## Your response

| Question | Your response |
|---|---|
| **Question 1: Respondents are invited to comment on whether they agree with Ofcom's preliminary view and to frame their views and responses with reference to, or in the context of, the statutory criteria in section 106(1A) of the Broadcasting Act 1990 (as amended).** | Confidential? – N<br>Yes. Due to the bewildering complexity across the market and the variety of services available, there does need to be easier methods for individuals and SMEs to access appropriate and timely advice. Modern life and business can be enhanced with the secure sharing of relevant communications data, such that offers have greater relevance, decisions are made more easily and then enacted more swiftly for increased benefit to consumers. |

| | |
|---|---|
| | With the levels of connectivity and data consumption growing exponentially there needs to be greater levels of transparency, convenience and trust across all the services provided to individuals and SMEs. With over 27m broadband subscribers, 84m mobile devices and 8m connected things, the UK population is increasingly dependent on the availability, quality and value received from Service Providers. A measure of dependency is that monthly mobile consumption of data by subscribers grew from 270Mb in 2013 to over 3.6Gb in 2019. Given that 5G will connect a vast array of additional devices, including connected cars, the reliance of individuals and businesses on connectivity will continue to serve the UK economy with billions of pounds of economic value and immense social value, as proven by the demand for connections with work and family during the pandemic in 2020. |
| **Question 2: Is there additional evidence of problems that people and SMEs face when engaging with the market that you would expect Open Communications to help address? Please explain and provide evidence.** | Confidential? – N<br>It's clear that the confusing presentation of tariffs, product data, rates of consumption etc leave consumers bewildered and falling back onto reliance on what they know - their existing service provider. In reality, this is penalising individuals and businesses for their loyalty. In your own analysis this amounts to £1.2 billion pounds per year being overpaid and in the current climate of economic hardship, the subscribers need clarity, transparency, choice and control to make timely decisions about who they take service from, for how long and at what price. |
| **Question 3: Do you agree with our view of the benefits for people and businesses that Open Communications could generate?** | Confidential? – N<br>Yes, only as with Open Banking, there is a danger due to a general lack of enablement in the population that despite the financial benefits on offer from Providers and Third Parties, a lack of advice, education and support will still prevent those that could really benefit from the advantages of smart data analytics will not be reached. As with financial inclusion, the terms of what's on offer in Open Communications based on the sharing of data need greater simplification. |
| **Question 4: Do you agree with our assessment of how Open Communications could enable** | Confidential? – N |

| | |
|---|---|
| **services that benefit people in vulnerable circumstances? Are there other ways it could benefit people in vulnerable circumstances?** | Yes. People in vulnerable circumstances by the very nature of their condition, depend on others daily for support. Their level of dependency is much higher and therefore accessibility and timely advice are paramount to the quality of their lives.<br>With an easier method of securely sharing relevant data for a Third Party to assess, it would also be valuable to look at the aspects of how people in vulnerable circumstances gain access to take advantage of Open Communications.<br>Given the propensity for those in challenging situations to rely on physical help, attention should be given to extending the access model so that carers and nominated family members can be delegated to act on behalf of the subscriber. |
| **Question 5: Are there any risks that we have not identified that could reduce the overall benefits of Open Communications? Please provide evidence, where possible.** | Confidential? – N<br>Most citizens, subscribers and customers think twice before sharing data due to high profile security concerns, data breach and identity theft. The benefits of data portability are clear, but if it's to work at scale for the whole demographic then the use of digital engagement methods has to be delivered with clear, concise and simple advice, enabled by explicit consent such that any consumer can understand what they're signing up to.<br>With such an initiative bringing lots of innovation to how static, personal data is analysed, it could easily by-pass those who would stand to gain most from it as people who are less 'tech savvy' or 'commercially viable' get left behind. |
| **Question 6: Do you agree with the core principles that we have identified for the design of Open Communications?** | Confidential? – N<br>Yes. As a technology provider focused on delivering simple and seamless experiences with robust security and privacy, our recommendation is that a Digital Trust Framework must be defined and be put in place between Service Providers and third-party providers (TPPs) with regulatory oversight. In this context the engagement of ForgeRock is focused on the digital identity requirements of such a Digital Trust Framework. |

Digital identity will have a key role to play in Open Communications, and as such, there needs to be a unified framework to ensure the integrity of each British citizen's digital identity. This is achieved through a trusted ecosystem of providers and technologies. The work being carried out by the Cabinet Office, GDS and OIX will establish a new Identity scheme in 2021 that could deliver the required trust as a foundation for digital engagement.

It is also our recommendation that strong customer authentication be enforced every time a customer accesses or initiates a new service transaction from an online account. Strong customer authentication is defined as the use of multi-factor authentication technology to prove the customer's identity based on something they have, such as a mobile device; something they know, such as the answer to a security question; and something they are, such as a biometric input.

Service Providers have a long history with customer authentication—in fact, its traditional approach can be a disadvantage. Most Service Providers have accumulated a complex matrix of authentication and fraud reduction mechanisms implemented differently on different channels, with separate silos for types of accounts, services, and devices; in-person vs. mobile vs. online; and so on. Built primarily as proprietary technology, these systems are renowned for making it much more difficult to deliver the seamless, unified experiences customers now expect.

For reasons of financial inclusion, security, regulation and international competitiveness, digital identity management is becoming even more important in the UK digital economy. Broadly speaking, the participants in the Open Communications ecosystem will have to be able to provide a seamless and consistent experience across every channel and service that their customers use, building a rich profile based on their activity, preferences, and characteristics across all touchpoints. This is important as Open Communications will intensify competition, ensuring that the service providers and TPPs that deliver the most personalized service will be best able to build strong, enduring customer relationships.

One of the most important challenges to solve is that of customer consent - a core tenet of respecting consumer data privacy. Service Providers must gain explicit customer consent for the execution of transactions, the initiation of new services and for third-party access to data according to the customer’s specifications (e.g. read-only access, or access only to a specific type of transactions), as well as ensuring that data will not be used, accessed, or stored for any purpose other than that requested by the customer.

The principle of informed consent implies that the customer must be able to clearly understand the authorization they are being asked to provide, including:

- who they are providing authorization to;
- what the authorization will permit the third party to do on their behalf;
- how long the authorization will last for.

Customers must have the ability to review this information before, during and after authorization has been granted and to revoke any authorization they have previously granted. They must also have confidence that their data will not be retained by a third party unnecessarily after authorization to access it has expired or been revoked.

Today, many Service Providers lack mechanisms for collecting granular consent, and both regulators and customers will expect much more than pre-populated opt-in checkboxes. To support the development of a consent-based data sharing model, there are a number of established open security standards such as OAuth2, OIDC and User Managed Access, that may be considered as mechanisms for enforcing user consent in an Open Communications context. An example of how the use of OAuth enables an ecosystem of

| | |
|---|---|
| | Open Standards, is User-Managed Access and Consent Receipts and a variety of robust technologies that enable next-generation consent, delegation, and account sharing use cases for customers – for example, giving account access to both internal and external parties.<br>Customer confidence is essential for this endeavour to achieve success and it is built on a number of elements, both tangible and intangible, although clearly security plays an important role. The engagement of consumers using modern methods of authentication, authorization and consent will inspire confidence and thereby increase the likelihood of widespread adoption. Ultimately, for customers, confidence may also link to the question of liability for losses that result from security breaches. This has security implications in that the security measures and standards employed should align with and support the liability model.<br>Open Communications has the potential to create openings for disruptive new business models and competitive opportunities, reduce barriers and increase efficiencies for customers and Service Providers alike. For this to work while minimizing risks, especially when managing highly sensitive personal data, security of the ecosystem and the digital identities that access it is critical. |
| **Question 7: On what kinds of communications providers do you consider that any obligation to provide customer and product data should sit?** | Confidential? – N<br>It is right to initiate the Open Communications ecosystem with a focus on the established Service Providers with considerable market share. These incumbents will offer the greatest level of valuable data for consumers to consent for secure sharing with accredited third parties thereby offering the greatest level of early adoption. Open Communications and the associated rules of participation and standards will have a roadmap for continuing development and as such a future phase must be designed to include service providers with smaller footprints in either the residential or SME markets. |

| | |
|---|---|
| **Question 8: Do you agree with our initial views on how to approach key issues for the design and operation of Open Communications? Do you have comments to make on other implementation issues?** | Confidential? – N<br>Yes. Ofcom's wish to "encourage innovation to enable quick and easy access while maximising the security of customer data" feels a little at odds with the chosen reference to ICO's advice "that authentication process which require users to verify their identity should use elements with which the user is familiar, such as a known password or account number". With a wealth of authentication mechanisms to choose from, such as biometrics and possession factors, as well as the rich contextual information available to make dynamic risk assessments to decide what authentication is appropriate, we would also like see legislation that encourages and does not stifle innovation. We strongly support the view a framework based on open standards supported by a wide range of technology vendors is in the best interests of the consumer as it will result in lower barriers to entry for third party providers and lower cost of implementation to communications providers as well as provide a proven security model. |
| **Question 9: Do you agree with our view of the data that Open Communications should make available to third parties? Is there data about accessibility needs or vulnerable circumstances that people would benefit from being able to share with third parties?** | Confidential? – N<br>Yes. For customers, simpler, more convenient, and more consumer-centric products and services are always priorities. Empowered with unified visibility of their data across all of their accounts and services, people will gain new insight into their spending and consumption patterns to enable better decision-making and a more holistic approach to managing their lives.<br>Instead of struggling to decipher complex pricing models, customers will be able to use digital comparison tools from TPPs to find optimal offers based on their own financial position and behaviours, and even automate account-switching according to rules they set themselves.<br>The possibilities created by Open Communications could benefit consumers and SMEs with new insights that help people and businesses manage their expenditure, access to products they may not have had before and new products that were not previously |

| | |
|---|---|
| | available. Services could be more personalised or tailored to the individual's behaviours and lifestyle, whilst also delivering improved cash-flow management for small and medium enterprises (SMEs). A range of new services will potentially make dealing with the increasing reliance on Communications Services more convenient, simpler and quicker.<br>At the same time, the British consumers and business owners who could potentially gain the most from having access to TPPs enabled by Open Communications, are also those who are the least likely to be able to access them, as a result of factors such as location and disability, for instance. Open Communications needs to be an activity that embraces the full demographic of the British population, so focus must be brought to ensuring that any current types of exclusion as a result of physical barriers are not exacerbated by the increasing benefits that digitally savvy consumers will be able to access.<br>New digital identity frameworks and tools that are trusted across all areas of the digital ecosystem will ensure individuals can prove they are who they are, in a secure and privacy enhancing way when using Services. It will also help businesses, governments, and consumers combat rising rates of cyber fraud and cybercrime, reduce the risk and friction of transacting digitally, and increase trust and safety for citizens. |
| **Question 10: What are your views on the appropriate arrangements for determining liability and redress in disputes between customers, providers and / or third parties?** | Confidential? – N<br>Liabilities are one of the most challenging aspects of data sharing within an ecosystem of service provision involving established providers and new entrants. It makes the use of accreditation as a means of assessing ongoing fitness of service provision an essential function of Open Communications.<br>Annual certification to the regulatory standard, combined with ongoing quality of service assessment will be necessary to maintain the confidence of the public and providers. The exchange of confidential data will be authenticated, authorised and consented in |

| | |
|---|---|
| | such a way as to provide an audit trail to assess the liability of any given party. Combining this with complaints data reporting will deliver on the requirement for greater levels of transparency. Redress for unanswered complaints and issues would be best addressed by an external ombudsman. |
| **Question 11: Do you agree that we have identified the main sources of costs for implementing Open Communications for both providers and services that use Open Communications data? Are there any sources of costs that we have missed?** | Confidential? – N<br>Yes. Our experience of supporting the Open Banking ecosystem between 2016 and today suggests that the sources of costs are well understood here. |
| **Question 12: What factors will drive the overall scale of costs to in-scope communication providers and to third parties? How might this level of cost vary depending on whether providers serve residential and / or business customers?** | Confidential? – N<br>We fully support the view that APIs are the best means to share data and that these APIs should be protected by an open standards-based, OAuth derived authorisation flow. Choice of an open standard means communications service providers and third-party providers being able to use commercial off the shelf products from a broad choice of vendors. With the scale of take-up of the services offered by third party providers not yet known it could be that fixed, rather than usage-based pricing, offered by vendors brings certainty as does a SaaS model that would scale elastically to meet demand. We have observed how investment to meet a regulatory requirement can provide a catalyst for digital transformation and the associated efficiency gains. |
| **Question 13: If relevant, please estimate and describe, as far as possible, the costs to your organisation of implementing and running Open Communications.** | Confidential? – N<br>This question is not relevant as ForgeRock is not a Service Provider.<br>The ForgeRock platform can help Service Providers and third-party providers with a way to bring Open Communications to market quicker, with less risk and at lower cost. |
| **Question 14: If relevant, would your organisation consider using Open Communications data as a third party to offer new services or enhance existing ones?** | Confidential? – N<br>This question is not relevant as ForgeRock is not a third-party provider.<br>We would consider ensuring our platform fully supports the Open Communications standard and position it to Service Providers and TPPs as a way to bring Open Communications to market quicker, with less risk and at lower cost. |