

Telephone: 020 7066 9346

Email: [enquiries@fs-cp.org.uk](mailto:enquiries@fs-cp.org.uk)

19 April 2018

## Consumer Panel Position Paper

### Consenting adults? - consumers sharing their financial data

#### Summary

As we move into a new era of financial data sharing, the Consumer Panel has sought to find out what this really means for consumers.

We commissioned a survey of the existing literature, and original consumer [research](#). Participants included both 'tech savvy' people who already use apps that require them to give third party service providers (TPPs) access to their data, as well as people who have not previously consented to share their data.

What we found is not surprising:

- People don't really understand the value of their data
- Even when people read terms and conditions, they are usually none the wiser
- They rely on reviews, or a vague feeling that government and regulators are looking after their interests
- People value privacy, but not as much as speed, when they want goods or services

Terms and conditions are not a useful basis for informed consent. They need a radical overhaul to bring them in line with advances in technology, as the government recognised in its recent consumer green paper<sup>1</sup>. This reform must go with the grain of consumers' clear preference for speed and convenience, and be bolstered by other consumer protection measures, otherwise the potential benefits of data sharing will not be realised and consumers will lose out.

#### Introduction

Open Banking<sup>2</sup> and the European Second Payment Services Directive<sup>3</sup> (PSD2) enable consumers to share access to their bank accounts with TPPs in new, more secure, ways. This is intended to open up the market to innovation and competition. The regulations pave the way for the growth of new services which allow consumers to bring together in one place information from their bank and other financial accounts; and enable people to make payments directly from their bank account without using a debit card.

It is possible to infer a great deal of information about consumers and their values from their payments data. The ability for people to share these data is happening at a time when there are increasing reports of the misuse of consumer data, the most recent being that by Cambridge Analytica of the personal data of millions of Facebook users.

---

<sup>1</sup> Modernising Consumer Markets – Consumer Green Paper, BEIS, April 2018

<sup>2</sup> <https://www.openbanking.org.uk/> Open Banking is intended to increase competition in retail and small business banking by driving innovation in the quality and variety of products and services available

<sup>3</sup> PSD2 builds on the existing Payment Services Directive and aims to bring about better consumer protection, improved security, clarity about liability for unauthorised transactions and data protection. In the UK, PSD2 was implemented by the Payment Services Regulations 2017.

Against the background of Open Banking and PSD2, and continuing examples of the “leakage” of consumer data, the Consumer Panel looked at how consumers of existing services are asked for consent to share their transactional financial data; how people might make more informed choices about sharing those data and whether they are adequately protected when they do share their data.

The Consumer Panel is keen to ensure that when people share their transactional financial data they can do so in an informed way and without being subject to behavioural manipulation.

### **The Consumer Panel’s research**

In late 2017 the Consumer Panel commissioned a team in the Department of Management at the London School of Economics and Political Science to investigate the extent to which existing customers of TPPs understand:

- the concept of ownership of their data;
- the nature of the consent they give to sharing data;
- the impact that the terms and conditions of the service have on their consent; and
- the cost – both implicit and explicit – of the service they use and its value.

The researchers looked at existing academic studies, and conducted qualitative research with 50 individuals who were already allowing a TPP to access their bank account by sharing their log-in credentials, and a larger quantitative study involving over 190 non-TPP users. This examined attitudes to financial data sharing.

### **Findings**

#### ***Consumer consent is not well-informed***

Data protection law, including the General Data Protection Regulation, which comes into force on 25 May 2018, requires consent to be ‘freely given, unambiguous and informed’, but the evidence suggests that this is often not the case.

Speed matters online. This is something that app and service providers are keen to exploit, often in the guise of making the customer journey slicker. Reading and understanding lengthy and complex legal documents has little place in this world. Moreover, these are non-negotiable contracts: users have to accept all the terms and conditions if they want access to the app or service.

Hardly surprising, then, that our research found that most people don’t read in any detail the terms and conditions or privacy notices of the services to which they subscribe. Even when they do, they are none the wiser. Instead, people rely far more on the ‘wisdom of the crowd’: the willingness of others to subscribe to services and reviews on the app store; or the perceived reputation of the service.

Among non-TPP users in our research, most at best skim-read the terms and conditions of online services: 45% said they had not read them, a further 41% said they had only skim-read them. The main reasons why participants did not read the terms and conditions were: text too long (42%); not enough time to read them all (23%); or an assumption that an online service would comply with the law (31%).

Over half of TPP user participants in the qualitative research said they did not read any terms and conditions for products and services that they had signed up for, including services that access their financial data. Many said that privacy policies were full of ‘legal jargon’ and not written with consumers in mind.

While they acknowledged the importance of understanding what they were signing up to, many TPP users had given their consent regardless of what was in

the terms and conditions because they had already decided to use the app or service, so the terms were simply not relevant. A small number of TPP users who had shared their banking security credentials to access a service which relied on the continuous provision of their data were unaware that this is what they had signed up to.

While most non-TPP users said they did not take any extra steps before agreeing to the terms and conditions of an online service, some had read reviews e.g. on the app store – relying on the experience of existing users to highlight potential issues.

Despite most of the research participants from both studies being from higher socio-economic groups and benefiting from higher levels of education, over three-quarters of non-TPP user participants said that they did not feel informed when they had read terms and conditions.

Most TPP user participants did not understand some of the terms and conditions to which they had agreed and more than half of them believed that the consent which they had given was “uninformed”. This is not surprising. Terms and conditions do not generally present in a readily accessible way all the information which a consumer needs to make an informed decision about an app or service. Moreover, the dense legal language means that they can typically only be understood by those with tertiary education-level reading skills.<sup>4, 5</sup> When asked questions about terms and conditions, only a small number of non-TPP users answered correctly after reading them once, and even when given an opportunity to read them again, they still answered poorly.

People giving consent without reading terms and conditions often relied on the regulatory environment, including data protection legislation and financial services oversight, to protect them if problems arose. This was based on the presumption that such protection and oversight was likely to exist in the UK, or a general knowledge about it, rather than any detailed understanding.

### ***People are concerned about their data***

While people generally accept that data sharing is necessary to obtain some products and services<sup>6</sup>, they nonetheless have concerns about ownership and control of the data which they share. The extent to which they *can* exercise control over the use of their data isn't clear to them. Opaque terms and conditions and privacy policies make it difficult for most people to understand how the data they share will be used and shared.

Where financial data are concerned, TPP users were most worried about identity fraud and losing money. However, their perceptions of risk were reduced with increased perception of ease of use, convenience or time saved. There is also some evidence to show that people don't attribute the same value or sensitivity to their financial data as financial institutions or regulators do<sup>7</sup>.

The non-TPP users in our research were concerned about the potential consequences of losing control of their data, that is: it ending up in many different hands; and the risks of security breaches or malicious activity.

---

<sup>4</sup> Joinson, A. N., Reips, U.-D., Buchanan, T., and Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online, *Human-Computer Interaction* 25(1), 1-24

<sup>5</sup> Schaub, F., Balebako, R., and Cranor, L. F. (2017). Designing Effective Privacy Notices and Controls, *IEEE Internet Computing* 21(3), 70-77

<sup>6</sup> European Commission (2015). Special Eurobarometer 431: Data protection, (available at [http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs\\_431\\_en.pdf](http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf))

<sup>7</sup> Brodsky, L., and Oakes, L. (2017). Data sharing and open banking, *McKinsey* (available at <https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking>)

Some TPP users differentiated between personal and financial data, but for others they were both examples of data that were sensitive in view of the risks that could arise if the data were mishandled.

### ***People don't understand the value of their data***

On the whole, people have a poor understanding of the costs of TPPs and whether they receive good value in return for the data they share.

Most people don't understand the value of the data they own, nor do they appreciate the ways in which those data, either alone or in combination with other data, can be used to make money, and what might be the consequences.

Some of the apps and services used by our TPP users were paid-for and some were free. Most people recognised that 'free' services were still being paid for indirectly. They saw the absence of advertisements as a benefit of paid for services, and also thought paying would get them a better service.

In general, TPP users considered that the use of aggregated, anonymised data to improve the services they used or to deliver more targeted advertising was a fair use of data, provided that the advertising was relevant and helpful.

### **Conclusions**

The success of Open Banking and PSD2 relies on two principal mechanisms to protect consumers from harm. The first is the authorisation gateway operated by the Financial Conduct Authority (FCA), or equivalent authority for TPPs from outside the United Kingdom. This should ensure that only reputable firms, which have successfully come through a rigorous authorisation process, can offer Open Banking and PSD2 enabled services. The second is the consumer's explicit and informed consent.

Based on the research evidence, consumer consent is unlikely to protect consumers from harm effectively. It is also unlikely to comply with the GDPR requirement that consent must be informed. Consent cannot be regarded as 'informed' when it is based on long and complex contractual terms and conditions and privacy notices that are frequently not read, and, when they are read, not understood.

The government has signalled its intention to drive simplification of online terms and conditions. That is welcome, but history tells us that, alone, it is unlikely to succeed. Firms write terms and conditions to protect their own interests, not to enlighten consumers. This must be addressed. A radical overhaul should also go with the grain of consumers' strong revealed preference for speed and convenience. Our research shows that, for many people, the terms and conditions are not relevant to their decision. These are non-negotiable contracts; the consumer has no choice if they want the service.

If people can't give informed consent, then they are not being treated fairly. They are giving up their data to get access to a service, but have no way of telling whether this is a good deal or not. The FCA's principles for business<sup>8</sup> govern the fair treatment of customers by those firms it regulates. However, some TPPs will only be regulated under the Payments Services Regulations, and not subject to the principles for business. This puts customers of those providers at a disadvantage.

The research shows that people do not understand the value of their data or the ways in which it can be used by TPPs, either alone or in combination with other data. If TPPs were required to alert people when they intended to pass on, or sell,

---

<sup>8</sup> <https://www.fca.org.uk/about/principles-good-regulation>

their data, with a mechanism to stop that sharing, this might be more effective than burying 'what we may do with your data' in a lengthy privacy statement. It would give consumers more tangible control over their data and would also incentivise firms to think more carefully about the dispersal of consumer data which they hold.

Consumers should also be able to rely on data protection legislation, which will be enhanced when the General Data Protection Regulation comes into force on 25 May 2018. However, in the light of comments made by the Information Commissioner<sup>9</sup>, there is a risk that the Information Commissioner's Office may not be adequately resourced to make these enhanced protections a reality for consumers.

Against this background the Consumer Panel concludes that significant work is needed to inform consumers about the new "data sharing" world heralded by Open Banking and PSD2. People need to understand both the risks and benefits. Regulated data sharing is much more secure than sharing credentials, and a world away from the reported misuse of data we have seen from the recent Facebook/Cambridge Analytica case, and similar reported breaches of trust. It would be a pity if the potential benefits of secure data sharing were lost because consumers did not understand the difference. It will also be necessary to find ways of ensuring that firms that use poor or exploitative practices are effectively excluded from the market, and other steps taken to avoid consumer harm.

### **Recommendation for all stakeholders**

- The FCA, Government, Law Society, industry and other interested parties should work together to find an alternative to lengthy and complex terms and conditions for specifying contracts in a technology-driven era. This must facilitate consumers' genuine, informed consent. The development of an alternative should also properly take account of consumers' behavioural biases, and overcome the current defensive nature of terms and conditions.

### **Recommendations for the FCA**

- The regulation of TPPs must keep pace with technological advances. The FCA should use 'RegTech' to enable effective supervision of firms making use of consumers' payments data, and set expectations about what is and is not acceptable.
- The FCA should introduce a requirement on all firms using consumers' payments data to have ethics committees to oversee the governance, use and sharing of that data.
- The FCA should test possible mechanisms by which TPPs could tell consumers in real time when they plan to share, or sell, their data, and give them the opportunity to stop the sharing.
- The FCA should require all firms to demonstrate to consumers their legitimacy in a way which is simple, reliable and trustworthy, so that fraud is kept to a minimum. The FCA should also ensure the robustness of the authorisations process and improve the quality and accessibility of the information on the FCA register<sup>10</sup>.
- The FCA should consult on extending its principles for businesses<sup>11</sup> to TPPs, which are currently only regulated under the Payment Services Regulations.

---

<sup>9</sup> <https://www.ft.com/content/01641ac6-9081-11e7-a9e6-11d2f0ebb7f0>

<sup>10</sup> [https://www.fs-cp.org.uk/sites/default/files/fscp\\_response\\_approach\\_to\\_authorisation.docx\\_.pdf](https://www.fs-cp.org.uk/sites/default/files/fscp_response_approach_to_authorisation.docx_.pdf)

<sup>11</sup> <https://www.fca.org.uk/about/principles-good-regulation>

- The FCA's forthcoming consultation on a duty of care for financial services firms should set out explicitly how TPPs should be required to act in consumers' best interests, with a view to avoiding potential harm<sup>12</sup>.

### **Recommendation for the Money Advice Service**

- The Money Advice Service (or its successor, the Single Financial Guidance Body) should lead a communications campaign to inform consumers about data sharing in the world of Open Banking and PSD2. This should differentiate between data sharing under Open Banking and the access consumers give to their data – often unintentionally – via social media or other online activity.

### **Recommendations for government**

- The government should ramp up the resources and capabilities of the Information Commissioner's Office to ensure the effective supervision and enforcement of the General Data Protection Regulation and introduce a Data Ombudsman Service to improve consumers' access to individual redress.
- The UK Data Protection Bill currently before Parliament should be amended to enable independent consumer organisations acting in the public interest to bring collective action on behalf of consumers affected by a data breach.
- To ensure consumer interests in data are properly represented, the government should appoint consumer representatives to the new Centre for Data Ethics and Innovation, established to build public confidence and maximise the potential of Artificial Intelligence and data.
- The government should support the proposed Money Advice Service communications campaign.

The Consumer Panel welcomes feedback on this position paper and the underlying research.

Please send any comments to [enquiries@fs-cp.org.uk](mailto:enquiries@fs-cp.org.uk)

---

<sup>12</sup> [https://hansard.parliament.uk/Commons/2018-02-06/debates/61057de8-769c-4609-a83a-0903fd00946e/FinancialGuidanceAndClaimsBill\(Lords\)\(ThirdSitting\)](https://hansard.parliament.uk/Commons/2018-02-06/debates/61057de8-769c-4609-a83a-0903fd00946e/FinancialGuidanceAndClaimsBill(Lords)(ThirdSitting))