

Ctrl-Shift's Response to the CMA consultation on the Future of OBIE

16th April 2021

Dear CMA,

Thank you for the opportunity to respond to your consultation on the future of OBIE. The questions raised in the consultation are wide ranging and pertinent, and two in particular relate to topics in which we feel we have greatest expertise. We have focused our response on these, Questions 14 and 15.

In our reply to Question 14 we outline our analysis, to provide context, before addressing the specific question. Our response to Question 15 follows from our thinking, described in our response to Question 14.

Question 14: Could or should the Future Entity, as UK Finance has suggested, be a suitable vehicle for the implementation of other “open” projects such as the FCA’s Open Finance initiative and the BEIS Smart Data project? The Open Finance and Smart Data initiatives are not, as yet, fully defined. How, therefore might the Future Entity be designed so as to accommodate their requirements?

Conceptually, the EU and the UK had different starting points from which they approached personal data sharing, and this shows through, despite the common ground of GDPR. The EU’s approach to personal data sharing is rooted in the extension of the Human Rights concepts developed in the 1950’s, into today’s digital era. At its heart lay ideas of extending individual freedoms and rights combined with economic growth imperatives. The UK’s perspective on personal data sharing has its roots in promoting competition within regulated markets, to address the friction experienced by customers in changing providers, which has led to inefficient markets.

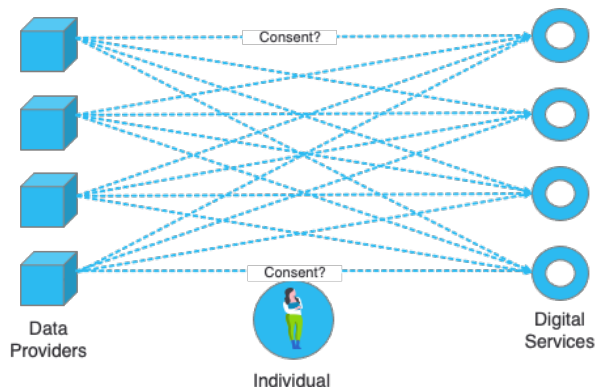
In their own way, both have borne fruit. In the EU with GDPR and in the UK with Open Banking. However, it is important to understand and acknowledge the limitations of Open Banking architecture as the basis for an approach to cross-sectorial data sharing.

The question relates to an end-state where an equivalent of “Open Banking Implementation Entities” (plural) are established for each industrial sector and the rules for that sector split between those Entities and the sector regulator, with some “Future Entity” created to promote lightweight “co-ordination” between the multiple sectors. This approach has at least three flaws, any one of which would be fatal to a UK aspiration to lead globally on cross-sectorial data sharing:

1. Consent management:

Under GDPR consumer consent must be freely given, specific, informed and unambiguous, when there are many digital service providers and data providers across multiple sectors the current architecture of Open Banking does not scale.

As our digital economy grows and accelerates and the data is needed to be shared from multiple data providers and used by an ever-increasing number of digital services, under the current Open Banking market architecture the number of consents that an individual will need to provide increases exponentially. This will rapidly become untenable from a individual and market management and risk perspective. The issue can be illustrated as follows:



Open Banking Architecture (Today)

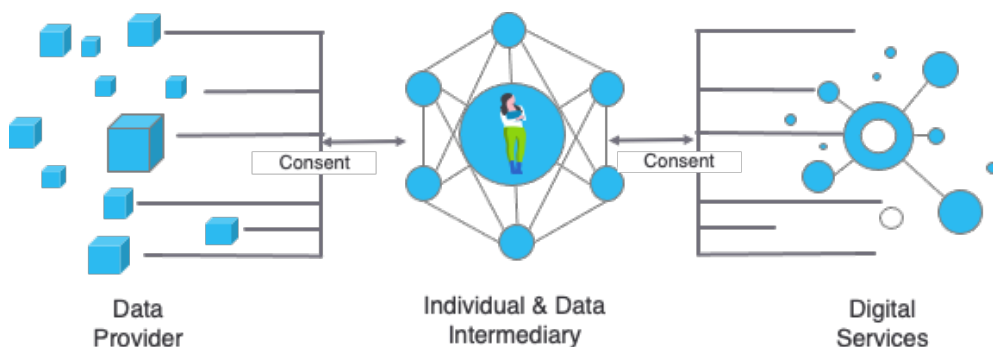
A Worked Example

If Angela has four digital services (e.g. personal financial management, debt management, pension management, wealth management) and requires data from her 4 financial service providers, as data providers (e.g. retail bank provider, loan provider, pension provider, mortgage provider) to enable those digital services, with the Open Banking Architecture this will require Angela to provide 16 individual consents.

If Angela, then wants to share her financial data with one additional digital service (e.g. Insurance dashboard) which requires one additional data source (e.g. Insurance provider) then Angela will need to provide 25 individual consents.

If Angela adds an additional service and an additional data source that then requires 36 consents. Very approximately if there are ' n ' number of actors in the ecosystem (actors being data providers and digital services) then Angela will need to provide n squared consents. In a cross sector market on average an individual has 75 suppliers (data providers) and on average an individual today has 80 apps on their phone, this would require Angela to provide 6000 consents, each requiring initial consent and ongoing management.

Today's Open Banking architecture does not scale for cross-sectorial data transfers and leads to a poor user experience. This will become ever more problematic as the size of the digital services eco-system grows, and therefore will limit its growth. The adoption of a Data Intermediary enabled market architecture largely removes these problems.



Data Intermediary Architecture

In the Data Intermediary market architecture where Angela has 75 data providers and 80 apps she needs to provide and manage only 155 consents, being only 2.6% of that needed in the Open

Banking architecture, this significantly reduces complexity for Angela and significantly increases manageability of the market, reducing risk and costs. With the advent of embedded digital services such as Embedded Finance (e.g. PayPal embedded in a retail customer journey) this may well become even more unmanageable over what could be a short period of time.

2. B2B data transfers

In the Open Banking architecture services are forced to undertake analytics within each digital service, forcing data to be moved to each digital service. At scale such an ecosystem would be creating untenable risks through the aggregation of huge amounts of data in each digital service. Using the Apple Apps as an example of the potential scale of the digital service and therefore the scale of the movement and storage of an individual's data, the Apple App Store has 1.82 million apps.

Such an architecture is also likely to fall foul of reduced lack of consumer trust, by creating multiple honey pots of aggregated consumer data consumers are unlikely to consent to that level of aggregation, this erosion of trust would in turn stifle growth.

With the Data Intermediary model this problem is addressed by enabling the analytics to be done at the intermediary level not requiring the data to be moved or aggregated. This would enable only the consented output of the analytics to be shared with the service provider and the underlying data to be kept secure and private. This appears a likely prerequisite for both consumer trust in the ecosystem and for businesses to manage their own risk/liabilities.

3. Regulatory stifling of innovation

Recreating the Open Banking architecture within each vertical would also stifle innovation caused by the regulatory load on entrepreneur and digital services. e.g. where a digital service requires data from multiple sectors the Open Banking regulatory architecture would require the entrepreneur to be regulated by a large number of regulators. Imagine if a "personal wellbeing" digital service drew on data about an individual's spending (bank), activity (location), social circle (telco), and health data (such services are already being worked on in UK innovation facilities) this approach requires the digital service provider to be simultaneously regulated by the FCA, Ofcom, ICO, CQC, HRA and MHRA. This outcome would significantly stifle not only entrepreneurial initiatives but also HMG initiatives such as that of The Secretary of Health visions for "...a data-driven NHS, and for the UK to become a world leader in healthcare technologies". Health being just one example of the value opportunity, albeit an important one.

The UK stands at a critical juncture, and faces a great risk of misstep by trying to start with the Open Banking market architecture, potentially stifling innovation and creating unmanageable market complexity and risk, and in so doing could undermine UK digital economic growth and that of the broader economy. However, there is a discernible path that offers an opportunity to galvanise UK assets, to retake a leadership position.

About half of Europe's early-stage VC funding flows into the UK and London is well placed as Europe's largest digital hub. Alongside this, the UK's recognised global leadership in Open Banking, and internationally renowned academic, legal and professional services ecosystems, offers considerable potential to forge and commercialise the path to cross-sectorial data sharing faster than our competitors. This will require speed, clear-sighted and determined action from HMG.

The creation of a "UK Digital Trust Framework" as part of our industrial strategy could catalyse innovation in cross-sectorial data. The Trust Framework could represent the evolution of Open Banking to a cross-sectorial data sharing capability, capturing the learnings and assets discovered there, while addressing Open Banking's current architectural weaknesses. To be globally competitive such a Trust Framework would need to be in pilot form in 2022 and fully operational by

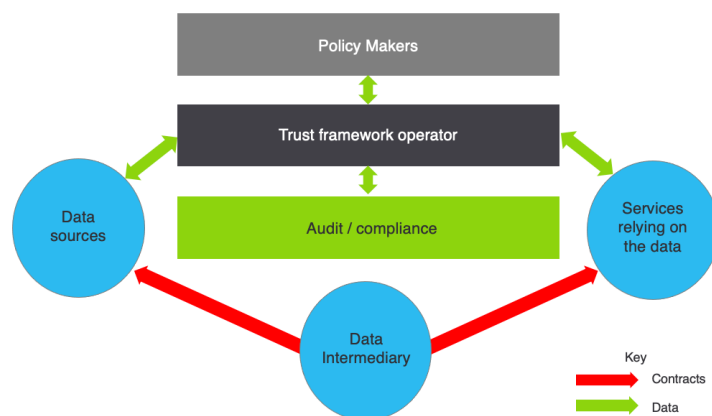
2023. This implies it cannot wait for the OBIE transition period to be completed and could be too onerous a task to ask of an organisation in flux.

The challenge is not just one of timing one but also of mindset. Two hundred years ago the concept of industrial sectors emerged. Over time these evolved Regulators, Trade Bodies and communities. Yet, people's lives are not lived in sectors, they are a construct that we need to break free of (at least in part) if we are to understand and harness the next wave of digital innovation. We need to facilitate an economy where the citizen, customer, person, is at the centre of the services provided for them. Cross-sectorial data enables both better services, new services and all these services to be combined in new ways to deliver the consumers goals.

To enable cross-sectorial data sharing, consumers need to have confidence that their data will not be abused and deliver tangible benefits for them. This is not primarily a technical or regulatory challenge, although both are part of the solution. A number of elements need to come together to create a UK data sharing infrastructure:

1. **Data Access rights:** to enable consumers to access their data in semi-real-time
2. **Technology:** standardised API's, data ontologies, privacy preserving technologies and architectures
3. **Data facilitators:** require a legal basis to act in the interest of consumers
4. **Consent requests:** need standardization
5. **Liability model:** who is accountable when something goes wrong
6. **Compliance model:** Kite mark for consumers and audit to indicate compliance
7. **Governance:** to act as a neutral trust anchor for all parties
8. **Ethics framework:** building on excellence work of CDEI

Together these comprise a "Trust Framework". They are the minimum required to enable the market to create an ecosystem to unlock the benefits of cross-sectorial data sharing. The following provides an example illustrating the different players within a Trust Framework where a Data Intermediary is in play.



Trust Frameworks for Data

The challenge of cross-sectorial data sharing requires the co-operation of many actors, and it is arguably due to a failure of market co-ordination that has to date prevented such an eco-system from arising. This presents a clear need for Government support and facilitation.

Based on the analysis above, we support the creation of a single entity which sets the framework for the sharing of personal data across sectors. Expecting such co-ordination to emerge

organically from interactions between numerous future sectorial entities is very unlikely to produce a timely world leading ecosystem, particularly given the state of international progress and competition in this area. The consequences would be serious for the growth of the UK digital sector and in turn the wider economy.

This raises the question of whether the “Future Entity” created by evolving OBIE would be the right vehicle to be the custodian of the UK’s cross sectorial data strategy development and execution. This seems unlikely for three reasons:

- **The timing is wrong:** The development and execution of the UK’s cross-sectorial data strategy would need to occur while OBIE is in transition to the Future Entity. This is not expected to be complete for another year in UK Finance’s proposals. In this period, we expect competitor trade blocks to have developed their own strategies in detail and passed enabling legislation before the UK is even out of the starting blocks.
- **Open Banking has an architecture which is ill suited to cross-sectorial data sharing:** As described above, the OB approach to consent will not scale to cross-sectorial data. While this could be adapted, it is not realistic to expect organisations who conceived and invested in the existing OB architecture to be fleet-of-foot in recognizing its weaknesses. The risk is that the Future Entity taking on these tasks would lead to a colonial mindset toward other sectors. This is akin to imposing the answer they believe works in one sector to all sectors, without fully recognizing that the exam question has changed, from finance to cross-sector value creation.
- **OBIE has the wrong culture for Cross-sectorial data sharing:** Cross-sectorial data mobility is not primarily a technical task. Consumer consent is critical for success and the key challenges to solve this are around consumer trust. This needs a different perspective to a techno-regulatory world view, additionally it requires a cross sectoral value understanding, managing a wholly different set of stakeholders, business models, value propositions and customer motivations. This culture will be very hard to change in a timescale the UK needs to become world leading in cross-sectorial data sharing.

For these reasons we do not feel OBIE’s successor is a suitable vehicle to act as a consolidation point for Smart Data and Open Finance. An approach which builds a Trust Framework can however accelerate cross-sectorial data sharing and digital innovation in the UK offering a multiplier effect on the UK economy, inward investment, and the UK’s position on the international stage

Question 15: It could be argued that the maintenance and development of payment initiation standards should be dealt with separately from account information and as a scheme. What should be the relationship between the new arrangements and the oversight of payment systems more generally?

Building on our answer to the previous question we see a need for the Account Information Standard to be aligned to a boarder cross-sectorial Trust Framework. Coupling it too strongly to the Payments Standard would seriously impede this. The result would be to balkanise the UK data landscape, carving out Financial data as a silo. This could do immeasurable damage to the UK’s ability to drive growth through data driven innovation.