: none"> • HEMS system security
Data Misuse		<ul style="list-style-type: none"> • Against the use of data for profit making • Profiling concerns • Penalizing people over use
Power Relations		<ul style="list-style-type: none"> • Utility provider controlling the amount of energy one can use

Figure 4: EP participants vs NP participants. This is to summarize the difference between the two groups of participants.

their energy project experiences, seeing what data can be collected and how it can be used. Participants from both groups shared similar concerns around transparency, accountability, and data protection assurances. This highlights the importance of these concepts, especially regarding data storage and processing. Thus, being transparent and providing assurances over data handling practices may be a significant differentiator around collecting and sharing energy data. We did not observe much differences between the two groups regarding power relations, but fewer participants from the no-energy

project discussed fewer issues concerning the utility provider having more power over consumers. Figure 4 provides a summary of these differences.

Energy data vs other smart home data

Data provided by HEMS offers more rich information making it possible to identify consumers' usage habits, appliances/devices, energy sources and automation routines, which may not be available with other electricity meters. As a result, it provides a larger surface

area for privacy invasions than data from other smart home systems and devices. It is also different because it may not only reveal consumer behaviour but consumers' socio-economic status as well. In fact, our findings revealed that some participants are worried about stigmatization that may arise from their energy data which may not be the case with other data. Moreover, unlike other data, energy data is not exchanged for free services, consumers still need to pay their utility bills. Considering these differences and our qualitative findings, it is important therefore to help and provide consumers with an understanding of what data is collected by HEMS and how they can share data without the risk of unwanted disclosures.

Why should energy data be protected?

Energy data should be protected because it contains more information about consumers and their practices which may harm their privacy. Our findings show varying perceptions concerning energy data, which suggest that some users may not be well informed on how to protect their privacy with some participants still holding mental models of traditional energy consumption data. We posit that applying the privacy design strategies we proposed will help users better understand the energy data ecosystem. Moreover, ensuring data privacy on HEMS will protect participants with optimism biases towards small green energy companies. Our findings revealed biases towards such companies which suggests users who hold strong opinions about the impact of energy on climate change may easily, uninformed, forego risks around energy data while sharing data for sustainability reasons. On the other hand, such energy companies understand the value of energy data which may extend to informing their other business ideas and models. It is, therefore, important to provide privacy by default to keep information asymmetry balanced, especially to help consumers who are less informed about the privacy implications of energy data.

It should be protected because privacy concerns may hinder adoption and cause conflicts in countries where smart metering systems like HEMS are mandatory, our study identified various concerns around energy data which may impede the adoption of HEMS or engaging in data sharing. A study conducted by Jakobi et al. [24] showed that 74% of users decided to change their energy data disclosure settings after encountering the corresponding privacy implications of doing so. About 9% decided to cancel sharing data with grid operator and utility provider. Providing privacy mechanisms may engender trust and promote adoption and data sharing.

Implications for research

Transposed mental models. Our findings suggest that most participants view energy data as not sensitive. We posit that this may be because traditionally, consumption data has always been aggregated information (i.e., meter reading), which showed the overall energy use. We, therefore, argue that transparency regulations should obligate utility providers to clearly communicate what data is being collected and how it can be used. Moreover, this information should be in a format that is user friendly or meaningful to users.

Stigma around energy usage. Stigma around energy use may affect how people want to share their consumption data. Some of our participants highlighted being uncomfortable with sharing data that may be seen by their neighbors or friends, suggesting a fear of being

stigmatized. Research should focus on understanding energy usage norms and social norms around energy to better inform designs that would address users concerns.

Protect users' energy data rights. Our participants were more worried about companies collecting and sharing their data for profit purpose but less on what they could potentially do with such data. We perceived a lack of trust towards big energy companies—users feel that these companies are motivated by profits but not to protect the environment. Our results also highlight a significant challenge for transparency particularly in large companies. Research should identify factors that engender trust in the energy sector, especially in green technologies. This also calls for policymakers to protect consumers' energy data rights, mainly where users may be unaware of the potential risks around such data.

HEMS Ecosystem. We found that our participants' concerns are limited to data collection, storage and sharing of data, little about processing. Our study does not give us insights concerning this, but we posit that this is due to our participants' limited understanding of the home energy management ecosystem. Since the home energy management ecosystem is broad with various aspects and data flows, privacy researchers should investigate privacy norms considering different aspect of the system, e.g., data processing. Moreover, we provide privacy design strategies for HEMS, research should implement and test our strategies and provide insights on what works to address concerns appropriately.

Data ownership and Monetization. Our results suggest that data ownership and monetization issues may play a role in how users may want to disclose their energy data. From our analysis, we perceived a strong sense of ownership towards energy data; participants perceive it as an asset; therefore, sharing it is seen as a contribution to the data controller's business aspect. We posit that this may be why they felt entitled to a share in any profits that may result from sharing their data, especially that in the case of energy data or HEMS, users still have to pay their bills, unlike in other free platforms. These issues need to be resolved particularly to encourage data sharing, which may be vital for energy security. Policies should aim to balance the power dynamic between data creators and holders.

8 CONCLUSION AND FUTURE WORK

While energy consumption data is crucial for various activities (e.g., billing, supply and demand management, feedback, and energy management), at its granular level, it poses several privacy concerns which may discourage consumers from sharing it. To this end, we presented an interview study with 30 participants, which investigated how users view energy data and their attitudes towards sharing it. Our analysis revealed that incentives, trust, transparency, the necessity of data collection and sharing, and assurances about data security are crucial for consumers to share data. Most importantly, our paper highlights a key set of strategies to move the privacy issue beyond specification in policies to how this could be built into the core of HEMS to provide more agency to users and more informed decision-making about privacy and other factors that will encourage take-up of HEMS and sharing of relevant information for wider societal benefit.

The future research in this area should tackle the issue of privacy around green technology. There is also an opportunity to examine energy data sharing schemes, mainly the 'how' part—how should data sharing be regulated. This is important, particularly for blueprints of future energy systems and how to transition from current fossil fuel-based systems. Data privacy will play a significant role because new players and use cases are emerging every day, therefore, regulating energy data is vital to ensure trust and encourage green technology adoption, thereby, using energy effectively.

ACKNOWLEDGMENTS

This research is funded by the UK EPSRC Refactoring Energy Systems (EP/R007373/1), Household Supplier Energy Market (EP/P031838/1) and EnergyREV (EP/S031863/1) projects.

REFERENCES

- [1] ALSHAMMARI, M., AND SIMPSON, A. Privacy architectural strategies: An approach for achieving various levels of privacy protection. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society* (2018), ACM, pp. 143–154.
- [2] ANDERSON, W., AND WHITE, V. Exploring consumer preferences for home energy display functionality. *Report to the Energy Saving Trust 123* (2009).
- [3] BERTOLDI, P., LÓPEZ-LORENTE, J., AND LABANCA, N. Energy consumption and energy efficiency trends in the eu-28 2000–2014. *Joint Research Centre: Ispra, Italy* (2016).
- [4] B'OSCH, C., ERB, B., KARGL, F., KOPP, H., AND PFATTHEICHER, S. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies 2016*, 4 (2016), 237–254.
- [5] BRAUN, V., AND CLARKE, V. Using thematic analysis in psychology. *Qualitative research in psychology 3*, 2 (2006), 77–101.
- [6] BUESCHER, N., BOUKOROS, S., BAUREGGER, S., AND KATZENBEISSER, S. Two is not enough: Privacy assessment of aggregation schemes in smart metering. *Proceedings on Privacy Enhancing Technologies 2017*, 4 (2017), 198–214.
- [7] CAVOUKIAN, A. Privacy by design. *Take the challenge. Information and privacy commissioner of Ontario, Canada* (2009).
- [8] CHEN, Y., CHOWDHURY, A. R., WANG, R., SABELFELD, A., CHATTERJEE, R., AND FERNANDES, E. Data privacy in trigger-action systems. In *2021 IEEE Symposium on Security and Privacy (SP)* (2021), IEEE, pp. 501–518.
- [9] CHITCHYAN, R., AND BIRD, C. Theory as a source of software requirements. In *Proceedings of International Requirements Engineering Conference* (United States, May 2020), International Requirements Engineering Conference, IEEE Computer Society. IEEE International Requirements Engineering Conference, RE2020 ; Conference date: 31-08-2020 Through 04-09-2020.
- [10] COUNCIL OF EUROPEAN UNION. Council regulation (EU) no 2009/72/ec, 2009. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0072&from=EN>.
- [11] COUNCIL OF EUROPEAN UNION. Council regulation (EU) no 2012/27/eu, 2012. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:315:0001:0056:EN:PDF>.
- [12] DILLAHUNT, T., MANKOFF, J., AND PAULO, E. Understanding conflict between landlords and tenants: Implications for energy sensing and feedback. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (New York, NY, USA, 2010), UbiComp '10, Association for Computing Machinery, p. 149–158.
- [13] DÖBELT, S., JUNG, M., BUSCH, M., AND TSHELIGI, M. Consumers' privacy concerns and implications for a privacy preserving smart grid architecture—results of an austrian study. *Energy Research & Social Science 9* (2015), 137–145.
- [14] DOTY, N., AND GUPTA, M. Privacy design patterns and anti-patterns patterns misapplied and unintended consequences. *Trustbusters Workshop at the Symposium on Usable Privacy and Security* (2013).
- [15] EMAMI-NAEINI, P., AGARWAL, Y., CRANOR, L. F., AND HIBSHI, H. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)* (2020), IEEE, pp. 447–464.
- [16] ENGEL, D. Enhancing privacy in smart energy systems. *e & i Elektrotechnik und Informationstechnik 137*, 1 (2020), 33–37.
- [17] ERICKSON, T., LI, M., KIM, Y., DESHPANDE, A., SAHU, S., CHAO, T., SUKAVIRIYA, P., AND NAPHADE, M. The dubuque electricity portal: Evaluation of a city-scale residential electricity consumption feedback system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), CHI '13, Association for Computing Machinery, p. 1203–1212.
- [18] ERKIN, Z., TRONCOSO-PASTORIZA, J. R., LAGENDIJK, R. L., AND PÉREZ-GONZÁLEZ, F. Privacy-preserving data aggregation in smart metering systems: An overview. *IEEE Signal Processing Magazine 30*, 2 (2013), 75–86.
- [19] FERNANDES, E., JUNG, J., AND PRAKASH, A. Security analysis of emerging smart home applications. In *2016 IEEE symposium on security and privacy (SP)* (2016), IEEE, pp. 636–654.
- [20] GÜRSES, S., TRONCOSO, C., AND DIAZ, C. Engineering privacy by design. *Computers, Privacy & Data Protection* (2011).
- [21] GÜRSES, S., TRONCOSO, C., AND DIAZ, C. Engineering privacy by design reloaded. In *Amsterdam Privacy Conference* (2015), pp. 1–21.
- [22] HOEPMAN, J.-H. Privacy design strategies. In *IFIP International Information Security Conference* (2014), Springer, pp. 446–459.
- [23] ISLAM, S. N., MAHMUD, M. A., AND OO, A. M. T. Impact of optimal false data injection attacks on local energy trading in a residential microgrid. *Ict Express 4*, 1 (2018), 30–34.
- [24] JAKOBI, T., PATIL, S., RANDALL, D., STEVENS, G., AND WULF, V. It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Trans. Comput.-Hum. Interact.* 26, 1 (Jan. 2019).
- [25] JAWUREK, M., KERSCHBAUM, F., AND DANEZIS, G. Sok: Privacy technologies for smart grids—a survey of options. *Microsoft Res., Cambridge, UK 1* (2012), 1–16.
- [26] JI, W., AND CHAN, E. H. Critical factors influencing the adoption of smart home energy technology in china: A guangdong province case study. *Energies 12*, 21 (2019), 4180.
- [27] JIN, X., BAKER, K., CHRISTENSEN, D., AND ISLEY, S. Foresee: A user-centric home energy management system for energy efficiency and demand response. *Applied Energy 205* (2017), 1583–1595.
- [28] KHWAJA, A. S., ANPALAGAN, A., NAEEM, M., AND VENKATESH, B. Smart meter data obfuscation using correlated noise. *IEEE Internet of Things Journal 7*, 8 (2020), 7250–7264.
- [29] LANGHEINRICH, M. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing* (2001), Springer, pp. 273–291.
- [30] LEIVA, J., PALACIOS, A., AND AGUADO, J. A. Smart metering trends, implications and necessities: A policy review. *Renewable and Sustainable Energy Reviews 55* (2016), 227–233.
- [31] MAHAPATRA, B., AND NAYYAR, A. Home energy management system (hems): concept, architecture, infrastructure, challenges and energy management schemes. *Energy Systems* (2019), 1–27.
- [32] MICHALEC, A., HAYES, E., LONGHURST, J., AND TUDGEY, D. Enhancing the communication potential of smart metering for energy and water. *Utilities Policy 56* (2019), 33–40.
- [33] MIKKELSEN, S. A., AND JACOBSEN, R. H. Securing the home energy management platform. *Energy Management of Distributed Generation Systems* (2016), 203.
- [34] NILSSON, A., WESTER, M., LAZAREVIC, D., AND BRANDT, N. Smart homes, home energy management systems and real-time feedback: Lessons for influencing household energy consumption from a swedish field study. *Energy and Buildings 179* (2018), 15–25.
- [35] NOTARIO, N., CRESPO, A., MARTÍN, Y., ALAMO, J. M. D., MÉTAYER, D. L., ANTIGNAC, T., KUNG, A., KROENER, I., AND WRIGHT, D. Pripare: Integrating privacy best practices into a privacy engineering methodology. In *2015 IEEE Security and Privacy Workshops* (2015), pp. 151–158.
- [36] NOWELL, L. S., NORRIS, J. M., WHITE, D. E., AND MOULES, N. J. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods 16*, 1 (2017), 1609406917733847.
- [37] RAHMAN, M. S., BASU, A., NAKAMURA, T., TAKASAKI, H., AND KIYOMOTO, S. Ppm: Privacy policy manager for home energy management system. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 9, 2 (2018), 42–56.
- [38] RICHE, Y., DODGE, J., AND METOYER, R. A. Studying always-on electricity feedback in the home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2010), CHI '10, Association for Computing Machinery, p. 1995–1998.
- [39] RODDEN, T. A., FISCHER, J. E., PANTIDI, N., BACHOUR, K., AND MORAN, S. At home with agents: Exploring attitudes towards future smart energy infrastructures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), CHI '13, Association for Computing Machinery, p. 1173–1182.
- [40] SAHA, A., RAHMAN, S., PIPATTANASOMPORN, M., AND KUZLU, M. On security of a home energy management system. In *IEEE PES Innovative Smart Grid Technologies, Europe* (2014), pp. 1–5.
- [41] SAJEEV, A., AND RAJAMANI, H.-S. Cyber-attacks on smart home energy management systems under aggregators. In *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)* (2020), IEEE, pp. 1–5.
- [42] SCHWARTZ, T., BETZ, M., RAMIREZ, L., AND STEVENS, G. Sustainable energy practices at work: Understanding the role of workers in energy conservation. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction:*

- Extending Boundaries* (New York, NY, USA, 2010), NordiCHI '10, Association for Computing Machinery, p. 452–462.
- [43] SKJØLSVOLD, T. M., JØRGENSEN, S., AND RYGHGAUG, M. Users, design and the role of feedback technologies in the norwegian energy transition: An empirical study and some radical challenges. *Energy Research & Social Science* 25 (2017), 1–8.
- [44] SULTAN, S. Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. *Computers & Security* 84 (2019), 148–165.
- [45] UKIL, A., BANDYOPADHYAY, S., AND PAL, A. Privacy for iot: Involuntary privacy enablement for smart energy systems. In *2015 IEEE International Conference on Communications (ICC)* (2015), pp. 536–541.
- [46] VAN DAM, S., BAKKER, C., AND BUITER, J. Do home energy management systems make sense? assessing their overall lifecycle impact. *Energy Policy* 63 (2013), 398–407.
- [47] WHITTLE, C., JONES, C. R., AND WHILE, A. Empowering householders: Identifying predictors of intentions to use a home energy management system in the united kingdom. *Energy Policy* 139 (2020), 111343.
- [48] WILKINS, D. J., CHITCHYAN, R., AND LEVINE, M. Peer-to-peer energy markets: Understanding the values of collective and community trading. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–14.
- [49] WUNDERLICH, P., VEIT, D., AND SARKER, S. Adoption of information systems in the electricity sector: The issue of smart metering. *Proceedings of the Americas Conference on Information Systems (AMCIS'12)*. (2012).
- [50] YUSSOF, S., RUSLI, M. E., YUSSOFF, Y., ISMAIL, R., AND GHAPAR, A. A. Financial impacts of smart meter security and privacy breach. In *Proceedings of the 6th International Conference on Information Technology and Multimedia* (2014), pp. 11–14.
- [51] ZHOU, S., AND BROWN, M. A. Smart meter deployment in europe: A comparative case study on the impacts of national policy schemes. *Journal of Cleaner Production* 144 (2017), 22–32.

A APPENDIX: INTERVIEW GUIDE (SEMI-STRUCTURED)

Thank you for participating in our study. As you read in the consent form, we will be recording the session so we can review it to make sure that we don't miss any part of our conversation. Your information will be kept confidential and will only be accessed by us. Your name will not be associated with any data we collect. We are interested in how people use energy in their homes and hence what potential there is to shift energy demand away from peak periods. If you don't want to or cannot answer a question, please say so at any time. Do you have any question?

- (1) Would you say that you care about or are interested in environmental issues?
 - Follow-up: would you say: not at all / a bit / sometimes / quite a lot / very much
- (2) Are you a member of any green / environmental organization? Or other group?
 - Follow-up-1: baby, books, community?

[**Daily Routines:** building a picture of how people perceive their appliances and how they use them currently]

- (3) What is your daily routine on weekdays?
 - Follow-up-1: Is it the same every day?
 - Follow-up-2: Are there some days when the house is occupied during the day?
- (4) How frequently do you use your washing machine,
 - Follow-up-1: Dryer
 - Follow-up-2: Dishwasher?
 - Follow-up-3: Which of these are smart?
 - Follow-up-4: What other appliance is particularly important to you (e.g., cooker, fridge, shower, TV/ console) – let's pick 3
[Thinking about these 3 appliances]

- (5) Can you describe the last time you used these appliances / 1,2,3 (from listed important ones)? Is that the normal way that you use them? Where are they in the house?
 - Follow-up-1: When / what time of day do you normally use them? Why? e.g., at specific times or varied. Is it different in the winter / summer?
 - Follow-up-2: Is the appliance set in a particular way e.g.,: time delay, eco-friendly, high heat, etc.?
 - Follow-up-3: What do you like about this appliance? e.g., speed, looks, effectiveness, capacity, controllability
 - Follow-up-4: What do you dislike about this appliance?
- (6) Do you have any restrictions to when you can use your appliances?
 - Follow-up-1: Does anyone in the building object to you using the appliances in a specific way/at a particular time?
 - Follow-up-2: who uses what and when?
 - Follow-up-3: Are there any constraints due to family schedule or noise (e.g., young children, old family members, illnesses, shift workers etc.)
- (7) Do you have any preferences on how you would like to use these appliances which might be different from how you currently use them?

[DSM Automation:]

Introduction: Use of energy here is particularly high during early mornings (between 7am – 8.30 am) and evening (4pm-8pm). Because of this, the grid needs to set up new generation facilities. But if people moved use of energy from these times to other periods in the day, the grid can avoid new generation investments, which cost money as well as cause increased environmental harm. It can also make better use of renewable energy. Because of this we are looking into automation or management of appliance use in order to move their use out of the critical time periods.

- (8) What if some of the appliances you mentioned could turn on/off to avoid peak demand time so you would pay less and so that the grid load was more evenly spread - would you consider some form of automation for some, or all of them?
 - Follow-up-1: Would you prefer only automating some appliances over others? Can you explain bit more.
- (9) How would you choose to automate them? What might work for you?
 - What degree of automation limits might you consider for each of the 3 appliances that we have been discussing?
 - Would you prefer to actively choose when to run it within only off-peak time limits

[If participant does not have an energy management system or heard about it. Explain it to the participant and then ask the following questions.]

- (10) How would you feel about having an energy management system which can manage things on your behalf in your household by automating some appliances? (within limits set by you). For example, so that you didn't breach an individual energy cap, to move consumption out of peak periods or to smooth energy consumption across a neighborhood?
 - Follow-up-1: What about more of a whole house automation system, integrating and managing your energy usage? Or even one that manages your alongside other users in your community?
 - Follow-up-2: Is personal automation different from a thermostat in the house starting/stopping boiler for temperature controls?
 - Follow-up-3: What other examples can you think of? (e.g., bread maker, security lights)
- (11) What can you foresee as difficulties or problematic issue with the system?

- (12) What motivations would most help you in changing the time/pattern of use of the appliance 1,2,3.
[if participant has or knows about energy management system, ask from here.]
- (13) How comfortable would you feel for your energy suppliers to have your data on appliance usage?
- (14) If data collection is mandatory, what data would you share, and with who?
- (15) Would it matter to you if your energy consumption data from this system was to be shared various parties? [Prompt participants with the following options if they don't say much.]
- Prompt-1: Researchers
 - Prompt-2: Energy generators
 - Prompt-3: Energy suppliers
 - Prompt-4: Other businesses which may find your data interesting
 - Prompt-5: Non-energy companies
- (16) How would want these data to be shared with these parties
- (17) If you were able to allow only selected businesses/individuals to view your consumption data, to deliver extra services with it, would you be more willing to allow this kind of data sharing?
- Explain your answer?
 - Who would you feel comfortable with sharing this information
- (18) if sharing consumption data is optional, what data would you share and with who?
- (19) How does the consumption data compare with other data, shopping loyalty card information gathering? (Data from smart home devices) [Anything else that you would like to say about energy use or that this had made you think about that I haven't asked you?] [Thank you]