Ofgem - Data Sharing in a Digital Future

Call for Input

Introduction

Thank you for the chance to respond to this call for evidence. We are writing on behalf of the Bristol Cyber Security Group and REPHRAIN, the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online. REPHRAIN is the UK's world-leading interdisciplinary community focused on the protection of citizens online. As a UKRI-funded National Research Centre, we boast a critical mass of over 120 internationally leading experts at 13 UK institutions working across 40+ diverse research projects and 23 founding industry, non-profit, government, law, regulation and international research centre partners.

As an interdisciplinary and engaged research group, we work collaboratively on addressing the three following missions:

- Delivering privacy at scale while mitigating its misuse to inflict harms
- Minimising harms while maximising benefits from a sharing-driven digital economy
- Balancing individual agency vs. social good.

We are addressing this consultation since our researchers have extensive expertise in the regulatory aspects of cyber security, measuring and defining harms, and evaluating authentication solutions. This is a submission from the REPHRAIN centre made by Dr Ola Michalec and Prof Awais Rasid.

We are happy to arrange a follow-up meeting to provide details of our work in progress in the area and discuss further details of developing a consumer consent mechanism.

1. Yes/No: Do you agree that a Consumer Consent solution is required as per the taskforce's recommendation?

Yes, we believe that consumer consent solution for enabling lowering bills as well as minimising carbon footprint is required and that it needs to be provided in a meaningful, standardised and trusted way.

The document states the need to devlop an 'easy' solution but this might not be realistic as this is an incredibly complex area so we should be careful of overpromising. However, there is some scope for doing translational/educational work of making privacy, security and data sharing topics less complex.

It is also important to clearly define what use cases of data sharing are not appropriate to prevent corporate surveillance practices or profiling for advertising. Finally, the scope of 'third parties' needs to be understood and clearly defined before pitching the idea to the members of the public.

2. Could you please provide any reasons why the current methods for obtaining consent from a consumer might be ineffective or inefficient?

The current consent mechanisms found across apps and websites are prime examples of what to *avoid* when it comes to the consent mechanism design.

Research across computer sciences, human-computer interaction, law and politics leveraged the following critiques of the current methods of consent in digital environments:
- technical and legal terminology in the consent forms; users shouldn’t be expected to engage with lengthy T&Cs full of jargon. Even the Ofgem documents outlines quite specific legal terms like “third-party providers, such as demand-side response service providers (DSRSPs), original equipment manufacturers” (Becher and Benolier, 2021)
- lack of standardised (or at least consistent) understanding what ‘good’ level of consent and privacy look like across software developers, UX designers and members of the public. For example, privacy some cookie notices might introduce the gold/silver/bronze levels of how widely you share your data, but in one case ‘gold’ refers to maxmised privacy and in other – maximised sharing. (Patanik, forthcoming; Iwaya et al, 2022)
- the lack of dynamic consent and functionality to revoke consent – users currently don’t have simple access to a mechanism which would allow them to revoke consent while preserving desired functionality of apps and web services (Schuler Scott et al, 2019)
- the aftermath of having ineffective consent mechanisms in web cookies is profiling users for the benefit of advertisers with intrusive or ‘creepy’ adverts, sometimes inferring deeply personal information based on their day to day activities.
- taking a broader view, users aren’t sufficiently presented with a convincing argument for data sharing and sufficient assurances of the trustworthiness of the service providers. Energy industry stakeholders shouldn’t assume that consumers agree that there is a case for data sharing.

3. Do you believe that consumers are sufficiently motivated to engage with the consent solutions proposed in this Call for Input? Please elaborate on your answer.

Currently, the need for consumer consent for energy data sharing is well articulated within the industry but less so with the general public, or at least smart energy device owners or the media. The articulation of the consumer benefits needs to be more specific using concrete examples beyond the generic goal of “with trusted market participants who can provide them energy services to lower their bills, as well as their carbon footprint”. This requires drawing on expertise in fields like speculative futures, scenarios or horizon scanning (Michalec and Bourne, 2023; and forthcoming).

Consumers need to be reassured at a granular level about the types of data that will be shared (esp. If they could be linked to inferring private activities), who with and for what purpose.

4. Do you agree that the four use cases referenced are high priority use cases? Can you describe any other high priority use cases?

We agree that the priority use cases should come from a variety of contexts, to demonstrate how the mechanism is serving the industry as a whole (consumer/industry/government), as specified in the document.

However, the consultation document doesn’t specify what they mean by ‘priority’ - are they priority because they’re the easiest to implement? The easiest to demonstrate and communicate the value? The most in need of a new approach? Each of them is a valid reason to prioritise a use case. Either way, Ofgem should specify how they prioritise use cases and communicate it in a transparent manner to consumers/testers.

The ideas proposed as use cases for vulnerable consumers could be abused for surveillance and extraction of money from the consumers. At the moment, energy industry has a poor record on this front. In this case, extra reassurances need to be provided to the consumer.

An example of a priority service with vulnerable customers in mind is the improvement of the Priority Services Register. Our research with energy sector stakeholders shows that the data of vulnerable consumers is dispersed across energy suppliers and each supplier has their own register with their own definitions. This makes it challenging to ensure continuity of supply for vulnerable people if they were to switch their providers (e.g. people using electric life-supporting equipment who cannot be cut off from power supply).

7. Which of the options referenced in this chapter do you believe would be the

most appropriate Consumer Consent solution, for the industry, the government, and the consumer?

- Option One: A single technical solution to obtain consent, such as a Consumer Consent dashboard. This proposal builds on the Energy Digitalisation Taskforce's recommendation to deliver a technical consent solution.
- Option Two: A set of principles outlining a consistent way for trusted market participants to obtain consent, such as Data Best Practice.
- Option Three: An industry-developed code of conduct outlining a consistent way for trusted market participants to obtain consent, such as the Confidence Code.

Option One: This option seems the easiest to imagine in practice and it appears the most consumer-facing. It is the only one which mentions *how* the consent would actually be obtained in practice. I think this one seems preferable as it is the most readily understandable, which is critical for engaging members of the public in any data-related questions.

Option Two: The history of internet regulations (Mittelstand, 2019) shows that princples-based solutions can be highly ineffective and lead to questionable market practices. For example, the rise of workplace surveillance tools since COVID which have been deemed GDPR-compliant in many cases due to the clause of 'reasonable use' (Metcalf et al, 2023). Our recent research on cyber security governance in energy sector (Michalec et al., 2023) shows the risks of principles-based approach in the emerging field where the maturity of expertise is so low that the sector hasn't arrived at a shared understanding of how practicing 'good' principles would look like. We, therefore, caution against Option Two.

Option Three: this option is the least bold one, which could be a benefit in terms of adoption. There could also be some learnings from the secure development code of practice for app environments (https://www.ncsc.gov.uk/blog-post/code-of-practice-for-app-store-operators-and-developers#:~:text=This%20Code%20of%20Practice%20is,malicious%20actors%20and%20vulnerable%20apps.). However, the concern is its voluntary and open nature will leave a lot of room for interpretation, hence likely delays. If Ofgem is serious about timely decarbonisation, it should use all political leverages to create stronger regulatory requirements.

8. Please can you explain why you chose a specific option? Do you have any suggestions on how to improve this option?

Ofgem and the energy industry broadly need to be careful about framing it as a 'technical solution' as it could be so much more than that. We recommend avoiding this term all together and instead find a name which describes a service provided to the consumers, e.g. ‘consumer energy data dashboard’. If implemented correctly, it could be a tool for public engagement, improvement in citizen participation in democracy and regulation of energy companies. The ‘risks’ of the solution outlined in the document (i.e., the need for additional public engagement to ensure the buy in from all demographics) should be the normal requirements for successful technology adoption anyway!

9. What barriers do you see to the successful implementation of a new consent solution?

A rich scholarship on barriers to technology adoption in energy and beyond provides plenty of useful lessons for this case. Sovacool et al (2017) caution against the apathy members of the public felt when pitched smart meters or when they first got them installed. Our past research (Michalec et al., 2019) showed that the initial government communications about the benefits of smart meters were vague and not enough relevant to members of the public, which causes mistrust and lack of engagement. Consumers need to know concrete examples of benefits to them.

Gaining public trust is key and it comes down to every layer – information security, governance and trust in institutions. Providing robust assurances and communicating the purpose and inner workings of the consent mechanism is key. Across the sector, institutional trust is not distributed evenly, with some companies having a poor reputation among consumers. This needs to be addressed before any data sharing mechanisms are widely proposed in the public or media.

There is a lot of mistrust about data sharing in the aftermath of Cambridge Analytica and the rise of ad tech in general. Members of the public need to know exactly who else benefits from their data and whether those are public services or products for sale. There need to be clearly communicated examples of inappropriate use/ inappropriate actors who won’t be part of the scheme. The potential misuse of AI e.g., for profiling should also be discussed (ideally clearly specified what counts as fair use and what the risks are).

Finally, we’re uncertain about the UK’s infrastructural capabilities to provide large scale secure capabilities to share data without privacy breaches. We need to be aware of a dim landscape w.r.t. the ongoing data breaches and learn from them as we go along.

10. What do you think are the roles of Ofgem, industry and other stakeholders in enabling a simple and effective consent solution?

The development of consumer consent mechanism could be a part of a nation-wide campaign to bring energy sector decarbonisation into the spotlight. So many exciting things are happening in the sector, yet they’re not widely known beyond the narrow circle of stakeholders. Bringing the case of digitalisation and energy data sharing as a public issue to be debated on TV and in new papers could improve engagement with the technology and test early ideas so that the system is developed in as socially acceptable and more democratic manner.

REFERENCES

Becher, S. I., & Benoliel, U. (2021). Law in books and law in action: the readability of privacy policies and the gdpr. In Consumer law and economics (pp. 179-204). Springer International Publishing.

Iwaya, L. H., Babar, M. A., & Rashid, A. (2022). Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organisational Culture, and Current Practices. arXiv preprint arXiv:2211.08916.

Metcalf, K., Irani, L., & del Águila, V. U. (2023). Contested Care: COVID-19 surveillance and health data in the workplace. *Surveillance & Society*, *21*(2), 139-153.

Michalec, A., Hayes, E., Longhurst, J., & Tudgey, D. (2019). Enhancing the communication potential of smart metering for energy and water. *Utilities Policy*, *56*, 33-40.

Michalec, O and Bourne, J. (2023) Electric Feels Artistic responses to research exploring human dimensions of digital energy transformation https://petras-iot.org/update/electric-feels/

Michalec, O., Shreeve, B., & Rashid, A. (2023). Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems. *Energy Research & Social Science*, *106*, 103327.

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature machine intelligence*, *1*(11), 501-507.

Schuler Scott, A., Goldsmith, M., Teare, H., Webb, H., & Creese, S. (2019). Why we trust dynamic consent to deliver on privacy. In Trust Management XIII: 13th IFIP WG 11.11 International Conference, IFIPTM 2019, Copenhagen, Denmark, July 17-19, 2019, Proceedings 13 (pp. 28-38). Springer International Publishing.

Sovacool, B. K., Kivimaa, P., Hielscher, S., & Jenkins, K. (2017). Vulnerability and resistance in the United Kingdom's smart meter transition. *Energy Policy*, *109*, 767-781.