Smarter Contracts

The power of trust

Whitepaper / April 2021

How next generation consent management will help Open Banking thrive in the Age of Privacy

Whitepaper
How next generation consent management will help Open Banking thrive in the Age of Privacy

It has often been stated that consent is “the heartbeat of Open Banking”. It is the very thing that banks and FinTechs need, in order to gain access to the financial data that will help them create personalised products and services that make Open Banking so uniquely innovative and wonderful.

Paradoxically, whilst the success of Open Banking is dependant on society sharing more of its data, the sentiment of society today suggests that this is something they are less willing to do on the scale they have done so in the past.

Growing evidence suggests we have now entered The Age of Privacy, and – in years to come, we believe everyone will look back on 2020 as the moment of its arrival. Society is now demonstrating its discontent over how personal data is being collected, processed and shared, on a scale never seen before.

This whitepaper is aimed at those who are already familiar with Open Banking and those that are somewhat new to it. It explains Smarter Contracts’ view of how ‘next generation’ consent management should work and how Open Banking can enable the introduction of next generation privacy tools that enable customers to have full control over their data, allowing them to manage it in the same way they manage their money.

Introduction

71%

of British consumers would stop doing business with a company if it gave away their sensitive data without their permission (McKinsey 2020)

104.9m

DuckDuckGo searches in a single day, Mon 11th Jan 2021

In 2021 the privacy-based search engine DuckDuckGo registered more than 100 million searches in a single day for the first time in its history. The privacy-enhancing BRAVE browser doubled its number of monthly active users in a single year, from 11.6 million to 25.4 million. Tens of millions more moved over to Signal and Telegram and away from WhatsApp, over alleged concerns that its users had about how their data might be processed and subsequently shared and used. This also contributed to the active Signal customer base growing 40-fold during 2020, and it doubled again in January 2021. In short, Customers are voting with their feet for platforms that are prioritising their privacy.

Businesses should heed a recent study conducted by McKinsey (2020), which found that 71% of consumers would stop doing business with a company if it gave away sensitive data without their permission.

It's easy to see how people's trust has been eroded. Starting with mass internet adoption in the 90s, the evolution of digital has gained not only pace, but breadth and depth. Today, there are few areas of life and commerce that don't feature some aspect of digital technology. It offers convenience, but at a price, with evidence of private data being collected without consent, and subsequently used with little to no regard for its value to the individual or concern about their privacy requirements.

Despite repeated headlines of huge data breaches at some of the world's most trusted brands, people still have very limited options when it comes to changing to more trusted service providers and this is exacerbated by the fact that safeguarding personal data isn't the only concern society has. Stories of deliberate misuse of data, such as the Cambridge Analytica scandal, has further eroded trust in data sharing.

Events like these have led to the emergence of privacy and security-enhancing products and services. As more of these products and services become available, we believe we will see more dissatisfied customers moving over to organisations who can demonstrate their respect for the importance of privacy and the value of trust.

Indeed, as society demands more control over who can access their data, it creates a challenge for Open Data initiatives whose success is predicated on people sharing their data. Without trust or effective controls in place, evidence suggests that less data will be shared, potentially starving these initiatives of the data they need to succeed and thrive.

"Privacy is becoming a reason for consumers to purchase a product, in the same way that organic, free-trade and cruelty-free labels have driven product sales in the past decade."

– Gartner (2020)

Open Banking / Overview

The European revised Payment Services Directive (PSD2) of October 2015 mandated the opening up of banking data to Third Party Providers (TPPs). This made it possible for TPPs to directly access transaction data or create payments on behalf of Customers. It was anticipated that this would drive greater competition in financial markets, and improve outcomes for customers.

In August 2016, the UK Competition and Markets Authority (CMA) mandated that the UK's nine largest retail banks (the 'CMA-9') should fund an organisation that would create common standards and interfaces for PSD2 Open Banking access, and that those banks should implement those standards.

This Open Banking Implementation Entity (OBIE) is close to finalising a set of common open banking standards and maintains a directory of compliant applications so TPPs can rapidly authenticate their application to any Account Servicing Payment Service Provider (ASPSP) or bank.

As of January 2021, over three million customers and businesses were using Open Banking products, an achievement the OBIE and all Open Banking participants should be extremely proud of.

The use of a common Open Banking standard has reduced barriers to entry for TPPs since connectivity to all banks only needs to be implemented once, rather than once for each bank. A small bank can also ensure connectivity with all TPPs by implementing the same standard.

Since the start of 2021, following Britain's exit from the EU, banking regulation in the UK has become the responsibility of the Financial Conduct Authority (FCA), replacing the European Banking Authority (EBA). The FCA rules around PSD2 and Open Banking, launched on January 1st, 2021, essentially replicated those of the EBA. However, some of these rules are now under review in an attempt to drive further growth and engagement in Open Banking.

3m+

No. of Open Banking customers (as of Jan 2021)

Open Banking Consents

All Open Banking activity must be carried out with the explicit consent of the customer, who ultimately owns the data that will be processed. A PSD2 consent is an explicit permission from a customer for an ASPSP to carry out instructions from a TPP: either sharing account or transaction data or processing a payment.

PSD2 consents, in contrast to consents granted under GDPR or ePrivacy regulations, involve three parties: The TPP, the ASPSP and the Customer. The creation of a PSD2 Consent necessarily requires the involvement of all three parties, and any of the three has the right to remove the consent. ASPSPs rights to refuse or revoke consent are limited to cases of suspected fraud.

Consents, like any authorisation, are largely worthless unless the parties involved have authenticated themselves to each other.
The Customer to TPP mutual authentication is outside of the scope of Open Banking, and TPP to ASPSP authentication is well specified and supported by Open Banking.
Customer to ASPSP authentication is more complex. The Open banking specification details the process by which a Customer is passed from TPP to ASPSP for Authentication and back again, but it doesn't specify how authentication should occur at the ASPSP. Strong Customer Authentication (SCA) regulations provide standards that ASPSPs should adhere to for authentication but do not mandate any one particular method.

ASPSP Authentication

SCA regulations require ASPSPs to authenticate Customers using a combination of items that prove their identity. This could be something they have (usually two physical items such as a payment card or utility bill), something they know (a password or PIN), or, increasingly, something that marks them as a real person (biometrics, like fingerprint or facial recognition). This approach provides strong guarantees that a Customer is who they say they are.

The combinations of factors used has been left to individual organisations to define. Electronic logins use a variety of means: Bank Cards, Mobile Devices, Fingerprints, Facial Recognition, Text Messages, Pin Entry Devices, Software and Hardware Code Generators, Voice Calls to telephones, Passwords and PIN codes have been used for authentication, with each organisation using different factors, or in slightly different ways.

In terms of user experience, this ever-changing range of options is a hindrance to moving to other banking providers, as a Customer has to learn to navigate new and unfamiliar authentication processes. This compares unfavourably with other, more standardised, authentication methods such as Chip and PIN, which works consistently across providers.

Inefficient authentication methods, such as those where a customer has to use another device to authenticate, will often cause Customers to give up on what they were trying to do, leaving them with a poor impression of the service. Microsoft's experience of SCA showed, as of December 2020, around 1 in 4 attempts to authenticate with SCA in a browser fail, and 1 in 7 Customers will eventually abandon the effort.

We at Smarter Contracts feel that much can be done to improve the performance of SCA. There are some fantastic examples, such as Apple Pay and Google Pay, where SCA is performed quickly and simply for payment transactions, authenticating a device and either a biometric or passcode. Work to simplify and standardise, from the Customer perspective, the SCA journey will bring great benefits.

1/4

of attempts to authenticate with SCA in a browser fail

90-Day Authentication

These awkward interfaces are a particular problem for Account Information Service Providers (AISPs). Customers can currently only consent for their ASPSPs to share data for 90 days, after which consent must be provided again. The 90-day period seeks to provide a balance. They need to provide long term access to transaction data for some TPPs, such as Accounting Software providers, without inconveniencing customers, and the need to ensure that Customers who are no longer benefiting from a TPP's services are not unnecessarily sharing personal data.

Of course, consent is only meaningful if authentication is carried out first, which forces the Customer to work through the SCA process for all accounts that are shared with each TPP - every 90 days. Some TPPs report drop-offs in Customer numbers at the time of re-authorisation. It is hard to say for certain how much of this is because the customer is no longer engaged with the TPPs service, and how much is an inability to engage with the SCA process.

In response, the FCA has proposed that requirements for re-authorisation with ASPSPs every 90 days should be dropped for transaction information consents. Instead, account information PSD2 consents have indefinite lengths, though the TPP must positively confirm the Customer's continued consent. Where access to payment details is triggered by a customer action at the TPP, the 'Direct Access' case, positive consent is inferred by the customer action.

If the TPP uses 'Indirect Access' to collect data in the background, such as an accounting provider loading transactions daily, they are required to gain explicit consent from the Customer at least every 90 days. If no consent is provided for 90 days, they must terminate the PSD2 authorisation and the customer must once again authenticate with the ASPSP.

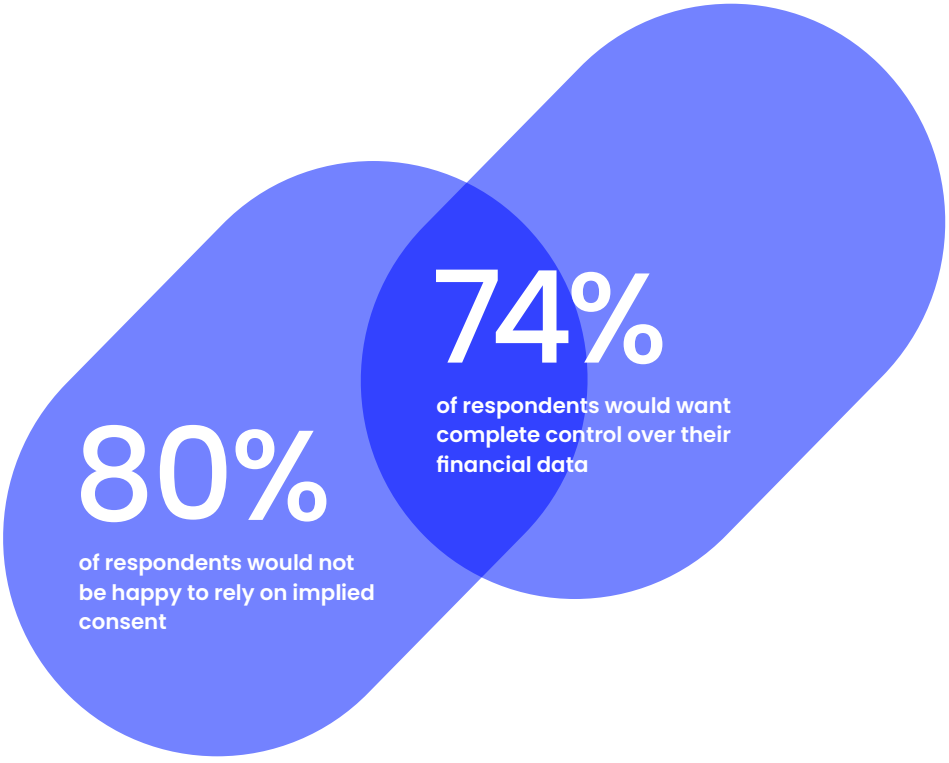
This contrasts with the approach from the EBA, which is pushing national regulators to ensure that ASPSPs remove obstacles, such as inefficient login processes, that would unfairly penalise TPPs, whilst retaining the need for reauthorisation every 90 days. At Smarter Contracts, we believe that care must be taken when adjusting re-authorisation processes to ensure that the existing aims (minimising friction without retaining unengaged customers) are still fulfilled. The proposed changes will look to retain the 90-day window for which a customer can provide consent. This will continue to protect unengaged customers from over sharing data. The exception to the 90-day limit for PSD2 consent applies only to customers that must actively trigger a data sharing request at the TPP. In this case, an active consent applies for each sharing event, and unengaged customers cannot over share data. Further variant proposals that would extend the 90-day window or remove it entirely, could affect customer protection negatively. At Smarter Contracts we believe there are alternatives that can help to achieve both goals.

Moving the consent process from the ASPSP to the TPP maintains the requirement for the customer to provide regular, informed, opt-in consent to data sharing. They can continue to manage and revoke consents at the ASPSP should they wish to. Removing the ASPSP from the re-authorisation journey will reduce customer friction and should improve customer retention for TPPs. The EBA approach of simplifying the SCA process at the ASPSP should achieve a similar goal.

Whilst we do not believe it is being considered, we strongly caution against approaches that would change the nature of re-consent from opt-in to either an opt-out method or attempting to link consent to levels of customer engagement.

In April 2021, Smarter Contracts surveyed 250 UK adults who regularly use a mobile banking app.
When asked about consenting to share their financial data in the future, 74% of respondents stated they would want complete control over their financial data, with only 20% of respondents stating they would be happy to rely on implied consent.

An opt-out method increases the likelihood that customers may unknowingly over-share data, and an implied consent approach is very difficult to regulate. Without a consistent definition of 'engagement' that applies across multiple business models and Open Banking participants, we do not believe that either method will offer customers sufficient control or protection.



“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

Prof. Alan Westin (1967)

Managing Consents

Today, there is no meaningful way for customers to manage all of their Open Banking related consents in one place. They lack the transparency over which ASPSPs and TPPs have access to their data, making it difficult to manage and control. Further to this, there are no effective means to identify or resolve issues when their data is not processed according to their wishes.

Open Banking in the UK continues to grow, and it is something the UK should be extremely proud of given its ever increasing customer base. It has pioneered a blueprint for other countries and regulatory bodies to adopt across the globe and is also being used as the foundation for other Open Data initiatives such as Open Finance and Open Energy.

To further the success of Open Banking, we believe greater privacy products and services will allow the UK to exceed the stated objectives of their Open Banking Consumer Manifesto:

"Open Banking should genuinely equip people with real power to control access to their account and use of their data. People should be able to stop sharing access to their account easily, without facing penalties."

Consent data is currently stored by both ASPSPs and TPPs, and only contains the consent relevant to that particular entity. Where a Customer has relationships with multiple TPPs and ASPSPs, it will be impossible for them to see all of their consents in one place. This is compounded by the need to authenticate with several entities to view and manage subsets of their consents.

If this seems complicated now, with a relatively small number of Open Banking entities, just imagine the Herculean task facing the customer when these other open data initiatives go live, and they are asked to manage their consents across different industries, with even more TPPs.

The 2020 BEIS Smart Data Research Paper on Consent commented: "The Open Banking model in its current form does not provide an appropriate model for the issues and challenges presented with cross sector data sharing".

We agree – and this is one of the reasons why we believe it is critical to re-evaluate the role of data privacy and consent management, while other Open Data initiatives are still in their nascent stages.

Each Open Banking participant currently has its own interface and process for managing consents and with no plans to standardise these dashboards, customers will not be able to control their data easily. Maintaining all accounts with a single ASPSP would simplify things for the customer, however we believe there could be arguments put forward as to why this could be considered anti-competitive and counter to the aim of the CMA, who want to promote competition within Open Banking.

It's a real problem for consents that can be revoked – consents used by AISPs to read transaction data, or long-running payment consents such as Variable Recurring Payments. It is unreasonable to expect a customer to actively keep a personal record of consents with each service provider they interact with.

At Smarter Contracts we believe it's time to introduce 'Data Sovereignty'. In this way, the customer takes control over their data.

The optimal option for Open Banking and future Open Data initiatives; would be to maintain a central registry of all data sharing consents. This registry will allow customers to manage their own consents with their TPPs as easily as with the ASPSPs.

Trust

Banking is an industry built on trust. More specifically, customers trust banks and their regulators to look after their money and financial data.

For Open Banking to be even more successful, customers must be convinced that TPPs will treat their data with care. With a steady stream of stories about data breaches in the news, many might decide that not sharing their financial data with third parties lowers their risk of data or financial loss.

Key to building trust for a customer is the feeling of being in control. Being in control means deciding what data is to be shared, for how long, to whom, for what purpose, and then having the visibility to be able to hold organisations accountable.

Such information should be available in real-time and should be completely transparent to the customer, ensuring that people can quickly and simply disable data sharing when it is no longer appropriate. The antithesis of trust is when Customers feel out of control, if they perceive that third parties are using data that they did not intend to share, or if their data is being used for an unexpected purpose.

A single consent dashboard application, with a simple user experience, is a vital element to creating and maintaining trust and control, especially if it helps users renew or revoke their consents. A customer can provide re-authorisation to the repository directly via the TPP or the ASPSP, and all parties would have a documented record of the re-consent. Far too often, data privacy controls are hidden away on applications and websites. Even when found, they are confusing to navigate. A customer dashboard should visualise the data that is being shared in a way that allows customers to determine if there's a fair exchange of value between them and their chosen TPP.

Shifting the burden of re-consent from ASPSPs to TPPs requires customers to place a greater level of trust in the TPP than is currently the case. This is a new burden on the TPPs and provides a potential for reputational damage not only to a TPP but the industry as a whole if customer data is misused. The customer experience around data privacy and consent management should drive people to engage more with their data. This would raise the expectations on TPPs to behave responsibly as temporary Data Stewards.

Conclusion

Smarter Contracts believe that next generation of Consent will help Open Banking to thrive in the age of data privacy. We believe that an industry-wide consent repository will build the trust and transparency needed to increase engagement in Open Banking in the UK and drive adoption across other open data initiatives in the future. If it is not possible to have a single repository of consent, the Open Banking network should work hard to ensure there is consistency amongst the consent management dashboards that are designed.

Society have made their preferences clear throughout 2020 and shown that there are growing numbers of customers who prioritise privacy and are prepared to change providers who share this core value.

A 2019 YouGov/ODI poll stated that '87% of people say that it is important that the organisation they interact with ethically uses personal data'. For customers to feel confident that organisations are changing their behaviour and acting in accordance with their best interests, then these customers are going to need two things. The first is to have far more transparency over how their data is being used. The second is the ability to control their data in a way that makes it as simple and everyday as they can currently engage with their finances using digital products and services.

We believe that transparency and control are two of the key components most needed to help customers feel more reassured about sharing their financial data. If customers have control over their financial data, they can trust the organisations with whom they share their data with. If customers feel confident that there is a fair exchange of value when consenting to share their data and that their privacy is being respected, then this can only drive Open Banking engagement further. This will ultimately enhance TPPs' ability to access the very data they need in order to offer better, more personalised products and services to Open Banking customers.

Appendix

Page 2
www.mckinsey.com (n.d.). Consumer data protection and privacy | McKinsey. [online] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative. [Accessed 30 April 2021]

DuckDuckGo (2011). DuckDuckGo Traffic. [online] Available at: https://duckduckgo.com/traffic. [Accessed 30 April 2021]

Page 3
www.gartner.com (n.d.). Gartner Predicts for the Future of Privacy 2020. [online] Available at: https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/. [Accessed 30 April 2021]

Page 4
Open Banking (2018). Open Banking. [online] Available at: https://www.openbanking.org.uk/. [Accessed 30 April 2021]

Page 6
www.linkedin.com (n.d.). Dean Jordaan on LinkedIn: Microsoft SCA Scorecard December 2020. [online] Available at: https://www.linkedin.com/posts/deanjordaan_microsoft-sca-scorecard-december-2020-activity-6754842861621116928-Ag-J/ [Accessed 30 April 2021].

Page 9
Reynolds, O.M. and Westin, A.F. (1969). Review of PRIVACY AND FREEDOM. Administrative Law Review, [online] 22(1), pp.101–106. Available at: https://www.jstor.org/stable/40708684?seq=1. [Accessed 30 Apr. 2021]

Page 10
The Finance Innovation Lab (2018). A Consumer Manifesto for Open Banking. [online] Available at: https://financeinnovationlab.org/a-consumer-manifesto-for-open-banking/ [Accessed 30 Apr. 2021].

Page 13
The ODI [online] Available at: https://theodi.org/article/nearly-9-in-10-people-think-its-important-that-organisations-use-personal-data-ethically/ [Accessed 30 Apr. 2021].

About us

Smarter Contracts is a UK-based FinTech company that has designed and built its own patent-pending privacy and consent management platform, Pulse®.

Pulse® has been designed to solve many of the consent-based friction points that have been identified by Open Banking participants in the UK and Europe and further outlined in this whitepaper. By building Pulse® we have created a platform that allows an individual to manage their data in the same way they manage their money. Indeed, our own research clearly demonstrates that consumers want to be able to manage their data in this way and they would be willing to share more of their data if they had access to the type of functionality that Pulse® has been designed to provide.

Pulse® allows for the management of Open Banking consents and authorisations, whilst it has also been built to cover GDPR and ePrivacy consents.

To find out more information about Pulse® and how easy it is to integrate into your current environments, or to learn more about the research we have conducted, please contact:

hello@smartercontracts.co.uk

Smarter Contracts

Smarter Contracts Limited
86-90 Paul Street
3rd Floor
London
EC2A 4NE

smartercontracts.co.uk