

The trust gap: Social perceptions of privacy data for energy services in the United Kingdom

Phil Grünewald and Theresa Reisch

Environmental Change Institute, University of Oxford, South Parks Road, Oxford OX1 3QY, philipp.grunewald@ouce.ox.ac.uk

Abstract

The integration of distributed renewable resources relies increasingly on ‘smart’ solutions, requiring data to schedule, control and plan the operation of distributed assets within future energy systems. Such data can include household and even personal information. Personal location data can give valuable insights with relevance for energy consumption. Movement patterns and occupancy states help with scheduling of appliances, heating loads or storage, and other applications may yet emerge. Many smart home business models rely on data for their service provision. The potential upsides from the use of personal location data are met with growing concerns over information privacy. We present results from a representative UK survey on attitudes towards location data sharing. Our findings suggest that many of the resulting service benefits are widely appreciated. However, trust in the organisations delivering them is low and may inhibit their uptake. Less than 20% of people are willing to share their location data with an energy utility. In addition, the sense of control over location data appears low. Only 15% claim to understand who had access to their location data and 70% of participants feel that these settings are outside their control. These findings pose challenges for policy and regulation of data access. We make policy recommendations that seek to ensure smart solutions are not inhibited by a lack of public trust. In some cases this may require default settings that better match public expectations of data sharing defaults.

Keywords: Data privacy, Location data, Smart home

1. Introduction

Smart homes offer new opportunities for energy providers and consumers [1]. Potential benefits include increased convenience, more sophisticated monitoring and controlling of personal energy use and improved energy efficiency. Whether smart technologies ultimately reduce consumption remains disputed in the literature [2, 3, 4, 5]. At the national level, smart homes can aid grid-balancing, facilitate automated responses to dynamic energy tariffs and match demand with supply in real time [6, 7, 8, 9].

A growing number of smart home services rely on personal location data. Smartphones and other sensors can provide personal location data to schedule appliances and heating systems and train sophisticated algorithms on daily routines to optimise their operation [10, 11, 12]. Smart home developments are therefore actively promoted by various policy initiatives [13].

In exchange for such benefits, smart homes and their emerging Internet of Things (IoT) vastly expand the collection, utilisation and dissemination of personal information, stretching ‘the boundaries of the home into cyberspace’ [4].

Smart home devices allow passive, sometimes imperceptible, data collection. Users intentionally, unwittingly or naïvely allow their personal information to be collected processed and shared by smart home technologies. The smart home literature suggests that preferences become more lenient the greater the perceived gains from data provision are [14, 15, 16, 17, 18].

For example, a study by KPMG [19] showed that while 79% of the respondents were concerned about providing their personal data to external organisations, 58% still agreed to grant them access if it reduced their mobile internet charges.

Trust in the organisations collecting data affects personal preferences on data access. Studies in Germany and the UK outline how electricity consumers mistrust utility companies, hindering the potential of smart meter roll-outs [20, 21]. Meyer and Rakotonirainy [22] find that smart home users are less concerned to share data insights with family members than with external enterprises.

Location data contain personal information on whereabouts, insights into mode of travel, relationships and interests and can also result in insights into moods, stress levels, personality type and health [23, 17, 24, 25]. Tucker [26] has shown that past location data records can be used to predict a person’s location up to 80 weeks into the future with 80% accuracy and

Weber [27] warns that the collective data from IoT devices can result in ‘total surveillance’.

As smart homes expand the collection and dissemination of personal data, information privacy is becoming increasingly important for smart home policy development [28].

IoT ecosystems make it challenging to control the flows of the data extracted, processed or shared, let alone to understand the wider social implications. Lack of awareness about the implications of sharing personal data is widely reported on [29, 30, 31, 32].

Transparency is complicated through data aggregation and widely prevalent practices of data-trading, machine learning and ‘black box’ algorithms [33, 34, 35].

Concerns have been raised that the IoT may disrupt the concept of information control, which ‘forms an integral part of information privacy’ [36]. Wachter [37] argues that awareness of personal data flows would be essential for informed decisions about and control of such data. Consent is therefore often granted too lightly and should not necessarily be considered ‘informed’ [38].

The energy research literature on information privacy and data sharing preferences covers many implications of smart meters and load profile data [39, 40, 41, 42, 43].

Data sharing preferences and information privacy implications of location data have thus far received little attention in the smart home literature. Most empirical studies look at data sharing preferences as simplistic, self-contained exchanges, in which a type of service is provided in return for location data. Risks relating to unsolicited access and secondary uses remain largely unaddressed [15, 44, 45, 46]. Neither is the need for people to have a sense of control over their data sufficiently addressed [17, 18].

This paper therefore explores preferences for location data sharing for smart home services. Based on insights gained from a representative UK sample the study assesses attitudes towards location data sharing, its perceived benefits to users and their potential concerns.

2. Aims and methods

Some clear energy service benefits can be offered in exchange for personal data. This study focusses on this exchange and the role of the service provider as a trusted agent. The following research question will be addressed:

How dependent is willingness to share personal location data on the offered services and their providers?

To address this question we evaluate the results of an online survey. The sample (N=701) is representative of the UK population above the age of 18 (see Table 1). It was recruited with the help of a market research company from a panel of 450,000 UK residence. Participation was incentivised with reward vouchers.

Table 1: Characteristics of the representative UK survey population (N=701)

Characteristic		Representation
Gender	Male	51%
	Female	49%
Age group	18-24	12%
	25-34	17%
	35-44	18%
	45-54	18%
	55-64	14%
	65+	21%
Income	up to £7000	8%
	- £15,000	18%
	- £25,000	27%
	- £35,000	18%
	- £45,000	11%
	- £55,000	5%
	£55,000 or more	7%
Education	GCSE	22%
	A-level (or equivalent)	22%
	Bachelor's degree	25%
	Master's degree	8%
	Doctoral degree	2%

Survey questions are listed in Table 4 in Appendix A. The survey collected a wealth of contextual information. Only a subset of these are part of this analysis. The focus here is on questions on willingness to share data and the sense of control over these data.

The first part of the survey establishes the general willingness to share personal location data ('I would feel uncomfortable to have my location tracked by my smartphone'). This question is repeated at the end of the survey to assess any changes in attitudes in response to the survey itself.

The second part questions the services for which people would be willing to share their location data (see Table 2) and some organisations they would share these data with to enable such services (Table 3).

Most responses are coded on a five point scale from 'strongly agree' to 'strongly disagree'. Unless otherwise stated we group 'agree' and 'strongly agree' as agreement and the same with 'disagreement'.

Table 2: Location data supported service choices for survey participants

Group	Service provision
Personalisation	Targeted advertisement
	Location relevant recommendations
	Improving the online services I'm using
Mobility	Travel directions and traffic predictions
	Finding nearby parking
Locating	Finding friends and family
	Letting friends and family find me
	Finding my phone
Public	Improving public transport
	Preventing spread of infectious diseases
	National security
Energy	Energy savings
	Scheduling washing machine

Table 3: Potential recipients of location data for survey participants

Group	Data recipients
Personal	Close family
	Close friends
	Spouse/partner

Group	Data recipients
National	High Court National Security Council National government departments (e.g. UK Department for Transport)
Local	Local police office Local government Local GP Local restaurants/bars/clubs
Commercial	Insurance companies (e.g. Aviva, AXA) Financial institutes Smartphone providers (E.g. Apple, Samsung) Retail stores (e.g. Sainsbury, Tesco) Utility companies (e.g. British Gas) Smart Home companies (e.g. Nest, Samsung, SmartThings) Unknown companies
Technology	Social Media Platforms (E.g. Facebook, Instagram) Internet retailers (e.g. Amazon) Tech companies (e.g. Google, Microsoft) Data analytics companies (e.g. Cambridge Analytica)
Other	Universities

The third part of the survey addresses data sharing settings (3.A ‘It is clear to me when my location data is collected’, 3.B ‘I understand who has access to my location data’) and control over these settings (2.E ‘It is difficult to control my location data settings’).

Additional questions have been collected about the nature of their privacy concerns and other habitual behaviour in relation to data (Appendix A). A fuller discussion of these contextual data is available from Reisch [47]. In this paper we focus specifically on willingness to share location data for services and with service providers. The wider survey responses did not produce any additional explanatory variables to support our analysis and are therefore not elaborated on here.

The level of familiarity with location data reliant technologies is taken into account. Respondents were asked whether they own a smartphone, how attached they are to their phone and how frequently they use it, as well as how frequently they use location-data reliant services. Likewise (after providing a brief explanation of smart homes) respondents were asked whether they own

smart home technology and, if so, whether these respond to their location.

The full survey data is available on request.

The quality of responses was generally high. The survey took on average 15 minutes to complete. Surveys completed in less than 5 minutes (48 cases) are considered invalid and are not included. These were replaced with new recruits to ensure the representativeness of the study.

3. Results

Figure 1 shows the unease participants expressed about sharing personal location data. At the start of the survey 49% agree or strongly agree that they would feel uncomfortable to share such data. By the end of the survey this figure has risen to 60%. The share of participants with no concerns drops from 24 to only 14%. We will return to this significant shift resulting from the awareness raising nature of the survey itself in the Discussion Section.

The overall ratings for willingness to share location data are highly context specific. Figure 2 breaks agreement and disagreement to share data down into three segments: appliances, services and service providers.

The least controversial smart appliances are lights and space heating systems. Motion sensitive lights are already commonplace as a safety feature and a heating system that responds to occupancy is also agreeable to nearly half the sample. It wasn't specified to participants how the data is collected in technical terms. The context of the survey suggests that the data is collected and shared via a smartphone. In the context of lights it is conceivable that participants had motion sensors in mind, which are a more private use of location data.

Some of the smart appliances most cited as examples in the smart home literature have considerably lower approval ratings. Less than a third would trust their hot water or washing machine to be operated based on location data and less than a quarter approve of fridges or dishwashers to be operated 'smartly' in this way. For fridges this finding is particularly interesting, given that smart fridges could operate within their thermal limits, such that the user experiences no discernible change in service. It is possible that a lack of information about the impact of a 'smart fridge' underlies these results and more communication and practical experience with such appliances is needed for the public to accept them more widely.

The highest approval for services to use location data applies to established services, such as 'find my phone' and navigation, which are in com-

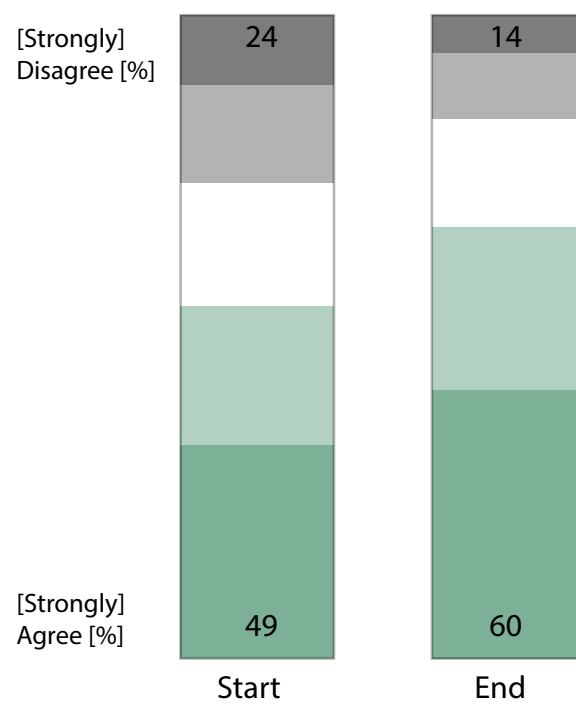


Figure 1: Increasing share of participant feel ‘uncomfortable to have my location tracked’ by the end of the survey

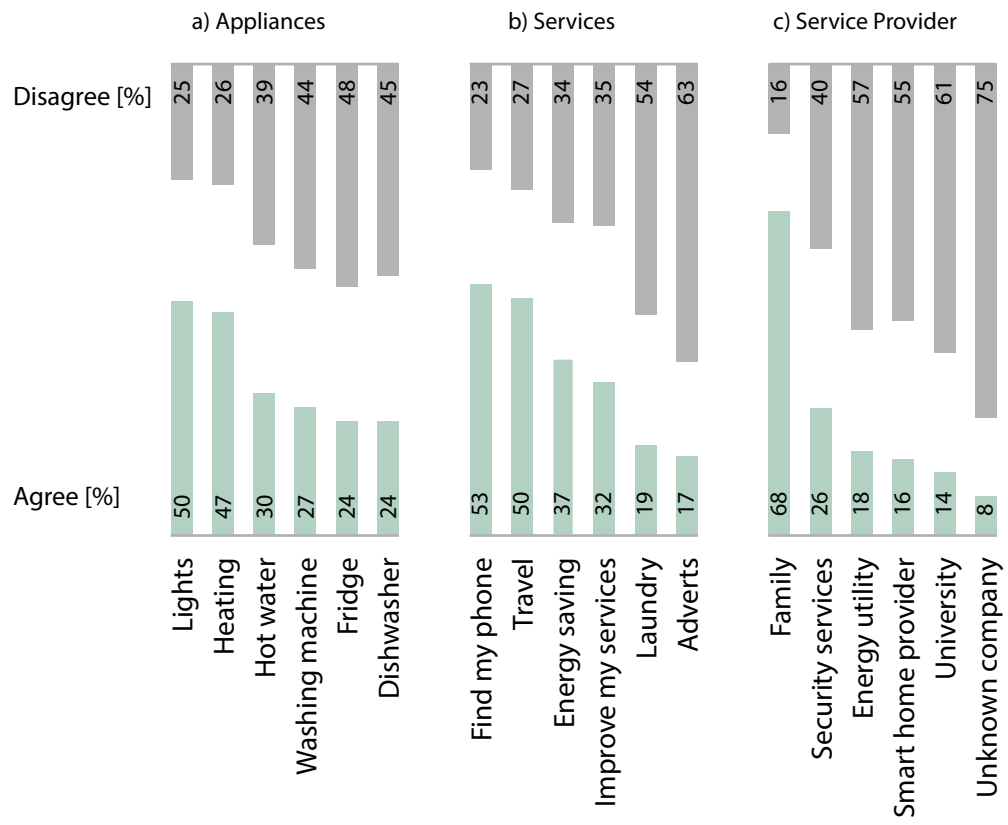


Figure 2: Willingness to share personal location data relating to appliances, services and service providers

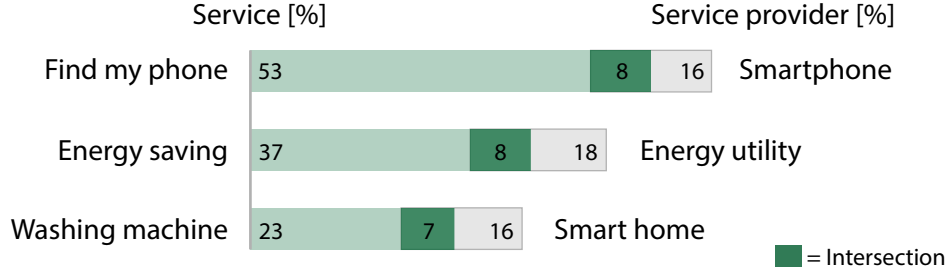


Figure 3: The combined approval for services and the relevant service provider is low

mon use and bring clear benefits to users. For energy savings the results are somewhat ambivalent. 37% would agree to share location data to save energy (costs) while 34% do not. Targeted advertising receives the lowest approval, with only 17% willing to share their location data for this ‘service’ (despite its ubiquitous use).

The highest diversity in approval ratings in Figure 2 is among potential data recipients. Sharing location data among family members has the highest approval of all categories (68%), while unknown companies rank lowest with only 8%.

The two service providers of particular interest for this analysis are utilities and smart home service providers. Neither of them receive high approval ratings. Compared to the 37% share of approval for energy savings, the share of people willing to share data with two of the most relevant organisations is 18% and 16% for utilities and smart home companies respectively. The intersection of these two groups is smaller still at 7% and 8% (Figure 3).

The tendency that willingness to share data for a service is greater than the willingness to share it with the relevant institutions is summarised in Figure 4. Across all services the rate of agreement to share location data is 50%, but across the service providers it is merely 28%. Nearly two thirds (64%) report that they would not agree to share their data with the institutions in Table 2.

The majority of respondents struggle with this differentiation between data uses and organisations that ultimately gain access to it. Only 15% claim to ‘understand who has access to my location data’, as shown in Figure 5. Consistent with this finding are high levels of unease about the levels of control over location data, as seen in Figure 1. 70% of respondents feel that data collection is outside of their control and 65% wished they had better

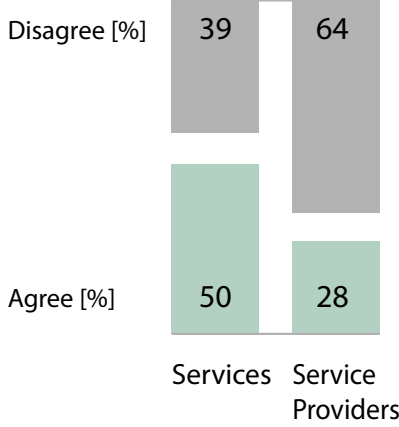


Figure 4: Aggregate willingness to share location data for services and with service providers

control over such data.

Participants more familiar with smart technologies are also more willing to share data. Regular users of mobile apps using location data report 12% less often that they are uncomfortable with having their location data tracked. This group is 36-39% more likely to share data for services and with organisations.

However, on average 69% of this group perceive the ways in which their location data is collected, processed and shared to be somewhat or completely outside of their control. The desire for more control is similar to those with less smartphone use and exposure to location tracking apps.

4. Discussion

The survey aimed to address the question ‘How dependent is willingness to share personal location data on the offered services and their providers?’. This section discusses the implications of our findings.

Even though the 85% of smartphone users have their location data collected [48, 49], almost half of the survey participants expressed discomfort about location data collection. This raises questions over the nature of their consent and could pose a barrier for many energy relevant saving opportunities, such as scheduling of space and water heating systems and training AI systems on load forecasting and estimation of demand side flexibility.

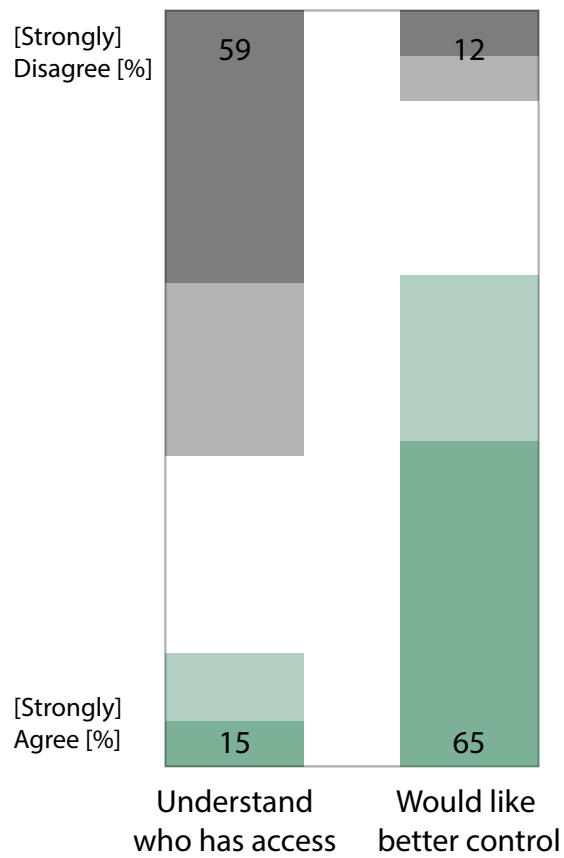


Figure 5: Few participants claim to “understand who has access” and a majority wished for “better control” over their location data.

Beyond a general discomfort, willingness to exchange personal location data depends on the offered services and their providers, with a striking discrepancy between the two. Just because data is made available for a service, does by no means equate to a permission for other types of uses or users. Large parts of the population are unsure about the extent to which their data is shared. With better controls they may not grant the access they currently do. These results apply to the frequent and non-frequent users of data reliant technologies alike.

Smart homes stand to increase the volume of data collection and with it the need to control these data. On the other side of the argument are calls for data to be ‘presumed open’ to maximise its potential benefits so long as these are not personal in nature or violate a set of conditions [50].

If a smart energy system, based on significant data sharing, is to be achieved in a consensual fashion, trust in the institutions collecting and sharing the relevant data will need to be addressed.

The results above indicate that initial privacy by design settings could be beneficial, especially for those 65% who wish they had better control over their data. Only personal information which is essential for specific service provision should be collected, as proposed by [51]. After use such data should be deleted by default [52, 27].

The GDPR already addresses some of these issues in the European Union [53]. Technical and organizational privacy by design measures represent one of the core tenets of the introduced standards. These prescribe data protection by design and by default, restrict data collection to what is absolutely necessary and constrain the sharing practices of such data with third parties (Article 25.1, 25.2 in EU, 2016). However, Wilson et al. [1] point out that smart home providers still lack adequate consideration of privacy measures.

A clear downside of a survey based approach and a limitation of this study is the potential gap between expressed and revealed preferences. An online survey is not a representative environment in which to express hypothetical choice preferences. The high willingness to share data in practice exemplifies this gap. However, increasingly often purchasing decisions and preferences are decided in online environments that are not unlike a survey, with little time and attention given to wider context and small print. Furthermore, the shift of 11 percentage points in unease about data sharing during the course of the survey itself suggests that even modest amounts of information are still able to shift not yet fully formed public opinions.

Even though 32% of respondents claim to frequently or always carefully

read through Terms and Conditions, only 15% state that they understand their data flows. McDonald and Cranor [54] estimate that thorough study of all online privacy policies would take a typical user about 244 hours per year. Either they haven't read the Terms and Conditions as carefully as claimed, or the information was not adequate to provide them with this understanding. As Véliz and Grünewald [38] points out, one has to question the degree to which their consent can be considered 'informed'. One of our reviewers suggested to follow up on the extent to which participants understand the implications of their responses more empirically. For instance, in a future survey participants could be presented with the opportunity to read Terms and Conditions relating to the survey itself and later ask specific questions about their content, to verify the extent to which these have been read or understood. This process could mimic the conditions under which consent is often provided in online environments.

As data increasingly becomes a tool of exchange through which consumers gain access to different services, new tools are needed through which consumers can adjust their data flows according to their varied and context-dependent preferences. This is especially the case when external organisations trade these data to extract additional value [55, 56]. For example, Amardeo et al. [57] propose a concept of 'virtual identity', which refers to a form of digital identity management. Data subjects only reveal what is deemed necessary for the delivery of a specific service, and which can be readily adjusted depending on the respective contexts and circumstances.

Cate and Mayer-Schönberger [58] suggest shifting informational privacy settings away from the data subject altogether, by postulating responsible data stewardship practices for the data users. Our survey data suggests that the heterogeneity of individual and contextual preferences does not lend itself to this one-size-fits-all approach. Furthermore, the number of shared appliances and applications requiring individual review of terms and conditions followed by a considered selection of complex access choices makes this approach increasingly impractical.

We therefore propose a personalised data sharing format, which allows users to set their preferences in one place and apply them to all their associated appliances. Jointly used appliances share the lowest common denominator of their associated users. This approach requires a degree of standardisation. Within such a system appliances cannot share any data unless their user(s) have authorised the appliance to do so.

Users keep an overview of any appliances and applications that collect and

share their data (and with whom). If they change their mind and wish to include or exclude organisations from their approved list, this can be applied to all appliances and applications in one go. Access settings can themselves ‘learn’ from other user preferences, such as with fuzzy trust based access control scheme or ‘privacy coach’ functionality [59, 60].

Enhanced control and awareness have been shown to positively affect individuals’ willingness to provide and share data [16, 61, 41, 42].

We recognise that many technical, regulatory and institutional challenges need to be overcome to realise such an approach. The importance of data for future services, warrants further discussion of improved personal data sharing preference formats.

5. Conclusion

A representative sample of 701 UK participants has been surveyed on their attitudes towards smart service provisions and their willingness to share personal location data for different services and with different parties.

A discrepancy between the willingness to share data for services and willingness to share data with relevant organisation has been exposed. Trust in some of the key organisations appears to be low. While 37% are in favour of using location data for energy saving, 8% or less agree to share location data with utilities or smart home companies for this purpose. Only 15% claim to understand who has access to their location data, raising questions over the degree to which their consent can be considered ‘informed’.

It is therefore plausible that data is currently collected without fully informed consent from wide parts of the population. While a significant number of people claim to read the Terms and Conditions (32%), far fewer (15%) seem to appreciate what they are consenting to. Terms and Conditions that are not understood by users should be considered void.

The lack of awareness is clearly exemplified by the shift in ease over personal data sharing observed during the course of the survey itself. The response towards feeling uncomfortable about location data tracking between the start and the end of the survey shifted by 11 percentage points.

These results raise questions over the willingness to share personal location data with institutions, even when the implicit service provision is desirable. Furthermore, 70% feel that location data collection is outside their control and 65% would like to have more control.

If a smart energy system based on significant data sharing is to be achieved in a consensual fashion, trust in the institutions collecting and sharing the relevant data will need to be addressed. We have proposed an individualised personal data sharing preference format, which may address the sense of control over personal data and ultimately increase trust for its consented use.

Acknowledgement

This work is supported by the Engineering and Physical Sciences Research Council (EPSRC) under grant EP/M024652/1.

References

- [1] C. Wilson, T. Hargreaves, R. Hauxwell-Baldwin, Benefits and risks of smart home technologies, *Energy Policy*, 103 (2017).
- [2] B. K. Sovacool, D. D. Furszyfer Del Rio, Smart home technologies in europe: A critical review of concepts, benefits, risks and policies, *Renewable and Sustainable Energy Reviews* 120 (2020) 109663. doi:<https://doi.org/10.1016/j.rser.2019.109663>.
- [3] IEA, Digitalization and energy, IEA (2017). URL: <http://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf>.
- [4] S. Darby, Smart technology in the home: time for more clarity, *Building Research & Information* 46 (2018) 140–147.
- [5] M. Friedli, L. Kaufmann, F. Paganini, R. Kybyrz, Energy Efficiency of the Internet of Things?, Technical Report, IEA, 2016.
- [6] A. Bhati, M. Hansen, C. Chan, Energy conservation through smart homes in a smart city: A lesson for Singapore households, *Energy Policy* 104 (2017).
- [7] N. Balta-Ozkan, B. Boteler, O. Amerighi, European smart home market development: Public views on technical and economic aspects across the united kingdom, germany and italy, *Energy Research & Social Science*, 3 (2014).

- [8] BPIE, Is Europe ready for the smart buildings revolution? Mapping smart-readiness and innovative case studies, Technical Report, Buildings Performance Institute Europe, 2017.
- [9] J. Ramirez-Mendiola, P. Grünwald, N. Eyre, The diversity of residential electricity demand - a comparative analysis of metered and simulated data, *Energy and Buildings*, 151 (2017).
- [10] M. Kragh-Furbo, G. Walker, Electricity as (big) data: Metering, spatiotemporal granularity and value, *Big Data & Society* 1–12 (2018).
- [11] K. Zhou, C. Fu, S. Yang, Big data driven smart energy management: From big data to big insights, *Renewable and Sustainable Energy Reviews* 56 (2016) 215–225.
- [12] S. Firth, F. Fouchal, T. Kane, V. Dimitriou, T. Hassan, Decision support systems for domestic retrofit provision using smart home data streams, presented at: CIB W78 2013 The 30th International Conference on Applications of IT in the AEC Industry (2013).
- [13] K. Gram-Hanssen, S. Darby, "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home, *Energy Research & Social Science*, 37 (2018) 94–101.
- [14] M. Ackerman, T. Darrel, D. Weitzner, Privacy in context, *Human-Computer Interaction* 16 (2001).
- [15] H. Xu, H. Teo, B. Tan, R. Agarwal, The role of push-pull technology in privacy calculus: The case of location-based services, *Journal of Management Information Systems*, 26 (2009).
- [16] I. Hann, K. Hui, S. Lee, I. Png, Consumer privacy and marketing avoidance: A static model, *Management Science*, 54 (2008).
- [17] G. Danezis, S. Lewis, R. Anderson, How much is location privacy worth?, In *Proceedings of the Workshop on the Economics of Information Security Series* (2005).
- [18] D. Cvrcek, V. Matyas, M. Kumpost, G. Danezis, A study on the value of location privacy, *Proceedings of the 2006 ACM Workshop on Privacy in the Electronic Society* (2006).

- [19] KPMG, Convergence goes mainstream: Convenience edges out consumer concerns over privacy and security, Technical Report, Consumers & Convergence IV., 2010.
- [20] A. Paetz, E. Dütschke, W. Fichtner, Smart homes as a means to sustainable energy consumption: A study of consumer perceptions, *Journal of Consumer Policy*, 35 (2012).
- [21] Which?, Which industry sectors/organisations do people most trust and distrust?, Consumer Insights, Which?, 2014.
- [22] S. Meyer, A. Rakotonirainy, A survey of research on context-aware homes, *Australian Computer Society Conferences in Research and Practice in Information Technology*, 21 (2003).
- [23] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, J. Hubaux, Collaborative location privacy, *Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems* (2011).
- [24] N. Eagle, A. Pentland, Reality mining: Sensing complex social systems, *Personal and Ubiquitous Computing*, 10 (2005).
- [25] S. Peppet, Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent, *Texas Law Review*, 85 (2014).
- [26] P. Tucker, Has big data made anonymity impossible?, *MIT Technology Review* (2013).
- [27] R. Weber, Internet of things: Privacy issues revisited, *Computer Law & Security Review*, 31 (2015).
- [28] G. Weinberg, B. Milne, Y. Andonova, F. Hajjat, Internet of things: Convenience vs. privacy and secrecy, *Business Horizons*, 58 (2015).
- [29] L. John, A. Acquisti, G. Loewenstein, Strangers on a plane: Context-dependent willingness to divulge sensitive information, *Journal Of Consumer Research*, 37 (2011).
- [30] A. Tsohou, E. Kosta, Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, *Computer law & security review*, 33 (2017).

- [31] E. Clemons, J. Wilson, F. Jin, Investigations into consumers preferences concerning privacy: An initial step towards the development of modern and consistent privacy protections around the globe, 47th Hawaii International Conference on System Science (2014).
- [32] Which?, Control, alt or delete? The future of consumer data, Technical Report, Which?, 2018. URL: <https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report>.
- [33] S. Ferber, How the internet of things changes everything, Technical Report, hbr.org, 2013. URL: <http://blogs.hbr.org/2013/05/how-the-internet-of-things-cha/>.
- [34] N. Singer, J. Merrill, When a company is put up for sale, in many cases, your personal data is, too, Technical Report, The New York Times, 2015. URL: <https://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html>.
- [35] O. Tene, J. Polonetsky, Big data for all: Privacy and user control in the age of analytics, *Northwestern Journal of Technology and Intellectual Property*, 11 (2013).
- [36] X. Caron, R. Bosua, S. Maynard, A. Ahmad, The internet of things (IoT) and its impact on individual privacy: An Australian perspective, *Computer law & security review*, 32 (2016).
- [37] S. Wachter, Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR, *Computer Law & Security Review*, 34 (2018).
- [38] C. Véliz, P. Grünewald, Protecting data privacy is key to a smart energy future, *Nature Energy* 3 (2018) 702–704.
- [39] S. Döbelt, M. Jung, M. Busch, M. Tscheligi, Consumers’ privacy concerns and implications for a privacy preserving smart grid architecture — results of an austrian study, *Energy Research & Social Science*, 9 (2015).

- [40] R. Hoenkamp, G. Huitema, A. de Moor-van Vugt, The neglected consumer: The case of the smart meter rollout in the Netherlands, *Renewable Energy Law & Policy Review*, 269 (2011).
- [41] M. Fell, D. Shipworth, G. Huebner, C. Elwell, Knowing me, knowing you: the role of trust, locus of control and privacy concern in acceptance of domestic electricity demand-side response, *ECEEE 2015 Summer Study Proceedings* (2015).
- [42] C. Horne, B. Darras, E. Bean, A. Srivastava, S. Frickel, Privacy, technology, and norms: The case of smart meters, *Social Science Research*, 51 (2015).
- [43] K. Raimi, A. Carrico, Understanding and beliefs about smart energy technology, *Energy Research & Social Science*, 12 (2016).
- [44] L. Zhao, Y. Lu, S. Gupta, Disclosure intention of location-related information in location-based social network services, *International Journal of Electronic Commerce*, 16 (2012).
- [45] E. Kaasinen, User needs for location-aware mobile services, *Personal and Ubiquitous Computing*, 7 (2003).
- [46] N. Limpf, H. Voorveld, Mobile location-based advertising: How information privacy concerns influence consumers? Attitude and acceptance, *Journal of Interactive Advertising* 15 (2015).
- [47] T. Reisch, Information privacy in the smart home: A user-centric study on location data, MSc thesis. University of Oxford. Available at: <https://www.academia.edu/41151718> (2018).
- [48] A. Mosenia, X. Dai, P. Mittal, K. Niraj, Pinme: Tracking a smartphone user around the world, *IEEE Trans. Multi-Scale Computing Systems* (2018).
- [49] Consultancy.uk, UK smartphone penetration continues to rise to 85% of adult population, Technical Report, Consultancy.uk, 2017.
- [50] L. Sandys, A strategy for a modern digitalised energy system, Technical Report, Energy Data Taskforce, 2019.

- [51] C. Advice, The Smart Meter Data Dashboard, Technical Report, Citizens Advice, 2018.
- [52] A. Cavoukian, Privacy by Design: The 7 Foundational Principles, Technical Report, iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf, 2016.
- [53] EU, EU General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, European Union, 2016.
- [54] A. McDonald, L. Cranor, The cost of reading privacy policies, *I/S A Journal of Law and Policy for the Information Society* 4 (2008).
- [55] J. Van Dijck, Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology, *Surveillance & Society* 12 (2014).
- [56] V. Mayer-Schöneberger, T. Range, Reinventing capitalism in the age of big, Hachette Book Group: USA (2018).
- [57] C. Amardeo, S. Girao, J. Girao, Identities in the future internet of things, *Wireless Personal Communications*, 353 (2009).
- [58] F. Cate, V. Mayer-Schönberger, Notice and consent in a world of big data, *International Data Privacy Law*, 13 (2013).
- [59] P. Mahalle, P. Thakre, N. Prasad, A fuzzy approach to trust based access control in internet of things, *Wireless VITAE 2013* (2013).
- [60] G. Broenink, J. Hoepman, C. van Hof, R. van Kranenburg, D. Smits, T. Wisman, The Privacy Coach: Supporting Customer Privacy in the Internet of Things, Technical Report, arXiv:1001.4459 [cs.CY], 2010.
- [61] K. Hui, H. Teo, S. Lee, The value of privacy assurance: An exploratory field experiment, *MIS Quarterly* 31 (2007).

Appendix A

Table 4: Full set of survey questions and response options

No	Question	Options
1.A	I would feel uncomfortable to have my location tracked by my smartphone.	
1.B	To what extent would you agree to have the following home appliances turn on/off in response to your location? (1) Lights, (2) Heating/thermostat, (3) Television, (4) Fridge, (5) Washing machine, (6) Hot water tank, (7) Dishwasher, (8) Air conditioning, (9) Radio, (10) Home security system, (11) Window shutters	
1.C	To what extent would you agree or disagree to share your location data in exchange for...	Table 2
1.D	To what extent would you agree or disagree to share your location data with...	Table 3
1.E	What is your gender?	(1) Male; (2) Female; (3) Other.
1.F	What is your age?	(1) 18-24, (2) 25-34, (3) 35-44, (4) 45-54, (5), 55-64, (6) 65+.
1.G	What is your highest educational qualification?	(1) Doctoral degree, (2) Master's degree, (3) Bachelor's degree, (4), Higher National Diploma,

No	Question	Options
1.H	What is your total annual income before deductions for income tax, National Insurance, etc.?	(5) Higher National Certificate, (6) A -Level (or equivalent), (7) GCSE, (8) None of the above. (1) up to £6,999, (2) £7,000 – £14,999, (3) £15,000 – £24,999, (4) £25,000 -£34,999, (5) £35,000 -£44,999, (6) £45,000 - £54,999, (7) £55,000 or more, (8) n/a.
1.I	When do you tend to adopt new technologies?	Scale 1-5, [1: I am amongst the first, 5: I am amongst the last].
1.J	Our global problems are. . .	(1) Created by technology, (2) Worsened by technology, (3) Independent to technology, (4) Improved by technology, (5) Solved by technology, (6) I'm not sure.
1.K	Do you own a. . .	(1) Smartphone, (2) Mobile phone, (3) Both (a mobile phone and a smartphone), (4) Neither.

No	Question	Options
1.L	My phone screen is amongst the last things I look at in the evening and the first thing I look at when I wake up.	
1.M	I only very rarely use my phone	
1.N	How often do you use the following services on your smartphone? [Maps/navigation; Track friends and family].	(1) Very frequently, (2) Frequently, (3) Sometimes, (4) Rarely, (5) Never.
1.O	Do you own any of the following smart home appliances? And if not, would you like to? [Smart thermostat, Smart lights, Smart plug, Smart meter, Voice assistant, Smart home security system, Smart fridge, Smart washer/dryer].	(1) I own it, (2) I want to own it, (3) I'm unsure if I want to own it, (4) I don't want to own it.
1.P	If you own smart home appliances, do they respond to the location of your smartphone?	(1) Yes, (2) No, (3) I'm not sure
2.A	The ways in which my location data is collected, processed and shared is...	(1) Completely outside of my control, (2) Somewhat outside of my control, (3) Fully in my control, (4) I'm not sure.
2.B	I would like to have better control over how my location data is collected, used and shared.	

No	Question	Options
2.C	I consciously disable my smartphone's location service. . . [Only posed to smartphone users].	(1) Always, (2) Frequently, (3) Sometimes, (4) Rarely, (5) Never, (6) I'm not sure.
2.D	I check and adjust my privacy settings. . .	(1) Always, (2) Frequently, (3) Sometimes, (4) Rarely, (5) Never, (6) I'm not sure.
2.E	It is difficult to control my location data settings.	
3.A	Compared to most people, my awareness of privacy issues is. . .	(1) Non-existent, (2) Poor, (3) Average, (4) Above average, (5) Outstanding, (6) I'm not sure.
3.B.	It is clear to me when my location data is collected.	
3.C	I understand who has access to my location data.	
3.D	I carefully read through Terms and Conditions. . .	(1) Always, (2) Frequently, (3) Sometimes, (4) Rarely, (5) Never, (6) I'm not sure.
3.E	I would feel uncomfortable to have my location tracked by my smartphone. [Posed towards beginning of survey].	
3.F	What information can be extracted from a person's location data?	Checkbox. [Check as many as applicable]

No	Question	Options
	[Regular habits and activities; Relationships; Income; Interests and hobbies; Political views; Spending patterns; Fitness profile; Profession; Mode of transport (walking, cycling, car, railway); A detailed map of their whereabouts and movements; Their age; None of the above].	
3.G	What are you concerned about when sharing your location data? [Identify theft; My data falling into the wrong hands; Commercial disadvantages; Targeted advertisement; Surveillance; Illegal hacking; My data being passed on; Other (not listed here)].	Checkbox. [Check as many as applicable]
3.H	To what extent would you agree with the following theoretical uses of location data? (1) Your family and/or spouse have a constant overview of your location; (2) Your location data has been used to assess how healthy your lifestyle is. Your health insurance premium and other services are affected; (3) Your credit rating is affected due to insights your credit institute gathers from your location data; (4) Your GP makes health and dietary recommendations based on your location data;	

No	Question	Options
	(5) A company targets you with adverts based on your daily routines from your location data;	
	(6) Your pay is adjusted after your employer reviews your location data;	
	(7) You track your child's location data].	
3.I	I would feel uncomfortable to have my location tracked by my smartphone. [At end of survey].	