Icebreaker One response to Ofgem's Consumer Consent Solution Consultation

FAO: Linsay Jones, Tom Jones, Charley Clark, Energy System Digitalisation Team
digitalisation@ofgem.gov.uk

This is Icebreaker One's response to Ofgem's Consumer Consent Solution Consultation[1]. It can be published openly.

Please note that throughout this consultation, Icebreaker One (IB1) uses the terms Open, Shared and Closed data as defined here[2]. Please note IB1's response to Ofgem's Governing of a Data Sharing Infrastructure (DSI) Consultation.[3] We urge the alignment of the design principles and governance principles between DSI and the consumer consent solution.

If you have any questions about our submission or require clarifications please do not hesitate to contact us via openenergy@ib1.org. Thank you for considering our submission.

Consultation response:

Q1. Do you agree with these Design Principles? Would you recommend any additional Design Principles?

Please note IB1's response to Ofgem's Governing of a Data Sharing Infrastructure (DSI) Consultation.[4] We urge the alignment of the design principles and governance principles between the Data Sharing Infrastructure (DSI) and the consumer consent solution. Please find our additional comments on each of the design principles below:

Simple and Low Friction

We recommend a simple and low friction option which **builds on previous implementation in other industries**, for example Open Banking which has been endorsed by the Competition and Markets Authority (CMA) and the Financial Conduct Authority (FCA), to ensure Ofgem is aligned with national strategy.

However, the solution outlined in paragraph 1.6 envisages a centralised system that introduces complexity and friction. The proposal introduces complexity by setting out a single implementation which must meet all requirements across the industry,

[1] https://www.ofgem.gov.uk/consultation/consumer-consent-solution-consultation
[2] https://icebreakerone.org/open-shared-closed/
[3] https://ib1.org/2024/09/24/ib1-response-to-ofgems-governance-of-a-data-sharing-infrastructure-dsi-consultation/
[4] https://ib1.org/2024/09/24/ib1-response-to-ofgems-governance-of-a-data-sharing-infrastructure-dsi-consultation/

particularly around integration, security, accessibility, and data synchronisation, while avoiding becoming a bottleneck for performance and availability.

It will add friction by requiring users to interact with (and be prepared to trust) an additional organisation, and maintain another account, password, and MFA method.

Interoperable

IB1 strongly recommends taking a joined up approach which is **interoperable with initiatives across the economy**. We suggest the solution define relationships with adjacent bodies in the energy sector and beyond to enable cross sector interoperability.

> Example of cross-sector data sharing initiative:
> Icebreaker One convenes the cross-sector Perseus Scheme[5] (ib1.org/perseus) to enable automated carbon emissions reporting for every SME in the UK. It creates the rules and processes that make automated reporting possible to enable products and services such as accounting platforms, emissions calculators, and reporting software to be developed that deliver higher-quality emissions data at scale. Perseus convenes hundreds of cross-sector organisations to ensure user needs and barriers from across the supply chains are captured and incorporated into the Scheme.
>
> The Scheme includes participants including SmartDCC, Perse, Sage, Visa, Lloyds Banking Group, to ensure strong alignment between the energy and financial sectors around Smart Data governance. It is additive to existing initiatives.

Agile, Flexible, and Scalable

We suggest introducing a clear process for **change managemen**t in this principle. As governance needs will likely change with time. This may include indication of how the list of permitted data use purposes will be maintained with additions and removals.

Transparent and Informative

IB1 strongly recommends that documentation is **published openly**, along with any accompanying processes, methodologies, and governance processes, as also suggested in our DSI consultation response.[6]

Inclusive by Design

The solution intends to protect vulnerable consumers, which can be at odds with requiring technical checks (MFA or similar). We urge the defined user journeys, messaging, terms, and customer support to be easy to use, transparent, and explained in a way that someone with a low technical reading comprehension can engage with.

[5] Schemes - which operate within a Trust Framework environment - are defined through structured programs to facilitate and govern the sharing of data among participating entities in the context of a specific use case, or set of related use cases.

[6] https://ib1.org/2024/09/24/ib1-response-to-ofgems-governance-of-a-data-sharing-infrastructure-dsi-consultation/

Secure by design
We encourage working with the National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC). We would also recommend an adversarial analysis to be performed to see where security gaps may occur, and may affect the proposed architecture. The solution must avoid creating large targets for hackers where a compromise affects many consumers.

Please find our comments on additional design principles:

- How will different household types be handled in this solution? (i.e. providing consent as an individual versus households)
- We suggest including an element of **trust** to the design principles. As mentioned in the Data Sharing in a Digital Future consultation[7], there is a lack of trust in energy companies by consumers. Trust is key for obtaining consent.
    - There may already be 'trust' in an entity if there is already an existing contractual relationship with suppliers (rather than introducing a new body).
- It is essential to view consumer consent mechanisms, such as Open Banking, **holistically** as a Trust Framework[8] – an entity incorporating technical, communications, engagement, legal and ongoing governance arrangements – rather than a technical solution.
- We suggest providing clearer information about use cases and the approach to defining them. A use case describes a specific situation, or set of circumstances, in which a product or service can be used, not just data types to be targeted. This approach to defining a use case can also assist in defining cross-sectoral use cases. (For example, Perseus uses both smart meter and tariff data to enable calculated emissions to be used in lending decisions by the financial sector).
- We note that 'Open Source' is not mentioned throughout the consultation. If not incorporated, there is a risk of inadvertently creating a monopoly.

Q2. Do you have a preference between the centralised, decentralised or hybrid models? Please elaborate.

IB1 has a preference for a decentralised model, which aligns with the approach taken by Open Banking, and the architectural principles of the Data Sharing Infrastructure. The proposed solutions are centralised, with a single database which manages consent across all Suppliers. As stated in IB1's call for input on Data Sharing in a Digital Future,[9] we suggest a Trust Framework option should be considered.

An Open Banking style Consumer Consent mechanism should be viewed **holistically** as a Trust Framework - an entity incorporating technical, communications, engagement, legal and ongoing governance arrangements - rather than solely a technical solution.

[7] https://www.ofgem.gov.uk/publications/data-sharing-digital-future

[8] Trust Frameworks operate at the level of a defined governance domain (e.g. sector or geography) to collaboratively establish and maintain a light layer of identity management, governance, definitions, principles and Open Standards for data sharing

[9] https://ib1.org/2024/02/01/ib1-response-to-ofgems-call-for-input-on-data-sharing-in-a-digital-future/

What are Trust Frameworks and Schemes?
Working on behalf of its public and private sector members, Icebreaker One operates Trust Frameworks and Schemes across a variety of sector specific and cross-sectoral domains. Trust Frameworks[10] operate at the level of a defined governance domain (e.g. sector or geography) to collaboratively establish and maintain a light layer of identity management, governance, definitions, principles and Open Standards for data sharing.

Schemes[11] - which operate within a Trust Framework environment - are defined through structured programs to facilitate and govern the sharing of data among participating entities in the context of a specific use case, or set of related use cases. They collaboratively define the rules concerning what data can be shared, why (purpose), by whom (roles), and how (technical requirements, legal structure, etc). They also address the communications requirements of the Scheme and its relationship with the surrounding policy, regulatory, and legislative landscape. The structural operation of Schemes, linked to specific Trust Frameworks, is capable of supporting the progression of multiple data-sharing initiatives with distinct needs (e.g. security requirements, personal data protection etc), whist ensuring interoperability, conceptual cohesion, open market development, transparency, and good governance principles (e.g. fairness, value-sharing, protection of data rights) across the wider Trust Framework domain.

The development of Trust Frameworks and Schemes by IB1 builds from existing bodies of knowledge and experience established by initiatives such as Open Banking, cross-sector governance initiatives such as the Smart Data Council, and expert knowledge bases within academic and industry research. Icebreaker One's work to date demonstrates that Trust Frameworks and Schemes provide a robust but flexible approach to the governance of data sharing infrastructure which is adaptable across multiple use cases, sectors, and governance domains. IB1 has worked with use cases and organisations spanning cross-sector spaces as well as energy, water, finance, insurance, transport, and supply chains sectors. It is working with Open Banking Limited on interoperability between Open Energy and Open Banking.

How a solution could be modelled on Open Banking:
Open Banking is decentralised, where suppliers are responsible for managing consent for their customers, using the existing trust and account management in the supplier/consumer relationship.

Each Supplier would provide a consent hub within their existing App and account management website. The implementation of this consent hub would be chosen by the

[10] https://ib1.org/definitions/trust-framework/
[11] https://ib1.org/definitions/scheme/

supplier, who are free to develop their own, collaborate on an open source implementation, or buy in a solution managed by one of many software vendors.

When a consumer is asked to provide meter data and consent, the service uses a centrally maintained list of Suppliers, and asks the user to choose their Supplier. Then, using standard protocols in a technical solution using the architectural principles from Open Banking, the service asks the user to authenticate with their Supplier. After the user gives consent, the Supplier returns a token to the service to access meter data.

Meter data can be fetched via the Supplier's service, or direct from Smart DCC using the token created by the Supplier.

When a consumer changes Supplier, a list of consents would be passed to the winning Supplier, who would then give the user the opportunity to give the same consents to maintain their connections to the services they use.

The advantages of this approach include:

- Matching the mental model of the user, who sees their Supplier as the source of data about their energy use, and therefore:
    - Reuses the login and protections of their online account with their Supplier
    - Minimises friction in the user experience, by identifying the meter through their supplier login, avoiding the need for the user to enter meter numbers and authentication codes from an IHD
    - Eliminates the ability of scammers to impersonate an official body that consumers do not fully understand
- Creation of an agile market of consent providers who can provide for different purposes and compete on functionality and capabilities, including
    - Integration into account management systems
    - Meeting diverse accessibility requirements by avoiding the need to wait for a central provider to solve, for example language provision in Welsh and other languages used in the UK
- Improved acceptance by Suppliers, who have invested in creating brand recognition and building trust with consumers
- Reduced delivery costs.
    - Customer support functions are already provided by Suppliers
    - Suppliers already securely process Smart Meter data
- Increased reliability through the use of an inherently scalable and resilient technical architecture.
- Increased security by eliminating a single big target, which would be attractive for hackers and has the potential to affect all consumers in the UK.

Q3. Do you consider the security measures referenced in this section, including the access control measures, will meet the requirements of a consent solution holding consumer data? Which additional protections would you recommend?

The ISO standard example is appreciated. However, it is also a closed standard which can be prohibitive for some organisations. As such, we suggest Ofgem follow best practice to always additionally reference an open standard to ensure optionality (and lay out an understanding why a standard is considered equivalent or acceptable). We have the following additional comments:

- In addition to security certifications, such as ISO27001 and Cyber Essentials, we recommend mandating specific technical security standards. These must be agile to respond to changing security requirements and threats. An example is FAPI,[12] which mandates specific security choices with sufficient implementation flexibility to be practical in most environments.
- We believe it is worth noting that where participation in society or consumption of common goods and services requires the occasional interaction with a well-known statutory body, scammers will use this expectation and trust to exploit consumers. Ensuring smart meter owners are well-informed as to the security threats and understand how to recognise and avoid them will be an additional communication and support burden on a centralised consent management body. We suggest awareness of:
  - HMRC has published a list of common methods scammers use to impersonate HMRC.[13]
  - The threat of disconnection of electricity is a powerful motivator to engage with a phishing email.
- The benefits of renewing consent every 12 months may be outweighed by disadvantages and risks. We recommend a risk/benefit analysis to ensure these are balanced, noting:
  - a renewal process gives an opportunity for phishing scams
  - a renewal request which comes from an organisation the user does not know is likely to be ignored, breaking data flows.
- Using MFA for security is good practice, but with a centralised consent hub, it requires a new login and authentication method which introduces friction. This would be unnecessary if the smart meter owner authenticates via an existing Supplier account, which will already have appropriate security measures.
- We encourage working closely with NPSA and NCSC to ensure their feedback is incorporated.
- We suggest performing an adversarial analysis to highlight gaps, and within this, prioritise consideration of vulnerable customers.

Q4. Do you consider these standards are sufficient parameters to ensure inclusivity, accessibility and interoperability for the consent solution? Which standards would you recommend?

IB1 suggest addressing the following comments on inclusivity:

- We recommend support for other languages (Welsh, other languages used in the UK)

[12] https://openid.net/wg/fapi/

[13] https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples

- We strongly suggest considering how the consent solution leads to digital exclusion, and compound exclusion
- We encourage a measurement of diversity which will be considered with design, including disabilities, excluded from the Equalities Act like dyslexia, or options for text dictation.

Q5. Do you agree with the options assessment conducted by Ofgem? If not, why?

We would value more insight as to why the assessment is limited to retail energy sector organisations, and does not include other well established and evidenced successful consumer facing organisations for consideration. We would suggest taking a broader view, and consider other classes of organisation that have regular, secure contact with consumers.

Q6. Do you agree with Ofgem's minded-to position that RECCo should be selected as the Delivery Body for the consent solution? If not, which of the three proposed organisations should be selected as the Delivery Body for the consent solution, and why?

We are currently unable to agree with the selection of any Delivery Body due to the following constraints:

- As stated in our response in Q5, we would appreciate more robust evidence as to why other organisations were not considered for this role
- We suggest an opportunity for the three organisations (DCC, RECCo, Electralink) to respond publicly to additional matters raised via this consultation before being able to indicate a fully informed opinion

Q7. Do you hold any views as to how the proposed solution should be funded? Please consider the points regarding fairness raised in paragraphs 4.12–4.14 and Ofgem's duty to consumers when providing your answer.

We have no comment on this.

Q8. Do you agree with our position to make sharing consent data with consumers (via the consent solution) an obligation for licensees?

We suggest any chosen consent mechanisms are adequately interoperable to be a part of a new obligation. At present we are not confident the suggested solution is adequately interoperable. We suggest the potential for a phased approach.

We also highlight a potential point of confusion for consumers if consent, which has been granted via other mechanisms, is displayed alongside direct consent which they have the authority to withdraw. We suggest clearly articulating to consumers how consent has been granted (if, for example, it has been granted via other means) and therefore what authority they have to withdraw this consent.

Q9 Do you consider SLC 0 an appropriate route for implementing these changes, or should Ofgem create a bespoke licence condition?

We have no comment on this.