Report on a study of how consumers currently consent to share their financial data with a third party.

The report is provided for the Financial Services Consumer Panel with the aim that it will help to ensure that consumers will be able give consent to share financial data with a third party in an informed way

Dr Edgar A. Whitley and Dr Roser Pujadas

Department of Management

London School of Economics and Political Science

London

March 2018

Research team

Lorena Carrasco

Alexandra Gencheva

Shaffra Gray–Read

Rovik Robert

Zahra Shah

Mario Washington–Ihieme

Kar Yee Yip

Executive summary

Introduction

The launch of Open Banking on 13 January 2018 means that the UK's largest account providers will be making it possible for customers to make the most of their financial data and easily and securely access services from a wide range of companies that better meet their needs. In the context of Open Banking, consent provides the main legal basis by which third–parties may process the financial data of customers. That is, open banking services can process personal data because the customer has given consent for their personal data to be used by the relevant online service. According to the forthcoming General Data Protection Regulation (GDPR) consent must be unambiguous, informed and feely given. Data subjects (consumers) also have the right to refuse, or revoke, consent at any time. In addition, GDPR strengthens the legal rights of consumers in relation to data ownership and the rights of data subjects to access their data. Nevertheless, despite such legal requirements, "informed consent" and data protection more generally raise many practical challenges that are examined in the research.

The report presents the results of a research study undertaken for the Financial Services Consumer Panel (FSCP) by a team in the Department of Management at the London School of Economics and Political Science. The research investigates the means by which consumer consent to sharing financial data can be given in a more informed way that is not subject to, or minimizes, behavioural manipulation. The research combined a mixture of quantitative and qualitative empirical research alongside academic style desk research. As this research was conducted in advance of the launch of Open Banking, the study focused on customers of current Third–Party Providers (TPPs) including Account Information Service Providers (AISPs).

Questions

In commissioning this research, the FSCP was particularly keen to better understand four key questions:

a. The concept of consumers "owning their own data";

b. The type of consent they have given to the Account Information Service Providers (AISPs) to make use of their data;

c. The terms and conditions of the service they have signed up to (with regard to the consent they have given); and

d. The 'cost'—implicit and explicit—of the service and whether this represents good value for money / data.

Key dimensions affecting consent

The desk research identified three key dimensions that can affect informed consent:

- provider practices including how terms and conditions and privacy policies are presented (length, clarity, relevance, etc.) as well as measures to optimise the customer experience.
- individual behaviour including customer perceptions of benefits and risks associated with sharing data, the extent to which privacy policies are read and understood as well as individual privacy attitudes etc.
- social context in which it happens including (knowledge of and expectations of) the regulatory environment and accepted norms and practices etc.

Empirical findings

The empirical part of the research drew on interviews and focus groups with 50 individuals who were already allowing a third–party to have access to their bank account and a large quantitative study of over 190 participants that examined their experiences with existing consent mechanisms as well as attitudes to financial data sharing.

How do consumers understand the concept of "owning their own data"?

The empirical evidence highlights the challenging nature of this concept. For some contributors personal data and financial data were very different, with different levels of risk associated with each. For others they were all examples of data that were sensitive in light of the risks that would arise if the data were mishandled.

Further complications arose around whether the data are shared with, or just accessible to, the third–party provider. Data that are shared, some felt, became even more uncontrollable. This ambiguity about ownership is heightened for contributors who hadn't fully appreciated the implications of the terms and conditions they had agreed to.

What types of consent do consumers give to third–party providers to make use of their data?

The evidence from the empirical research suggests that consent is frequently neither freely given, nor unambiguous nor fully informed. Over half of the contributors claimed not to read any terms and conditions for products and services that they sign up for, including the specific services that access their financial data. Similarly, only a small proportion of participants correctly answered a question about a detail in the policy even after having an opportunity to re–read the policy in a research setting.

In the absence of an ability or willingness to consent to the processing described in the privacy policy, many contributors drew on alternative support when assessing whether or not to provide consent. For some, this would involve detailed research into the operation of the service and might also include trials with less critical bank accounts. Others would rely on proxy assurances such as adverts, reviews on app stores or the recommendations of friends and colleagues.

For some, consent would be given regardless of what was specified in the terms and conditions because they had already decided to use the app or service. A final approach was to give consent and simply rely on assumptions about the regulatory environment, including data protection and financial services oversight, if problems arose.

How well do consumers understand and appreciate the terms and conditions of the service they have signed up and given consent for?

Given the poor comprehension of terms and conditions it is perhaps unsurprising that during the interviews, few research contributors fully appreciated the consequences of what they had signed up to, including some who believed that they hadn't even given consent for that data sharing to take place.

In terms of additional uses of personal and financial data there was a general acceptance, or resignation, that, as customers, they would likely be subject to personalised marketing messages and associated online tracking. There was far less understanding of other things the service provider might do with their data, including data aggregation and profiling.

How do customers understand the implicit and explicit costs of the services they are using and do they think this represents good value for money / data?

Some of the apps and services used by the research contributors were paid for services, whilst others were offered for free. There was a general recognition that services that were not paid for directly were still being paid for indirectly, typically through targeted marketing and data aggregation etc. Few fully appreciated the risks that can arise from data aggregation, for example, in terms of price discrimination or sub–optimal recommendations.

Acknowledgements

The project team would like to acknowledge the assistance of Lars Wicke, Leo Beattie, Seth Lutsic, Jane Ellison and Peter Broekema.

Table of Contents

List of Figures

List of Tables

1 Introducing the study

This report describes a research study undertaken for the Financial Services Consumer Panel (FSCP) by a team in the Department of Management at the London School of Economics and Political Science. The research study investigated questions of data governance and security in the context of consumers giving consent to third–party apps and services allowing them to access their financial transactional data in advance of the launch of Open Banking in January 2018.

The FSCP is keen to draw on the research results with the goal of ensuring that when consumers consent to share their financial data with a third–party in relation to Open Banking they are able to do so in an informed way and without being subject to unnecessary behavioural manipulation.

The panel is specifically interested in finding out the extent to which customers understand:

a. The concept of consumers "owning their own data";

b. The type of consent they have given to the Account Information Service Providers (AISPs) to make use of their data;

c. The terms and conditions of the service they have signed up to (with regard to the consent they have given); and

d. The 'cost'—implicit and explicit—of the service and whether this represents good value for money / data.

2 Introducing Open Banking

The launch of Open Banking on 13 January 2018 means that the UK's largest account providers will be making it possible for customers to make the most of their financial data and easily and securely access services from a wide range of companies that better meet their needs. Open Banking is a term that describes "a secure set of technologies and standards that allow customers to give companies other than their bank or building society permission to securely access their accounts" (Open Banking Implementation Entity 2018).

The technological infrastructure that Open Banking enables is explicitly intended to address both concerns about the level of competition between the nine largest UK banks as well as financial services reforms from the European Union, specifically the second Payment Services Directive (PSD2) (Manthorpe 2017). Open Banking extends the role of application programme interfaces (APIs) from PSD2 to enable customers to use services from a range of different types of regulated companies without the need to share credentials with any third–parties, as the APIs provide secure, two–way, access to the accounts held by the banks.

Many commentators are suggesting that the use of APIs to access and manage financial data heralds a significant digital transformation of financial services as well as a new way of dealing with personal data as a valuable and scarce resource (Birch 2017; Manthorpe 2017; Zachariadis and Ozcan 2017). Open Banking is therefore the latest feature of a rapidly transforming digital landscape which some have described as embodying a new logic of accumulation (Zuboff 2015). This new logic helps produce new markets of behavioural prediction and modification by extracting value from personal data.

That is, whilst the aggregation, analysis, monitoring, recommendation, automation and payment request tools (Lindley 2014; Reynolds 2017) offered by Open Banking might transform the customer experience by increasing innovation and competition they may also exacerbate information asymmetries, create conflicts of interest or worsen problems of financial exclusion (Connington and Murray 2018; Hickey 2018; Morley 2018; Reynolds 2017; Rudgard 2018). Customers may also have concerns about the integrity of the API access provided by Open Banking as well as the efficacy of the Open Banking Consent Model (Open Banking Implementation Entity 2017) or the clarity of the terms and conditions / privacy policies of the various Open Banking services.

For example, a recent post in an online financial discussion forum highlighted the importance and value of personal data associated with financial transactions:

> *These free apps are just data miners*. They will monetise the data they hold on you by sharing with anyone who cares to pay. The next logical step is targeted advertising, anything from savings accounts to Insurance policies. If you are wary of your bank being hacked, imagine a database that has all of

> your bank, credit card and savings accounts, along with your spending patterns, being hacked. (MSE Forum 2017a emphasis added).

Another poster queried the business model underlying another service:

> Voluntarily giving away my financial privacy for the sake of a 3% interest rate? Are you having a laugh? *Data is the new oil*. This app is a Trojan horse to access your data, whilst pushing the sweeteners it offers with no reference to its main agenda. *This company will never disclose exactly what they are doing with your data, nor how valuable it is to them*. Until you are sure about how they will exploit your data, do not agree to it. Protect your privacy. We have very little left. It is not worth it. The house always wins. (MSE Forum 2017b emphasis added).

Other posters highlighted potential security concerns associated with allowing third–party apps to access your bank account:

> The problem with these third–party services is one of them will be hacked. It's not a question of if, but a question of when. *That puts every single account you own at some sort of risk*. I really don't think the risk is worth the reward of seeing all your accounts in one place. I don't really see the benefit in it either. Most people who are operating several accounts will have their own way of organizing it all, why should they suddenly now need a third–party to do this for them? (MSE Forum 2017c emphasis added)

Issues of access to the appropriate technology were also raised:

> I don't have a smart phone so I guess I couldn't opt–in even if I wanted to (Davidson 2017 Comment following article).

3 The legal requirements for processing personal data

In the UK, data protection law requires that the service provider ("data controller") who is processing data about a customer ("data subject") must satisfy specific conditions for the data processing to be considered lawful, such as the case of processing financial data for Open Banking services. A data controller might request another person (other than an employee of the data controller) to process the data on behalf of the data controller. This person is known as the "data processor" (Information Commissioner's Office 2018a).

The potential conditions for processing data include processing that is necessary in relation to a contract between the data subject and the data controller, processing that arises because it is necessary to protect the data subject's vital interests (typically matters of life or death), processing required for administering justice, processing that is in accordance with the "legitimate interests" condition (Information Commissioner's Office 2017) in the Data Protection Act or processing that takes place because the data subject has given their consent to the processing.

In the context of Open Banking, consent provides the main legal basis by which (Third–Party Providers) TPPs may process the financial data of customers. That is, open banking services can process personal data because the customer has given their consent for the personal data to be used by the relevant online service (Bechmann 2014; Curren and Kaye 2010).

Open Banking uses consent as the basis for processing data because it aims to "put the customer in control of their finances" (2018). Open Banking has tested and implemented a sophisticated consent–based model whereby a customer needs to give consent to the third–party provider to allow them to approach their Account Servicing Payment Service Provider (ASPSP) to gain access to the customer's account details via an API (Open Banking Implementation Entity 2017).

Further steps in the customer experience include authentication with the ASPSP and authorisation which confirms that the ASPSP may respond to a request from the third–party provider to whom the customer has given consent.

4 Unpacking the concept of "consent"

Despite the role that consent–based processing of personal data places on individual autonomy and agency (Whitley 2009), defining what is meant by "informed consent" raises many practical challenges (EU 2011) and has been subject to much discussion and reflection.

The EU Article 29 Working Party, which is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission, has published a detailed review working on a definition of consent within European data protection law (EU 2011). The review clarifies, for example, the meaning of unambiguous consent by suggesting that only consent that is based on statements or actions to signify agreement constitutes valid consent.

One implication of the analysis presented by the Article 29 Working Party is that relying on consent given via pre–ticked boxes would not constitute valid consent as it is not based on an explicit action (choosing to tick a box) and instead relies on the fact that most people don't bother to untick a box. Previously, therefore, companies were able to claim that they had consent to process data even though the consent was ambiguous and may have been obtained through the manipulation of behavioural norms.

Consent also needs to be "informed" and this relies both on data controllers providing suitably clear information about what processing they intend to do with the personal data provided, and data subjects reading and understanding this information, typically found in the service's terms and conditions or privacy notice.

A recent example nicely illustrates these concerns with current consent practices. The popular unroll.me service, which is presented as providing an easy, automated unsubscribe service for managing email inboxes, was also selling aggregated data to Uber about the health of its rival Lyft by analysing the number of Lyft receipts unroll.me service users had in their email inboxes (Biddle 2017).

The company's 2000+ word "plain English" privacy policy includes the statement that the company "may collect and use your commercial transactional messages and associated data to build anonymous market research products and services with trusted business partners" (unroll.me 2016). However, as the company CEO noted, "Sure we have a Terms of Service Agreement and a plain–English Privacy Policy that our users agree they have read and understand before they even sign up, but *the reality is most of us*—myself included—*don't take the time to thoroughly review them*" (Hedaya 2017 emphasis added).

This example would suggest that it is unlikely that customers were giving truly informed consent for the processing of their personal data nor that they were unambiguously giving consent both to the primary (unsubscribe) service and the secondary data analysis for the additional, anonymous market research products and services.

These kinds of concerns about whether consents that are given are truly informed (Bechmann 2014) or are "engineered" rather than freely given (Kerr et al. 2009) echo the broader concerns of the FSCP about the extent to which Open Banking customers might be subject to unnecessary behavioural manipulation.

Some authors even question whether a consent model makes any sense in an era of large scale data processing (Cate et al. 2013) and challenge the underlying assumptions that policy objectives are addressed by offering consumers "notice and choice" before they make their decisions (Barocas and Nissenbaum 2009; Solove 2013).

5 General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) that comes into force on 25 May 2018 can best be understood as an update to the EU Data Protection Directive (EU 1995). It seeks to harmonise further data protection within Europe and introduces a series of additional measures including increased fines for serious breaches of the regulation, clearer guidance about notifications of data breaches and a limited right to erasure of personal data. The GDPR also introduces a new organisational role, namely the data protection officer and mandates the use of data protection impact assessments when new types of processing are introduced.

The UK Data Protection Bill (2018) is a related piece of legislation that localises key aspects of the GDPR but also puts in place legislation ready for when the UK leaves the EU following BREXIT.

5.1 Consent under GDPR

The GDPR takes the Article 29 recommendations and provides greater clarity (and higher requirements) on the use of consent as a basis for processing personal data than is found in earlier legislation. In particular, a key feature of consent under GDPR is that data subjects should give "unambiguous" consent and they should be "informed" about the forms of processing they have given consent to, both in terms of the potential benefits of the processing of their data and the risks associated with doing so (Whitley and Kanellopoulou 2010).

In relation to the conditions for processing personal data, the regulation states that the consent of the data subject means:

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (EU 2016, pt. Art 4(11))

It also states that where data is used for multiple purposes, consent must be explicitly obtained for all purposes (EU 2016, pt. 32).

Article 7 of the GDPR requires that where consent "is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" (EU 2016, pt. art 7(2)).

Alongside concerns about ensuring that data subjects are properly informed about the consent they are giving, the regulation also highlights the importance of data subjects having a genuine choice as to whether to consent or not. This suggests that in situations where it is not meaningful for customers to have a real choice then another legal basis for processing the personal data should be used. For example, personal data processing may be justified as "necessary for the performance of a

contract" that the data subject is a party to or "necessary for compliance with a legal obligation to which the controller is subject" (EU 2016, pt. 6(1)). In these situations, asking for consent is inappropriate.

5.2 The reach of "informed" consent

The GDPR emphasizes the need for organisations to be clear about the data processing that they intend to undertake as well as the expectation that the data subject giving consent for the processing clearly understands what they are consenting to.

> The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. … That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing (EU 2016, pt. 60).

5.3 Revocation of consent

Choice in this context also means giving the data subject the opportunity to refuse, or revoke, consent without detriment (EU 2016, pt. 42; Information Commissioner's Office 2018b). This echoes the use of informed consent in many forms of research (Hoeyer 2009). This is a stronger, and more explicit, articulation of the withdrawal of consent than is found under the UK Data Protection Act and other data protection laws (Curren and Kaye 2010; Kerr et al. 2009).

6 Informed consent in practice

Although informed consent forms a key part of the legal requirements for processing personal data under the data protection regulations including the forthcoming GDPR, the FSCP is interested in learning more about informed consent in practice, specifically the types of consent customers have given to Account Information Service Providers (AISPs) and other Third–Party Providers (TPPs) to make use of their data and the terms and conditions of the service they have signed up to. In order to obtain the maximum insights from the empirical studies, it is helpful to begin by reviewing the academic literature around the practice of giving informed consent.

Most existing empirical studies have found that consent giving is seen as a practice that is, for the most part, a tedious exercise. Individuals who consent to services processing their personal data often do so ineffectively, unaware of what it is they have explicitly consented to (Schaub 2017). This arises from all aspects of the practices for sharing and interpreting the information about what is being consented to, i.e. the content and presentation of privacy notices and terms and conditions, the interpretation of and attitudes to the available information in the privacy notice and other aspects of the customer experience.

6.1 Privacy notices and informed consent

One study found that if people were to read privacy notices, policies and terms and conditions word for word on every website they visited, it would take them 201 hours annually (McDonald and Cranor 2008). Other studies suggest that even if read, they can only be understood by those with college–level reading skills (Joinson et al. 2010; Schaub et al. 2017).

Assessing the quality and usefulness of the content of privacy notices is further complicated by the natural tendency for individuals to present themselves in socially acceptable ways. One consequence is that they may often claim to be well informed about the content of the terms and conditions of services they are using, claiming to have spent time reading the privacy policy of the service, when, in practice they may not have read or understood the documentation at all.

According to one EU study only 18% of people claim to have read privacy policies fully, with this statistic being 13% for the UK specifically. Only 20% of EU citizens in the study felt they are always informed about data collection and the ways data are used (European Commission 2015). In the UK the study reports that this number is up to 27%, with 47% claiming they are sometimes informed. Of the EU citizen respondents who said they do not read privacy policies many respondents said they found them too long to read (67%) or too difficult to understand (38%).

Between 70% and 75% of individuals in research studies report disagreeing with the idea that privacy policies are easy to understand and thus need to make an effort

when reading them to be able to understand them (Moores 2005; Turow et al. 2005). Consumers often express frustration with vague statements that aim to cover a range of information that a service is providing, without explicitly stating the information that will be collected, how it will be used and with whom it will be shared (Solove 2013). Reports of individuals subsequently failing to register online because of the incoherent nature of the privacy policy statement have also been highlighted.

This has led Bechmann (2014) to put forward the suggestion of an emerging "non–informed consent culture", the idea that consent giving to online services with regards to social media, relies on group processes. As a consequence the likelihood of one consenting to use an online service is contingent upon social forces and the reputation of the service rather than being an intentional act of human agency—a service might appear more acceptable if many people use it (van Lieshout 2014). This also reflects tendencies of first wave adopters of any technology to pave the way for others.

Steeves (2009) also questions the current notion of privacy—considered as informational control—and suggests reconceptualising it in an intersubjective social context. Here privacy is a social construction that we create as we negotiate our relationships with others on a daily basis. As such, Steeves sees this working–definition of privacy as something that "reinvigorates our ability to question—and limit—the negative impact of surveillance on our social and democratic relationships" (Steeves 2009, p. 193).

Evidence by Awad and Krishnan (2006) indicates that information transparency does not deter consumers from wanting to share their personal information with online services. This is supported by recent evidence by Karwatzki et al. (2017) who also found that alternative features such as the personalisation of online services, and importantly, the extent to which one values their privacy, have a major impact on the decision for a consumer to disclose their information. Similarly, research by Tsai et al. (2011) provides some evidence that customers may be more likely to make purchases from online websites when provided with salient privacy policy information.

6.2 Behavioural constraints on decision making

Several pieces of academic research have concluded that policymakers and protectors of consumer rights need to be better at adopting accurate models of users' agency and resulting behaviour into the formulation of both policy and technology (Acquisti and Grossklags 2004, p. 176; Kerr et al. 2009). Evidence from the social science literature demonstrates that the ability to make informed decisions is hindered by a variety of factors meaning that individuals often click through presentations of a service's terms and conditions in order to obtain the immediate benefits that arise from using an app or service (Whitley 2009).

One approach to understanding this phenomenon is through consideration of bounded rationality. This research stream suggests that people are not fully and completely rational—in that they are working with limited time and limited

cognitive resources—and therefore are inclined to make bounded decisions, ones that are not objectively the most rational (Jolls et al. 1998). For example, behavioural research shows that people tend to value short–term rewards over long–term goals, when they are faced with a decision (Kahneman 2012).

A Princeton study found that emotional and rational parts of the brain compete for control when a person tries to balance near–term rewards with long–term goals. The study concluded that impulsive choices or preferences of immediate rewards were a result of the emotional part of the brain winning over the logical reasoning (McClure et al. 2004).

Scientific studies also tell us that the brain's emotional side responds positively to instant gratification and this side sees increased activity the closer someone is to obtaining a reward. Moreover, businesses and governments understand the existence of cognitive fallibilities and tendencies of human behaviour and have recognised soft approaches to engineering consent while maintaining an illusion of completely "free choice" (Kerr et al. 2009).

Research also shows how such decision biases and behavioural tendencies can be used to either nudge people toward consent or to dissuade people from acting fully on their privacy rights (Kerr et al. 2009; Thaler and Sunstein 2008). These influences may play a part in the way customers view their data at the point of choosing to engage in a third–party service or product.

As well as immediacy biases in decision making there are other behavioural factors that affect customer perceptions of their data. People tend to have greater sensitivity to losses than to gains (known as loss aversion) (Thaler et al. 1997). Research also shows that people value what they own higher than what they do not own, known as the endowment effect (Thaler et al. 1997).

These behavioural influences also apply to the case of withdrawing consent. Not only are people not likely to revise consent already given, they are also unable to recognise that they are likely to behave in this way (Kerr et al. 2009). This can be explained by decision theory, with subjective utility (the personal value of an outcome) changing over time. This theory suggests that gains and losses are perceived as less bad or good, respectively, if the person knows they are to be experienced in the future than in the present (Loewenstein and Elster 1992). Research has also shown that the rate of this decrease is higher for gains than for losses (Ortendahl and Fries 2002). This means that a customer considering their initial consent to sharing their data is likely to value the immediate gain higher than the theoretical loss of privacy, potential security issues or other unknown (or not understood) implications, in the future (Kerr et al. 2009).

The reverse situation, of revoking consent, heightens this tension. The immediate loss of the service or product is likely to be perceived as being more significant than a gain in the future.

In other situations, the process of giving consent may arise after the basic decision to use a service has already, effectively, been made. For example, Heimer (2012) presents a case of consent processes in the context of a HIV clinic noting that

many research participants may agree to participate in clinical trials because they have no other way to secure treatment. She continues "People arrive at the point of being 'consented' having already made a considerable investment in research participation. … In these instances, informed consent procedures may give people a last chance to change their minds or different reasons to do what they had already decided to do" (2012, p. 23).

6.3 Optimising the customer experience

It is widely understood, and easily observable, that speed matters where our online and digital journeys are considered. This is reflected in the way digital giants and companies in all industries that serve customers online strive to enhance the customer experience—not least because it affects the bottom line. Technology giants like Google, Amazon and Facebook are constantly looking for ways to optimise, and capitalise on, the digital experience investigating how to reduce user frictions such as pop–ups, delays and other irritations.

Research has shown that a delay of as little as 100 milliseconds leads to a 7% drop in transaction completion and a two second delay leads to a 103% increase in abandonment rate on a website. At the same time 53% of mobile device users will leave a web page if it takes longer than three seconds to open (Akamai 2017; Doubleclick 2016).

Delays in the online experience affect the long–term relationship and trust built with customers (Schrage 2016) and can result in loss of profit and unaccomplished business objectives, as well as the inability to make use of user and traffic data analytics (Doubleclick 2016; Facebook Business 2016). Banks are having to compete with other industry disruptors, such as financial technology companies and challenger banks, for customer acquisition and retention, with the new battlefield being the digital customer experience. Customer journeys, especially more complex ones such as getting a mortgage or financial advice, need to be designed and delivered in a seamless, straightforward way.

Complexity caused by multiple touch–points, regulatory compliance and multiple interests increases the prospect for interruptions and friction in the customer journey, which may result in higher drop–off rates (Finextra Research 2017). In fact, according to a report on trends in the retail banking sector, a seamless digital experience and smooth flow that reflects consumer preferences will lead to "improved satisfaction, loyalty and referral scores" (Digital Banking Report 2016).

However, in the context of new services such as Open Banking, there is an argument for adding additional delays to enable a more informed and thoughtful consent process to take place.

Taking this into account research conducted by Ipsos Mori for the Open Banking Implementation Entity showed how consumers see these delays, i.e. positive friction, specifically within the context of AISP. It reviewed the role of "positive frictions" in the form of a three–step consent model, where the final Authorisation step actually

serves as a final mental pause for customers to review the data they are agreeing to share and what they are consenting to.

The Ipsos Mori research also found that when discussing the effects of "positive friction" and whether it helped customers be more thoughtful about the consent they were giving, most interviewees mentioned the fact that if they are at the consent stage they have already thought about what they are doing. In addition, minor delays in the journey would not result in them abandoning the journey, as they felt they would not be going through the process and effort had they not already wanted the product or service, echoing Heimer's point presented earlier.

In the study, the early adopters suggested that the reason for not abandoning the journey when faced with positive frictions was that they felt they made a choice to be there—they would have been informed, felt comfortable enough and didn't feel they needed the extra step of Authorisation.

The research results have been used to inform the drafting of the Consent Model Guidelines (Open Banking Implementation Entity 2017), which provides a non–binding consistent best practice standard to implement the consent model within the OBIE interpretation of the relevant regulation.

6.4 Summary

Taken together, these academic studies highlight a range of concerns that can affect the decision as to whether to give consent for data processing to take place, such as whether to sign up for Open Banking services that will process financial data. There is evidence that privacy notices and terms and conditions are often difficult to read and understand. They may not present all the information that an individual would need to make truly informed decisions about the consents they want to give. Moreover, there is growing evidence that behavioural constraints influence decisions, with perceived short–term benefits often influencing consent decisions more than the details of the processing being consented to. Finally, attempts by service providers to optimise the customer experience by avoiding unnecessary delays and other frictions can further influence the practice of giving informed consent. These elements are explored further in the empirical research.

7 Individual factors affecting the consent process

The content of privacy notices and the design of the customer experience, coupled with behavioural constraints can all affect decision making around giving consent to share personal data. The literature also suggests a range of individual factors that can affect the consent process, specifically individual privacy attitudes as well as individual risk appetites and other aspects of how personal data is valued. This literature provides a useful background for two more key questions for the FSCP: how consumers understand the concept of "owning their own data" and their appreciation of the 'cost'—implicit and explicit—of the services they are using and the extent to which they believe this represents good value for money. The literature on these questions is explored in this section to inform the design of the empirical research.

7.1 Privacy attitudes

At an individual level, the evaluation of the benefits and risks of disclosing privacy information is dependent on how much an individual values their privacy (Westin 1967). Academic research has developed this concept into a measurable personality attribute, whereby it is claimed that those who value their privacy more (with high privacy valuation scores) are more likely to perceive the risks of disclosing their personal information online, compared to those who value their privacy less (those with low privacy valuation scores) (Karwatzki et al. 2017). Research has also focused on age differences with suggestions of a generational shift of privacy concerns, with the assumption that the younger generations, who grew up during the technological boom, care less about privacy (Nussbaum 2004; Solove 2013) although this has been countered by Hoofnagle et al. (2010) with evidence of young and old adults possessing similar privacy concerns and beliefs about how companies should deal with their data.

Privacy attitudes are also used to help explain the privacy paradox, whereby espoused attitudes to privacy differ from actual behaviours (Acquisti and Grossklags 2004; Carey and Burkell 2009; Preibusch 2015). The evidence in this area is inconclusive, suggesting the extremely contextual nature of privacy concerns (Nissenbaum 2011), with important distinctions between different types of data and organisations (Carey and Burkell 2009) as well as possible changed attitudes following the Snowden revelations (Davies 2014; Pew Research Center 2014).

Choosing to share personal information with an online company is also dependent on the relationships between the discloser and the recipient. If an individual is clear about how their information will be used, then a level of trust for the online service will be gained (Joinson et al. 2010; Karwatzki et al. 2017). This is supported by research which finds that privacy concerns and the effect of the intention to share personal information was mediated by trust (Malhotra et al. 2004; Metzger 2004).

7.2 Understanding the value of personal data

Within the Open Banking ecosystem, different categories of data warrant different levels of security and permissions, which customers often don't understand (Brodsky and Oakes 2017). Where financial data is concerned, customers normally cite identity fraud and loss of money as key concerns. However, most people do not have a comprehensive view of the data they own or understand its value (van Lieshout 2014). They also often don't appreciate the ways in which it can be used or combined with other data to make money (Zuboff 2015) and what the consequences of this could be. There is also some evidence that shows that consumers don't attribute the same value or sensitivity to their data as financial institutions or regulators do (Brodsky and Oakes 2017).

Research shows that people who seek and prefer convenience are more likely to sign up to a service or feature if it simplifies their experience (Hann et al. 2007). This debate has extended from similar discussions in the context of social media (Hutchinson 2015) and the Internet of Things (Salmon 2016) with the trade–off between privacy and convenience. Convenience, time– and money–saving aspects of e–banking are also seen as positive features of e–banking, increasing the uptake of e–banking services. At the same time, however, research has found that where supplying personal information was a prerequisite, concern for privacy was increased and may inhibit the adoption of such e–banking services (Kolodinsky et al. 2004).

The uptake, use and consumer choice of e–payment services has also been found to be affected by some design attributes (physical control feature, information transfer method, acceptability of payment method) in the way that they reduce different perceived risks (financial–, privacy– and time–risk) (See-To and Ho 2016). In other words, perception of risk is reduced with increased perception of ease of use, convenience or time saved, which positively affects the adoption of this type of e–payment service.

The same study also found that while convenience and saving time are positive factors these are not of higher importance to people than "the method of transfer of information" (See-To and Ho 2016). In practice, this showed that people did not prefer to enter and send over personal information in a browser, as it felt riskier. In fact in the early phases of online banking solutions, security and privacy concerns played a part in the reluctance for initial uptake of those solutions (Nienaber et al. 2014).

7.3 Summary

This literature suggests a range of further factors that need to be explored in the empirical studies, namely the extent to which individual privacy attitudes and the valuation of personal data are presented as reasons for using or not using Open Banking style apps and services.

8 Environmental factors affecting the use of financial services apps

Some broader environmental factors, particularly the broader regulatory environment may also affect the extent to which individuals will chose to engage with Open Banking at all and the extent to which customers feel that they are being treated fairly and are confident that any grievances they may have will be properly addressed. In many cases, these considerations about the broader regulatory environment may come before decisions about which particular app or service to use and give consent to.

8.1 The regulatory environment

An important element of customer trust is provided by the regulatory environment within which data processing activities take place. This includes the existence of appropriate data protection laws coupled with effective, independent oversight (Greenleaf 2012) and a well–functioning legal system. In the context of Open Banking, the regulatory environment also includes the Financial Conduct Authority (FCA) (Hickey 2018).

The regulatory environment is particularly important in the context of the role of competition in driving Open Banking. A competitive environment, by definition, is likely to have organisations that are successful as well as those that are less successful and may leave the marketplace. The regulatory environment, and the support it provides for customers who have used one of the less successful organisations in the market, is likely to be a key factor influencing customer decisions to engage with Open Banking[1].

For ordinary citizens, the regulatory environment is something in the background and is simply "ready–to–hand" and available (Heidegger 1937; Winograd and Flores 1986) rather than something that is "present–at–hand" and the focus of explicit consideration. Just as an individual doesn't notice their glasses whilst they are wearing them, items that are ready–to–hand typically only reveal their characteristics in the event of a "breakdown" where their unavailability or unsuitability reveal key characteristics, such as when the glasses are lost or broken.

The perceived effectiveness of this combined regulatory environment can help explain current attitudes to sharing data with third–parties in advance of the launch of Open Banking. Research from Accenture in October 2017 found that 69% of British consumers would not want to share their bank account information with third–party providers. In fact, more than half said they will never change their existing banking habits and adopt Open Banking (Accenture 2017).

[1] We are grateful to Katie Evans, Head of Research and Policy at Money and Mental Health for highlighting this connection.

Whilst this low level of interest can be partly explained by the novelty of the Open Banking proposition, concerns about fraud, data protection risks and potential cyber–attacks were also cited as the top obstacles for people adopting Open Banking, by 85%, 74% and 69% of consumers respectively. These sentiments are reflected more widely than just the UK and apply beyond Open Banking, suggesting a level of ambivalence around the perceived effectiveness of individual organisations and the regulatory environment when it comes to looking after personal data.

The most recent EU–wide Eurobarometer (2015) commissioned by the European Commission on EU citizens' perceptions and attitudes to data privacy, shows that 71% agree that "providing personal information is an increasing part of modern life". Notably, 68% also believe there is "no alternative other than to provide it if they want to obtain products of services" (European Commission 2015). Smith (2018) develops the notion of digital doxa to recognise the ways in which digital data—and the devices and platforms that stage data—"have come to be perceived in Western societies as normal, necessary and enabling".

However, 67% of respondents to the EU survey are concerned about not having complete control over the information they provide online and 55% are concerned about the recording of their activities via payment cards and via mobile phones (European Commission 2015).

Other important findings from the EU citizens research, pertinent to this study are:

- Roughly seven out of ten people are concerned about their information being used for a different purpose from the one it was collected for;
- Almost all Europeans say they would want to be informed should their data ever be lost or stolen;
- Two–thirds of people think the public authority or private company handling the data should be the ones to inform them if it has been lost or stolen;
- More than 80% do not feel they have complete control over their personal data; and
- 69% of British respondents feel they can trust banks and financial institutions to protect their personal data (the average for the EU was 56%) (European Commission 2015).

The GDPR explicitly seeks to address a number of these concerns, for example about data breach notification and purpose limitation. However, the extent of likely GDPR compliance is unclear and evidence of compliance and enforcement of existing data protection regulations can inform customers about the role of GDPR in affecting decisions to use Open Banking.

8.2 GDPR compliance

GDPR enters into application on 25 May 2018 and, formally, all organisations are required to comply with the new regulation from that point. In practice, however, it

is unclear whether all organisations will be fully compliant on day one, raising further concerns about the effectiveness of the regulatory environment (cf Hill 2018).

Moreover, previous studies, relating to the EU Data Protection Directive, demonstrate a clear gap between EU legal theory on data protection and actual practice by e-commerce services in the UK (Borghi et al. 2013).

For example, of the top 200 UK websites studied in the research by Borghi et al. (2013) over 54% do not indicate whether they will notify the data subject in case their privacy policy changes and 19%"do not specify whether data subjects will be given options to update their personal data" (Borghi et al. 2013) even though these are key obligations under the Data Protection Directive. The same study found that 69% of websites specifically seek consent for direct marketing. Yet most of these do not comply with obtaining unambiguous consent as set by the EU Data Protection Directive (Borghi et al. 2013). While this is one study and pertains to an earlier version of data protection law it is worth recognising that organisations may fall short of full compliance with the GDPR as well.

There is certainly a lot of attention from organisations in all industries about complying with the GDPR, however with less than three months to go companies are largely concerned about being ready in time or risking big fines (Hunt 2017). Another study showed that 46% of small to medium sized business owners in the UK had not even heard of GDPR (Aldemore Bank 2017) and 38% of UK cyber security specialists have said that the May 2018 GDPR deadline is not seen as a priority by their organisation (Hunt 2017). A report for the Department for Digital, Culture, Media & Sport in 2018 reports that only 38% of businesses and 44% of charities as having heard of the General Data Protection Regulation with only a quarter of these having implemented changes in response to the GDPR's introduction (DDCMS 2018).

The outlook appears to be a little more positive in the financial service sector. While only 8% of UK companies are fully prepared to meet GDPR compliance, financial service companies are leading in this progress, according to a November 2017 PWC survey (Hayer 2017).

8.3 Summary

The final set of issues to be explored in the empirical work relate to the extent to which users and potential users of Open Banking services know about and appreciate the support available to them from the broader regulatory environment for Open Banking. This includes knowledge of existing data protection regulations, including the forthcoming GDPR and financial regulations and oversight.

9 Introducing the empirical research

Sections 4 and 6 presented a summary of the key insights from the mainstream academic literature around the role of consent for processing personal data as will be the case in Open Banking. The review highlighted the complexity of the notion of consent, particularly in the context of GDPR. It identified concerns about how well suited privacy policies and terms and conditions are for making customers aware of how their personal data will be processed. The review also emphasised the role of behavioural constraints on how customers make decisions about using Open Banking services or giving consent to share data, even in situations where they might be fully informed.

These themes raised a series of additional constraints around the consent process including the extent to which individual privacy attitudes affect behaviour, the role of the regulatory environment for supporting customers as well as the extent to which companies will be GDPR compliant in the coming months and how this will influence trust in Open Banking and data handling more generally.

The literature review also presented research findings that are, at best, ambiguous and, at times, contradictory, suggesting important methodological challenges associated with existing empirical research. These include rapidly changing contexts that might limit the applicability and generalisability of existing research findings. For example, it is unclear to what extent findings about trust in early e–commerce websites still apply in an era of smart phones, online banking and apps. Equally, the effects of the financial crash and the Snowden revelations about government surveillance alongside an increasing appreciation of the business models of the internet giants might shift attitudes about regulation and trust from those reported in earlier research.

The empirical research undertaken in this study draws on this existing literature and presents timely findings of users (and non–users) of apps that can have access to financial data, in advance of the launch of Open Banking. The study finds evidence to help address the questions set by the FSCP around the concepts of ownership and value of personal (financial) data as well as the types and understanding of consent given for services.

9.1 Research design

The research was led by two Principal Investigators from the LSE, Dr Edgar A. Whitley and Dr Roser Pujadas, supported by a team of seven research officers who were a mix of recent and current MSc students.

The research combined a mixture of quantitative and qualitative empirical research alongside academic style desk research. The overall goal was to better understand the means by which consumer consent to sharing financial data can be given in a more informed way that is not subject to / minimises behavioural manipulation.

The launch of Open Banking will involve the use of application programme interfaces to access and manage financial data by third–parties. As this research was conducted in advance of the implementation of Open Banking, the study focused on current Third–Party Providers (TPPs)—specifically Account Information Service Providers (AISPs). These existing third–party providers typically do not have API access, but instead rely on "screen scraping" to collate and aggregate customer transaction data from their accounts.

Screen scraping is enabled by the customer sharing their username and password with the third–party provider and the provider logging into their online account and "scraping" transaction data from the bank account. Screen scraping therefore introduces higher risks to customers around the use of financial data when compared to the specific access to data via carefully specified application programme interfaces found in Open Banking.

Based on the original research brief, the team identified four high level research areas and a further six sub–areas that guided the research process, see Table 1.

RA1	How people are currently asked to consent to share their financial transactional data with TPPs?
RA2	Identification of best practice about asking for consent
RA2A	How might individuals share financial data in an informed way?
RA2B	How might individuals share financial data without being subject to behavioural manipulation?
RA3	Suggested areas for improvement to help people make more informed choices about sharing their data
RA3A	Extent to which consumers understand the concept of owning their data
RA3B	Extent to which customers understand the type of consent they have given to AISPs to make use of their data
RA3C	Extent to which customers understand the terms and conditions of the service they have signed up to
RA3D	Extent to which customers understand the cost - implicit and explicit of the service and whether this represents good value for money / data
RA4	Gaps in the current regulatory framework that leave people unprotected

Table 1 Initial research areas and questions

The project itself was then broken into five distinct studies that sought to address the different research areas. The bulk of the research was undertaken in studies 2 and 3 which focussed on the contributions from individuals who were already using some form of Third–Party Provider.

Study 1 was a large scale, quantitative study that drew on the LSE Behavioural Research Laboratory (BRL) Participant Pool. Participants in Study 1 were explicitly screened to ensure that they were not users of existing TPP apps and services.

Studies 4 and 5 involved desk research. The full range of studies is presented in Table 2.

Study 1: Survey	Large scale, quantitative study of participants' experiences with existing consent mechanisms as well as attitudes to financial data sharing
Study 2: Interviews	Qualitative research with existing TPP customers (i.e. research contributors who have already given consent to TPPs to access their financial data)
Study 3: Focus groups	
Study 4: Desk research	Privacy policies: Transparency and accessibility
Study 5: Desk research	Treating customers fairly

Table 2 Study descriptions

Combining the research areas with the studies highlights the interactions between the studies and the research areas, see Table 3.

		Study 1	**Study 2 & 3**	**Study 4**	**Study 5**
RA1	*How people are currently asked to consent to share their financial transactional data with TPPs*		√	√	
RA2	Identification of best practice about asking for consent	√	√	√	√
RA2A	How might individuals share financial data in an informed way	√	√		
RA2B	How might individuals share financial data without being subject to behavioural manipulation	√	√	√	√
RA3	Suggested areas for improvement to help people make more informed choices about sharing their data	√	√		√

RA3A	Extent to which consumers understand the concept of owning their data	√	√		√
RA3B	*Extent to which customers understand the type of consent they have given to AISPs to make use of their data*		√		
RA3C	*Extent to which customers understand the terms and conditions of the service they have signed up to*		√		
RA3D	*Extent to which customers understand the cost - implicit and explicit of the service and whether this represents good value for money / data*		√		√
RA4	Gaps in the current regulatory framework that leave people unprotected			√	√

Table 3 Research areas (italics: AISP customer specific research questions)

9.2 Research participants and contributors

Participants for study 1 and contributors to studies 2 and 3 were recruited from a variety of sources including the LSE Behavioural Research Lab participant pool, advertising the research on various LSE social media networks (including the Department of Management Linkedin, Facebook and Twitter feeds) as well as the social networks of the researchers. Further participants were identified via facilitated introductions from two AISPs (MoneyHub and Money Dashboard), posts to the Money Saving Expert Discussion Forums (with the permission of the MSE Forum Team) and personal contacts. In total, there were 241 research subjects, see Table 4.

More details on the methodology and characteristics of participants are provided in the appendix, but it is worth mentioning that, overall, the research participants and contributors were predominantly educated to, at least, a degree level. In addition, contributors to studies 2 & 3 can be all considered early adopters of Open Banking style apps and services and several of them studied or worked in the financial or technology sectors.

Nevertheless, despite these characteristics that differentiate them from the overall population, the research highlighted that even this educated and well–informed group had a limited understanding of how financial data might be used or the meaning of privacy policies and terms and conditions they had consented to.

Study 1: Survey	206 signed up for the study	191 participants
Study 2: Interviews	39 research contributors	50 contributors

Study 3: Focus groups	Two focus groups (3 and 8 research contributors)	using 13 different apps and services
Study 4: Desk research	Privacy policies (4 Credit Bureaus, 4 Accountancy services, 2 Affordability Check services, 3 Personal Financial Apps, 2 Personalised Price Comparison companies, 3 Personal Data Store companies, 1 Marketing company)	19 third–party providers
Study 5: Desk research	Treating customers fairly	N/A

Table 4 Study participants, contributors and cases

10 Empirical findings: Content analysis of privacy notices

Customer behaviour is dependent on both the information that is available to them in the form of privacy notices etc. and on the ways in which customers engage with, understand and act on this information. The presentation of the empirical findings therefore begins with results from Study 4 which involved a content analysis of the privacy policies and terms and conditions of 19 third–party providers. The analysis examined the extent to which these policies and notices explained existing legal rights that customers have. It also examined the extent to which additional information was presented about technological factors such as cookies, international data transfers and retention policies.

Study 4 found considerable variability in the level of information provided to customers in the privacy policies studied. This included differing detail about how customers can exercise their existing legal rights as well as technological details such as where the data is hosted and processed. The policies also have differing amounts of detail about the role of cookies and communication opt–outs. Some also include additional information about, for example, the form of encryption used by the service. Customers may find this kind of information helpful in making choices about which services to use. The findings are discussed in more detail below.

10.1 Presentation of existing legal rights

Existing data protection laws provide customers with a range of legal rights, for example, in relation to how the organisation handles international data transfers, how long it retains personal data from closed accounts or how it may send marketing communications to customers.

In terms of other existing legal obligations under data protection law, a large proportion of the privacy notices studied (79%) detailed how data subjects could exercise their subject access rights (i.e. obtain a copy of all data held about them). More than half of the companies studied (53%) failed to specify whether data subjects have the right to request the erasure of any personal information they hold about them when they no longer require their services. Only 21% of companies failed to indicate whether data subjects have the right to rectify any inaccurate information about them.

The organisations studied were generally poor at providing clear information about who their nominated subcontractors or affiliated service providers were that would be processing personal data outside of the EEA, another requirement found in current data protection law and the GDPR.

In terms of data transfers, Study 4 found that fewer than half of the companies (42%) explicitly assured that personal data will only be transferred to third countries which guarantee an adequate level of data protection. In some cases, data subjects were informed that transfer agreement mechanisms would be used while exporting their personal data to a third country outside of the European Union or the European Economic Area (EEA), see Table 5:

EU–U.S. Privacy Shield Framework (4 TPPs)
Swiss–U.S. Privacy Shield Framework (1 TPP)
Asia–Pacific Economic Cooperation (APEC) Privacy Framework (1 TPP)
Standard Contractual Clauses (EU Directive 95/46/EC) (1 TPP)
Australian Privacy Act (1 TPP)
Contract in place (2 TPPs)

Table 5 Transfer agreements mechanisms for exporting personal data outside EEA

The remaining TPPs either kept the data within Europe or failed to specify the legal basis for international data transfers. In addition, a significant proportion of companies (68%) indicated that they transferred personal data outside of the EEA for processing or use in accordance with their privacy policies, but did not specify the legal basis for doing so.

In terms of data retention, a significant number of companies in Study 4 (63%) specified their retention policy in their privacy notices. This was particularly noticeable where the retention of some personal data was required to comply with legal obligations or was reasonably necessary for reconciliation purposes and internal reporting.

Only a small minority (10%) of organisations explicitly stated that personal data would be promptly deleted from their systems and that the organisation would no longer have any access to data once it had been deleted by the data subject. Additionally, the vast majority of organisations failed to provide any detail as to what would happen with inactive, rather than deleted, accounts.

10.2 Presentation of technological details

Given the technological underpinnings of Open Banking, some potential users might be interested in technological details of the offered services that provides information that goes beyond an articulation of existing legal rights.

More than half of the companies studied (58%) failed to specify the security and technical mechanisms used in handling personal information. Only two–fifths of companies (42%) were clear about the security measures taken against unauthorised access, loss or damage. The security features for providing data confidentiality found in the policies are presented in Table 6.

Security and Technical Mechanisms	**Percentage of Companies**
Use of encryption (Total)	42%
Industry Standard SSL with 128-bit encryption	10%
Industry Standard SSL with 256-bit encryption	5%

Extended Validation SSL Certificate with 256-bit encryption	5%
Use of read–only application	16%
Use of cryptosystem	5%
Security partners	10%
24/7 security guard presence	10%
Use of disaster recovery and risk management	5%
Use of threat modelling and attack scenarios	5%
Use of Direct Payments Solutions Limited	5%
Use of Master Password	5%
Use of Trusted Device authentication	5%
Use of biometric authentication	10%
Zero–knowledge account recovery	5%
Use of web application and Next-Generation firewalls	5%

Table 6 Security features mentioned in privacy notices

More than half of the companies (58%) indicated that they store user information on secure servers, but only 10% of them clearly specified the location of the storage server and with whom (third–party data hosting provider) they host their services.

A small minority of companies stated that they utilise third–party data hosting providers such as Amazon Web Services (10%), Rackspace (5%) and Microsoft Azure (5%) to host their services. These service providers typically offer hosting services based within Europe as well as globally. International hosting of data potentially raises privacy concerns (Whitley et al. 2013), particularly in relation to the failure of Safe Harbour provisions and challenges to its replacement, Privacy Shield (Orlowski 2015, 2017) which seek to specify where data can be hosted and still satisfy EU data protection requirements.

10.2.1 Cookies

The use of cookies was discussed by eighteen of the contributors in studies 2 and 3 and typically reflected an attitude to data cleanliness, whereby cookies would be deleted at the end of a session to "cover my tracks" [Contributor 11, male, App05B

User[2]] and limit the amount of tracking and to prevent unwanted targeted advertising.

Study 4 found that despite the prominence of cookie notices, these notices tended to be fairly general. In the context of cookies gathering non–personal information, this lack of detail about the focus, use and lifetime of the cookies used might be intentional as, according to Alcorn et al. (2014), knowing the specific kinds of cookies used is often advantageous to hackers when attempting an attack on user sessions. As the lifetime of cookies and the values of session timeouts determine how long a user can maintain access, attack intruders can take advantage of the publicly available information to implement an attack on an active session. This attack is called "Cookie Hijacking".

Thus, whilst some details about cookies might be sensibly left off a privacy notice, most organisations were generally vague about the effects on the service provided if users were to turn certain cookies off. For example, what services would users miss out on if they were to turn off those cookies?

More than half of the companies (58%) failed to inform data subjects of the use of cookies throughout their websites. Typically a pop–up message would appear on their home page and would then be hidden. Exemplary cookie notices also exist, see for example Figure 1.

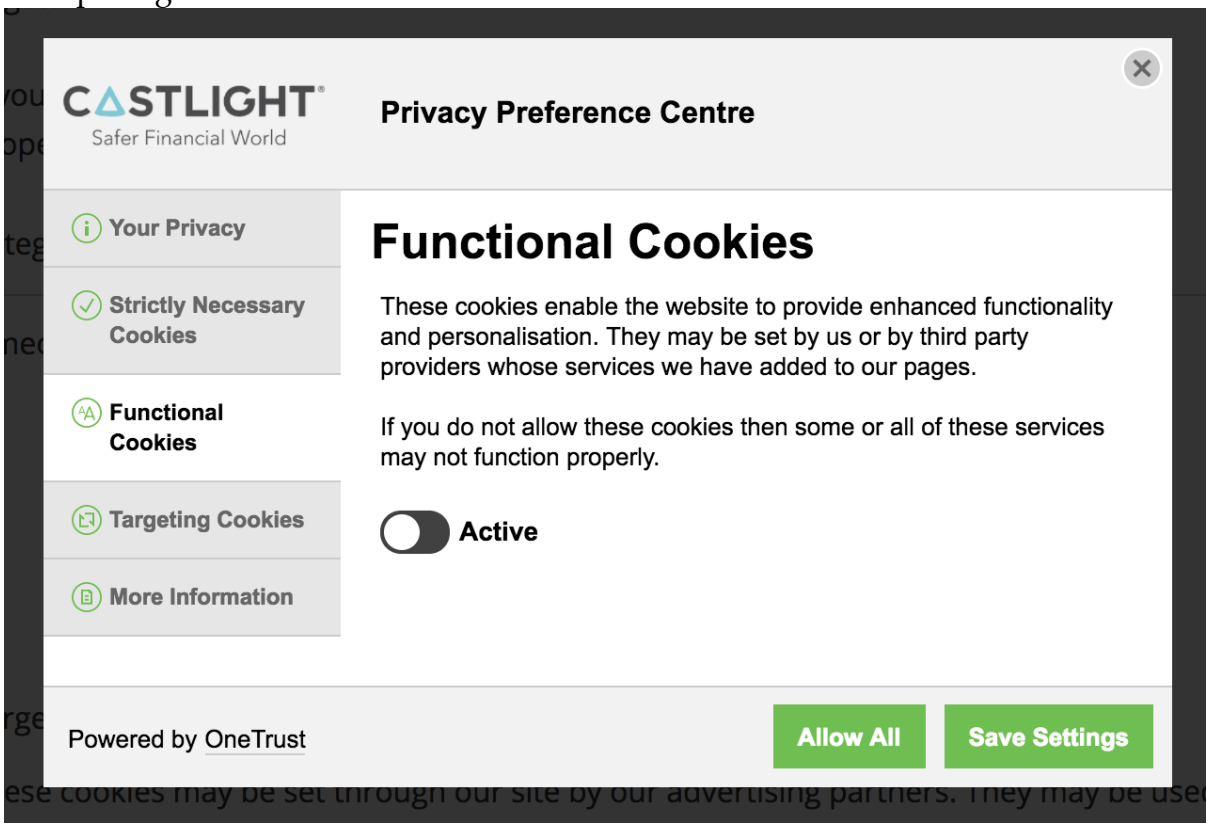

Figure 1 Cookies on Castlight

[2] All apps and services are disguised in the report. App codes ending B were budget / spending tracker apps, F offered financial / banking services, K offered book keeping services and S supported savings.

Additionally, only 26% of companies provided specific instructions on how to manage, reject or delete cookies on data subjects' browsers, not least because the steps to follow are different for different browsers, see for example Figure 2 and Figure 3 .

5.3	If you do wish to stop your browser from accepting cookies, see the following pages:
5.3.1	Mozilla Firefox: http://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences
5.3.2	Google Chrome: https://support.google.com/chrome/bin/answer.py?hl=en&answer=95647&p=cpn_cookies
5.3.3	Internet Explorer: http://windows.microsoft.com/en-us/windows-vista/block-or-allow-cookies
5.3.4	Safari: http://support.apple.com/kb/PH5042

Figure 2 ClearScore - to how disable cookies https://www.clearscore.com/privacy-policy

Browser	PC	Mac
Internet Explorer	• Choose **Tools** • Select **Internet Options** • Click the **Privacy tab** • Use the slider to choose your preferred settings	• Choose **Preferences** from Explorer menu • Select **Receiving Files** options • Select **Cookies** • Use the slider to choose your preferred settings
Mozilla Firefox	• Choose **Preferences** from the Edit menu • Select **Privacy & Security** • Then select **Cookies** • Choose your preferred settings	• Choose **Preferences** from the Edit menu • Select **Privacy & Security** • Then select **Cookies** • Choose your preferred settings
Chrome	• Click the Chrome **Menu** icon • Select **Settings** • Click **Show advanced settings** • Click **Content settings** in the **Privacy** section • Select **Allow local data to be set** to allow both first-party and third-party cookies. To only accept first-party cookies, check the box next to **Block all third-party cookies without exception**	• Click the Chrome **Menu** icon • Select **Settings** • Click **Show advanced settings** • Click **Content settings** in the **Privacy** section • Select **Allow local data to be set** to allow both first-party and third-party cookies. To only accept first-party cookies, check the box next to **Block all third-party cookies without exception**
Safari	• Choose **Preferences** from the Safari menu • Select **Security** icon • Cookie settings are shown in window • Choose your preferred settings	• Choose **Preferences** from the Safari menu • Select **Security** icon • Cookie settings are shown in window • Choose your preferred settings

Figure 3 GoCompare - how to manage cookies http://www.gocompare.com/about/cookie-policy/managing-cookies/

10.2.2 Communication opt–outs

Alongside giving consent to share personal data, most of the services examined in Study 4 also collect consent around the choice of communications channels that might be used by service provider. This is currently regulated by the Privacy and Electronic Communications Regulations (2003) rather than the Data Protection Act

(Information Commissioner's Office 2015). In general, customers are given the option to refuse consent to particular forms of marketing communications although a small minority of companies (10%) failed to indicate the availability for opting out on any communication while using their service. The opt–out option is available in the following communications in the companies studied, see Table 7:

Type of Communication	**Percentage of Companies**
Newsletter	10%
Marketing	68%
Billing information	5%
Service updates and notifications	16%
Information on new products or features	10%
Request participation in market surveys	16%
The use of personal information	5%
The processing of Usage Data from users' browsers and websites visited	5%
The use of location feature on users' App to target advertisements	5%
Further emails at any time	10%

Table 7 Available communication and marketing channels

However, as with the lack of specificity about cookies, organisations were generally unclear about the effects on the user experience if customers chose to opt–out of certain communications. For example, what potential benefits (e.g. special offers) they would forego by opting out.

11 Empirical findings: Informed consent in practice

The academic literature on informed consent practices suggests that consent giving is often seen to be a tedious practice, with few customers actually taking the time to read the detailed text in terms and conditions. Customers tend, instead, to use behavioural constraints such as favouring near–term benefits over longer–term disadvantages and, if they have already chosen to engage in a service like Open Banking, often finding that positive frictions in the user experience are unhelpful.

The empirical research therefore sought to explore current consent giving practices, both for existing users of apps and services that access their financial data and for other smart phone users who did not use apps that managed financial data.

The findings from study 1 and studies 2 and 3 highlight how ineffective terms and conditions are for explaining intended data processing to customers. As a result, consumers rarely read the text of these notices and, as study 1 found, even when they are read they are not necessarily understood properly. All too frequently they are written with little consideration of their intended recipient (i.e. the consumer).

As a consequence, the studies found that many customers did not fully understand or appreciate the implications of how their data would be processed, particularly beyond the processing necessary for the core service that had been signed up for. In some cases, taking part in the research caused them to reflect on their attitude to terms and conditions and resulted in some considering closing their accounts. The findings are discussed in more detail below.

11.1 To what extent are existing terms and conditions effective at explaining intended data processing to customers?

In Study 1, which focussed on regular smartphone and app users rather than TPP customers, participants were asked how frequently they read the terms and conditions of the service they were using. 45.2% of the 191 participants admitted to not reading the terms and conditions of the service with a further 40.9% claiming that they "skim–read" them.

When the 45.2% of participants who admitted to not reading the terms and conditions were asked why they did not read the terms and conditions, 41.9% of them indicated that the text was too long, 23.1% indicated that they didn't have enough time to read them all and 31.2% indicated that they assumed that the service would comply with the law. Finally, 17% of the non–readers indicated that they didn't read the terms and conditions because the app was providing a useful service for them.

Study 1 also asked what extra steps participants would take before agreeing to the terms and conditions of an online service. 54% indicated that they don't take any extra steps whilst 28.6% indicated that they read reviews (e.g. on the app store)—effectively relying on the wisdom of the crowd to highlight any potential issues.

According to Study 1, it is not just the effort involved in reading terms and conditions that is problematic as 77% of participants noted that they didn't feel informed when reading them.

To test this element further, Study 1 included a timed exercise where study participants were shown an extract of a sample terms and conditions page for the app "FMA" (based on a popular social media application). They were then asked a series of questions about the terms and conditions but were also provided with an opportunity to review them again before answering. If the terms and conditions were clear, one would expect that most participants would spend some time reading the text and then correctly answer the questions. If the terms and conditions were unclear or, as suggested above, rarely read properly, then one would expect participants to choose to review the text before answering.

Statement	Percentage of respondents who gave the correct answer after the initial viewing of the terms and conditions	Percentage of all respondents that went back to review terms and conditions	Percentage of those who had reviewed the terms and conditions and then gave the correct answer
1) FMA guarantees the safety of the application	17.2%	41.4%	7.0%
2) FMA can advertise other unrelated services without having to identify them	36.6%	40.3%	23.1%
3) The service will notify you of any changes made to the terms and conditions and give you the opportunity to review them before accepting	51.6%	31.7%	22%

Table 8 Timed Exercise: Answering questions on terms and conditions

The first statement was only correctly answered by a small number of participants after reading the terms and conditions once. Moreover, even when participants were able to review the text it was still answered poorly, suggesting a lack of clarity and understanding about this aspect of the service.

Responses to the second and third statements were better (which might be the result of a combination of factors including "expected" behaviours of apps (advertising, changing the terms and conditions) as well as increased exposure to the terms and conditions as something "present–at–hand" and clearly the focus of attention in this part of the study).

These findings were mirrored in studies 2 and 3 when the actual customers of third–party providers acknowledged the importance of understanding terms and conditions, but fundamentally found them to be of little relevance when making the decision to use a particular third–party service. In fact, 28 out of 50 contributors claimed not to read the terms and conditions of *any* of the products or services they sign up for and 27 of the 50 contributors did not read the terms and conditions of the specific financial service app they were using.

11.2 Concerns about the presentation of terms and conditions

A consistent finding in studies 2 and 3 related to concerns about the ways in which privacy policies and terms and conditions were presented. A specific issue relates to the terminology used to describe their content. An analytic code referring to 'Legal Jargon'[3] was prevalent within most of the transcripts. It implied the way legal terminology was deployed by the TPPs, from the perspective of someone who has little experience of the law, such as phrases like "Denial–of–service attack" or "Distributed denial–of–service attack" [Contributor 24, Male, App02B User].

> I think quite often these Ts & Cs are just far too long and contain far too much legal language which ordinary people, you know, a) they don't have the time to spend two hours reading it and understanding it … it's written in such a way that it's not easy to understand. [Contributor 14, male, App05B User]

When contributors were asked how they tried to understand the implications of the Ts & Cs in more detail, they reported that the first glance at the terms and conditions caused feelings of uncertainty, or they felt they were "daunting". This is portrayed in Contributor 11's statement:

> The Ts & Cs as we said right at the beginning are usually and I don't remember App05B but are usually so long that nobody really reads all the way through. I try to skip down to paragraphs that headed data privacy and what they do with your data. There's probably plenty I miss. [Contributor 11, male, App05B User]

The overall look of Ts & Cs is an important factor in understanding how people currently consent to share their transactional data. It affects how Ts & Cs are perceived, including how they make contributors feel. Frequently the organisation of the material is seen as problematic:

---

[3] Codes like legal jargon that were used in the analysis of the interview and focus group data are indicated with 'single quote' marks.

> This thing it says, "what you allow us to do" that should probably be, like, way up. Limitation of liability, that part is just very confusing … I mean loss of goodwill, that could mean any detail. [Contributor 12, male, App05B User]

Contributor 14 (Male, App05B User) suggests 'Legal Jargon' is a protection for companies from "courtroom drama".

Additionally, 'Blanket Statements' hindered understanding of Ts & Cs whereby vagueness contributes to being uninformed about current Ts & Cs for third–party providers. Contributor 20 mentions this is the reason he did not read the Ts & Cs:

> because, let's face it, the Ts & Cs for any kind of commercial website are pretty similar. [Contributor 20, male, App02B User]

11.3 Understanding of implications of Ts & Cs

Studies 2 and 3 found that whilst many contributors had a basic understanding of the service they were using and hence gave consent that enabled the service to operate, most failed to comprehend the implications of some of the Ts & Cs they had agreed to, i.e. that were associated with the consent they had given.

This tension between individual agency and engineered consent is explored by Contributor 47:

> Most people ask for forgiveness of their terms rather than approval. As a society, we are very unclear as to where forgiveness is required and where consent is required. If you always ask for consent, you will never do innovation. [Contributor 47, male, App11K User]

This notion of forgiveness was also apparent in Contributor 50's annoyance when she discovered that the TPP doesn't require further consent when terms and conditions change or update. The Ts & Cs only require acceptance at the start of the service use and the TPP wouldn't alert her to changes. Despite this annoyance, the contributor showed a willingness to forego these new approvals if it meant that the benefit of the new services she was receiving—for instance the ability to borrow money from the TPP—outweighed her lack of agreement to the changes. Thus, even though the TPP has not received the user's updated consent, it could be doing some really innovative things with their user's data to create something new and improve services. It should be noted, however, that under GDPR a service provider will be required to obtain informed consent before any new forms of processing could take place.

More than half of the contributors believed that the consent they had given was uninformed. In many cases, this was because there were underlying notions of confusion. For example, when asked if Ts & Cs helped make an informed choice, Contributor 8 responded:

> No. Well, not for anyone that I know. They're just dense—I don't really know what it is. They're just … I don't know. [Contributor 8, female, App04F User]

This sentiment was echoed throughout most of the focus groups and interviews.

The combination of 'Legal Jargon' and 'Blanket Statements' peppered throughout the Ts & Cs, meant contributors often have a limited understanding of data processes and what they have given consent for. This is particularly evident in Contributor 19's denial that he shares financial data with his TPP:

> My financial data I wouldn't share, so I would not do that. Personal information, again, depends on what type of information, so name, number, address perhaps, I wouldn't, that's all available online anyway, so I wouldn't mind too much to sharing that. But then, anything that extends beyond that I would find …
>
> Interviewer: Okay. And how do you feel about consenting your financial data with App04F?
>
> I wouldn't consent that. [Contributor 19, male, App04F User]

Contributor 19 is confident that he does not share his financial data, contrary to his actions. He is wary of sharing financial data, but is less concerned about sharing personal data. Personal data to him compromises of name, number and address. Due to the abundance of information online, his personal data is seen to be compromised already. This shows disparity in the level of control he feels over his personal and financial data.

This, for instance, was Contributor 1's response when asked what happens to her data once shared:

> I know they look at transaction history. I don't know where it is stored. [Contributor 1, female, App10S User]

Unlike Contributor 19, Contributor 1 is aware that her financial data is shared with App10S. However, she is unclear about what happens to her data. Furthermore, Contributor 2 (Female, App04F User) was unclear as to whether her data would be aggregated and sold by her TPP, "I think that might be possible, I don't know". She even questions if App04F has the capabilities to do this kind of aggregation. Moreover, this lack of knowledge elicits uncertainty:

> You don't know what information has been shared with them. It's that uncertainty and that ambiguity which I think concerns me more than anything else. [Contributor 46, male, App02B User]

It is interesting to note that towards the end of the majority of interviews, the researchers were thanked for allowing contributors to reflect on the importance of reading and understanding Ts & Cs. One contributor went on to say the following:

> I'll probably delete App06P, I'll probably read the Ts & Cs a bit more now. [Contributor 7, male, App06P User]

Contributor 26 echoed this sentiment:

> You know what, it's going to sound weird, but after this, I think after this interview I advise people to read the Ts & Cs regarding, just pay attention to the data sharing part. It just hit me, other than the financial stuff, I think App04F does that, but like Nat West or Barclays or any normal banks, when you have to apply for a bank card, you still have to enter a lot of your personal stuff. App04F doesn't take my number, but the normal bank does take my number and stuff like that. [Contributor 26, male, App07S User]

Contributor 7's and Contributor 26's trust is noticeably shaken by the end of the interviews as they have reflected on the implications of the consents they have already given. They question the personal and financial data they have provided to App06P and App07S. Knowledge of financial services is anchored in services received from traditional banks who were broadly perceived as trustworthy in terms of provision of financial services.

11.4 Suggestions for good practice

Suggestions for good practice around asking for consent and presentation of terms and conditions and privacy policies were obtained in studies 1, 2 and 3.

In Study 1, participants were asked to rank (on a 1–7 scale where 1 indicated their highest preference and 7 the lowest) what they thought would be ideal in a terms and conditions statement, the weighted average ranking is:

- Short Length of Text (2.60)
- Highlighting of potential consumer risks at start of the Terms and Conditions (2.74)
- Simple use of language and fewer technical terms (2.75)
- Highlighting of major features at start of Terms and Conditions (3.26)
- Smaller Chunks of Text at a time (4.57)
- Confirmation of Understanding with follow up questions (5.17)
- Others (6.91)

In studies 2 and 3, all contributors asked for a better written, visual presentation and organisation of Ts & Cs. It was widely understood that the presentation of Ts & Cs can be a factor which deters people from giving consent. A popular suggestion was writing Ts & Cs clearly for all to understand, echoing the results from Study 1. This was manifested in Contributor 13's statement:

> I think that would take a lot of effort that they won't put in, like I worked in technical writing and so my whole job was to take complex software and simplify it for the end user. That was my job. That would need somebody in that role to simplify Ts & Cs and they're not going to do that, because sure it would be super helpful and people would appreciate it, but the value would

not make it a good business case to hire that person. [Contributor 13, Female, App03B & App08S User]

Contributor 13 had background knowledge in technological writing. She lobbies for Ts & Cs to be simplified so that they can be useful to the many. However, she also presents a meta–perspective of the TPPs. She attributes their reasoning for a lack of clarity to financial losses for businesses. This idea was furthered by discussing the implementations of 'Layman Terms', whereby basic terminology is valued in comparison to difficult, advanced language. This is echoed in Contributor 11's statement:

Clarify the Ts & Cs. Make them briefer. And say in big type, "we don't sell on your data". [Contributor 11, male, App05B User]

Furthermore, just like Contributor 11, the length of Ts & Cs proved to be troublesome for many contributors. They postulated that the shorter the Ts & Cs, the better the understanding. For one contributor reading through the exhaustive current list of Ts & Cs "tested her patience" (Contributor 2, female, App04F User). This thought was also found Focus Group 2:

Contributor 43: I think they are just too long, boring, but they are trying to make their stance

Moderator: Okay, anyone else?

Contributor 41: I think they have to highlight the main points of the contract, because every time when you come to the bank and open an account, the assistant in the bank will hand you some papers and he will use the pen to highlight something important for you when you have to know when using the accounts. So if you're starting to use a digital platform, you do not have the assistant to do this for you, so the platforms themselves have to highlight what are the main points for the customers to have a look at. [Contributors 37–44, App09F Users]

Contributor 41 compares App09F to a traditional bank. There is an element of future banking being faceless as traditional banking, to her, conveys human interaction. She finds signing and agreeing to consent online as passive, whereby human interaction is needed to make an informed choice.

Interactive presentation of Ts & Cs was a suggestion highlighted by some contributors. They reasoned that this would help visualise the Ts & Cs, as opposed to passively retaining information through reading. Contributor 26 shared his thoughts regarding this area:

Obviously like reading the whole terms and condition is very tedious, wouldn't it be great if there's like a way they can make it into a video, but with specific guidelines. If you have to use the app and then you have to finish watching the video, stuff like that. Then still again, people would just

> put it somewhere unless it's like five minutes. [Contributor 26, male, App07B User]

The suggestion of video content is very reflective of the way in which news and information is consumed on social media, which shows a juxtaposition that although the TPP itself is forward–thinking in its use of technology, actually, Ts & Cs—and the way they are written and viewed—are still lagging behind.

Moreover, the organisation of Ts & Cs could be improved. Many contributors argued for a Bullet Point list, highlighting a need for synthesised material.

> I think they could probably put the important section on top, like what they really want to tell the consumer first. And then because normally when you sign the Ts & Cs it will be these windows and then you tick it. So normally what Ts & Cs are inside—1.1 Introduction. Then you really won't read it. But if it's, "This is very important …" then you will. [Contributor 6, female, App01B User]

Many of these suggestions correspond to recommendations made by the Information Commissioner's Office in their guidance on privacy notices (Information Commissioner's Office 2016).

12 Empirical findings: How customers make decisions around the choice of apps and services

Although the terms and conditions of potential services are likely to influence the take up of particular apps and services, studies 2 and 3 also found evidence that the decision to use a particular app or service was often already made before the terms and conditions were considered and before consent was given to allow the app to access their financial data.

The research findings revealed that some consumers found the service proposition so appealing that they didn't bother to examine the terms and conditions of the service. When exploring the potential risks of using a particular service some adopted the strategy of trialling the service with less critical bank accounts. Other users relied on other proxy measures, such as the reputation of the service provider to make the decision. The findings are discussed in more detail below.

For many, the mere notion of money management functionality enticed contributors to use the TPP. For instance, Contributor 48 (Male, App02B User), mentioned how the money management service "is a very nice way of tracking where you are in the month on your budget and where you are with your spending. Sort of keeping on top of everything. You can obviously budget ahead, as well". Moreover, the functionality of the app and the interface it provided to the accounts was integral to why contributors would choose to use a specific TPP. For instance, when Contributor 32 was asked why she used App02B, she argued the following:

> Ease of use. I looked at what kind of accounts you could put on. Not all of the apps allowed you to do different types of accounts. There were some where you couldn't add your pension in. Others, you couldn't add any trading / investments … So App02B seemed to be the one that had the availability to add lots of different types of financial accounts into. [Contributor 32, female, App02B User]

The ability to trial the use of App02B before committing to the service was found to be useful and addressed concerns about engaging with an organisation that was not known and hence not already trusted:

> There's like a free 30–day trial period, so I ran it for a few days without it connecting to any sources and just manually put in balances and checked the functionality. I think then, like I said, I tested it with a few accounts, just made sure nothing weird happened and then continued to use it. Then the 30–day free trial lapsed and I decided then to pay for it. [Contributor 18, male, App02B User]

Knowing that "nothing weird happened" to his accounts during the trial period, helped Contributor 18 make a full commitment to using (and paying for) App02B services.

In a similar manner to Contributor 18, Contributor 20 highlights the independent research he conducted by comparing different TPP offerings:

> I did research, I was just simply looking at and I just basically just researched and went into all the different sites that did this. [Contributor 20, male, App02B User]

Advertisements on social media platforms also influenced contributors to join specific TPPs. Others put emphasis on customer reviews and the reputations of the service providers. Understanding existing customers' experience of sharing financial data was pivotal for some contributors. This was a common practice exercised amongst contributors. For example, Contributor 2 commented on the importance of the experiences of other customers:

> It's like other people have used this before. They say that like it's good then I would really bother to read. [Contributor 2, female, App04F User]

Contributor 2 echoes the findings of Study 1 by suggesting that reviews by other customers have a deciding factor on whether she is likely to share her data with a specific TPP. If she finds a consensus when reading reviews, she is likely to engage with a product. The power of decision in this case lies with existing customers.

Contributors were also likely to research the reputation surrounding the TPPs and how their financial data is used. Many used Equifax as an example of a financial service that has sustained damage to its reputation after a data breach. Moreover, Contributor 14 expanded this thought further by arguing for the value of reputations:

> I mean it seemed to have a good reputation in terms of the articles I read and the reviews I read and it seemed to be a well–constructed site and the banks that it communicated with didn't seem to have an issue with it either, so … App05B was a reputable, trustworthy site to hold my data. [Contributor 14, male, App05B User]

Many of the contributors expressed a tension in freely choosing to give consent to the TPPs. When asked about whether he would agree with certain practices by the TPP, Contributor 19 repeated that with "conscious consent" he wouldn't agree. This suggest that he may have unconsciously consented to forms of processing by the TPP that he doesn't necessarily agree with. This was particularly noticeable in the case of apps that encouraged consumers to save. If the app was effective at its main goal, e.g. encouraging saving, research contributors were likely to sign up and not consider the implications of many of these apps being provided for free. Equally, Contributor 19 also highlights an interesting point with regards to giving consent:

> Well, if I'm the one that's providing that additional information, then I can't see why that would be an issue. If they change without my consent, then there might be some concerns. [Contributor 19, male, App04F User]

Here we find that although the terms of the service might change without Contributor 19's explicit consent, he conditionally suggests there might be concerns, but these concerns don't necessarily prevent him from using the service. Thus, although freely deciding to give consent is the preferred method, many contributors are aware of the extent of freedom they have allowed the TPPs, too.

Therefore, as mentioned previously, many contributors felt coerced into consenting. Despite not wanting to agree to the terms and conditions of the TPP, because of a lack of understanding about what happens to their data or from a data–moral standpoint, they had no choice but to consent if they wanted to get to the next stage of the app or even to see a particular webpage. As asserted by Contributor 11 (male, App05B User), "it's a bit of a catch 22". This shows the extent to which consent–gathering processes can be engineered to manipulate decision–making at an individual consumer level. Nevertheless, although this paradox is presented as a lack of choice, Contributor 17 still acknowledges the individual agency involved:

> It's the choice you make to sign up to their website. It's not forced upon you. I think you have to have a certain level of trust to give your password to a faceless internet website, so I think I have to say I'm happy to do so. Otherwise I wouldn't be using it. [Contributor 17, female, App02B User]

Study 1 asked participants what they would do if, having decided to use a particular kind of service, such as an Open Banking app to help with financial planning or savings, they did not agree to or were unclear about the terms and conditions of a particular online service that appeared to address their needs.

Study 1 found that 55.9% of participants reported that they would find another application that served a similar purpose, 30.1% would clarify their concerns with the service provider (i.e. through email or a phone call) and 22% would have somebody else read terms and conditions for clarification. In Study 1 40.9% reported that they would probably install the application anyway.

13 Empirical findings: Individual factors

The empirical studies also examined the effects that individual attitudes to privacy, perceptions of risk to personal data and the value of personal data had on the decision to give consent to a third–party provider.

Although the empirical research was focussed on consumers who had agreed to allow apps and services to have access to their financial data, the findings highlight considerable variation in terms of attitudes to risk and privacy even within this group of users. The special status of financial data and the risks that it faces were discussed in detail by contributors echoing the findings in study 1. The research also explored the understanding of, and attitudes to, additional processing of personal and financial data beyond that necessary for the service that had been signed up for. Some contributors recognised the role of this kind of data aggregation and exploitation with some having clear views on what was considered a reasonable, or inevitable, use of this data and whether this was a fair price to pay for the service. The research findings also included consideration of the implications of this for notions of ownership and value of the (aggregate) data and the consequences of the revocation of consent in such cases. The findings are discussed in more detail below.

13.1 Privacy attitudes and risk assessments

Amongst the contributors to studies 2 and 3 many expressed sentiments and exhibited attitudes of being both risk averse—suggesting that contributors were cautious about sharing their financial data—and risk takers—not least because contributors had already offered to share their financial data with the app or service they were using. This dual behaviour is manifested in Contributor 5's dialogue:

> I have an account which I share with them, but it's only for basic expenses. The other account they do not have access to is the account I use to pay for my fees, accommodation and tuition. This is the one I won't be sharing with App05B. [Contributor 5, female, App05B User]

Contributor 5 manipulates the information so that what appears to be all of her accounts in one place, are in fact just a few of her accounts. Fundamentally, she makes the link between financial data and financial worth and her risk–averse and risk–taker behaviour. Similarly, Contributor 3 also exhibited this dual trait:

> I think you have to key in like your details, like your sort code and your account number. So that is quite like high risk information. [Contributor 3, female, App12B User]

Contributor 3 shares her financial data with App12B and uses the phrase "key in" which suggests that in order to use this financial service she has no other choice but to share her data, despite acknowledging that it is risky to do so. The service is an essential factor in the way customers understand whether it is a good–value in

exchange for data; if they believe the service offered is worthwhile then they are prepared to risk sharing their financial data.

An interesting point to consider is that some of the student contributors didn't hold the same level of value towards their financial data as non–students and so the explicit and implicit cost of the service for their financial data / money was quite different. This was the case for Contributor 27:

> Yes, it is financial data and things like that, plus I feel it's a lot to do because I am still a student, so I don't really have a stable income which I feel may be affected. Maybe as I started earning on a regular basis I might feel differently. [Contributor 27, female, App03B User]

Therefore, because many students will not have large amounts of money in their account many view their use of the service as quite low risk / good value for money and this becomes part of their privacy calculus. This is highlighted by Contributor 26:

> I feel like for me, I don't have that much to lose. It sounds very ignorant, but even if I lost my data or it got hacked, I don't really have that much to lose because it's all just groceries and food for me. [Contributor 26, male, App07S User]

This quotation highlights a limited understanding of how other data points (such as the grocery purchasing habits) may still be valuable to firms who may be able to infer valuable insights from this additional data.

13.2 The status of financial data

In the context of giving consent to sharing of financial data, many of the concerns emerging from studies 2 and 3 were related to the unprecedented pace of technological developments. Thus, it is reasonable to consider that concerns regarding financial data are equally unprecedented for many of the contributors, especially given that all contributors in studies 2 and 3 had also signed up for various social media services.

All contributors mentioned the distinction between personal and financial data, but some merged these two types of data together. Some argued that personal and financial data were both sensitive, yet financial data was often compromised of personal data:

> I'm trying to remember the terminology, but there's personal data and then there's sensitive personal data and I would consider financial data to be sensitive. So, like data about me, my name, address, email address and potentially date of birth, I would consider to be personal data. My medical records, or political affiliations or whatever, are considered to be sensitive data. Financial I would consider to be sensitive data because there would be a very, very small group of people that I would be willing to share financial

> information with, but my name and address much wider. [Contributor 18, Male, App02B User]

In this discussion by Contributor 18 there is a hint of ownership too, whereby he believes that some data is rightfully his. Therefore, for Contributor 18, there is no difference between personal and financial data. In contrast, some contributors believed their personal data to be of more value. For instance, Contributor 13 prizes personal data over financial data:

> Hmm. I guess … To me, financial data feels less private … Surely it's more personal to know exactly where I'm spending my money and how much I'm earning and all those details. But it feels like it's already out there anyway, versus personal details which I elect to share. [Contributor 13, female, App03B User]

Contributor 13 argues that she has voluntarily submitted her financial data to App03B and Equifax, yet has not shared her personal information. She admits this sounds counter–intuitive but for her, it is the only way to exercise some form of control over shared data.

This topic was touched upon in focus group 1 too (Contributors 34–36, App02B User & App05B Users).

> Moderator: Okay, great. And do you think, I guess, mainly you'd think that the one that has more about financial data will have less value than personal data, do you think one does have more value than the other?
>
> Contributor 34: I think to me, they have a difference in value … like financial data has a lot of value to a lot of companies.
>
> Contributor 35: Yeah, it depends who the company is that's wanting the data and what they want from it.
>
> Contributor 36: I would say it's more the source of the data for financial data, not really the data itself but how they get it, through my passwords and everything.

This conversation exemplifies how financial data is important to all contributors in this focus group, although for Contributor 36 it is the meaning and process of how companies obtain this data that is key. The contributors speak in terms of value for the companies and not themselves.

Furthermore, for most contributors, there are levels of sharing personal data. They control the degree to what they share, again voluntarily. This is echoed in the same focus group:

> Moderator: Great. So talking more generally now about data sharing and privacy, do you all use social media and what sort of things do you share on social media?

> Contributor 35: I don't share a lot. I only really use … Instagram is probably the only social media that I actually use and mine's private and I probably post something once a month. I'll use other social media sites just to look at things but not post anything myself.
>
> Contributor 34: I'm the same as you. I rarely post anything so I'll go on and check other people's stuff, but I rarely do anything, and if I do, it's on Instagram. I think I was really scared, because I was a teacher previously and just heard some horrendous stories about people … and then it gets brought up and I got very, very wary about being on there, so people have had their accounts taken over and they can get into big trouble and it's just too complicated and not worth it. I'm very wary about what I put on and about where I am and often don't put it on at the time I'm there and that kind of stuff.

This was echoed throughout most interviews and focus groups. The agreement between Contributor 34 and 35 denotes different levels of trust for different social media platforms. This caution was seen to be reasonable as breaches of personal data on social media platforms could jeopardise future career prospects, although this would often be misuse by other users of the platform rather than by the platform owner.

This distinction was also highlighted in Contributor 5's (Female, App05B User) concern too: "I share what I've eaten but nothing like full name, phone number, so I only share information which I comfortable with other people knowing". There is caution as to what is shared on social media where sharing can have tangible effects.

In the context of financial data rather than social media data, the way financial data is currently being used and transferred onto servers is a concern of Contributor 18.

> For me, that's a flawed model. I would rather that my device is connected, collecting the information and it's never going anywhere near App02B's servers. I don't understand technically why that's not possible, because it would have been much more of a no–brainer for me, but I do remember reading this now and thinking, "Gosh that's not great, but I'm short of time, so I'm going to go ahead anyway". [Contributor 18, male, App02B User]

This issue was also explored in Study 1 when participants were given a brief introduction to the functionality that Open Banking would enable. They were then asked to describe their concerns with the Open Banking process and their qualitative responses were then coded. The top concerns related to provision of data to third–parties, over exposure of their data and the risk of security breaches / malicious activity.

Study 1 also revealed a (statistically significant) difference amongst participants in relation to their reaction to data breaches in financial and social media data with reactions to financial data breaches being rated more negatively than social media

data. Participants also gave statistically significant different ratings of caution between consenting to share data with a financial services app and a health app, with participants reporting a higher level of caution towards accepting Ts & Cs of financial data applications (4.09) compared to health applications (3.63).

13.3 Risks to the data

Contributors discussed a range of risks to personal data processed by third–party providers with data breaches being the most commonly cited concern amongst contributors. A data breach can be defined when data is disclosed without the consent of the data owner:

> I don't want all and sundry knowing my date of birth and mother's maiden name and things like that. In fact, on at least one website I've given a fictitious date of birth because if anybody hacked it, used that date of birth, hopefully anything they applied for would get rejected because it was the wrong date of birth. I don't know if that would happen. I just hope it would. [Contributor 11, male, App05B User]

Contributor 11, like other contributors, has tried to outwit the system by providing a fictitious date of birth. This action reveals how, although he has shared his financial data, he lacks trust in sharing personal data. He has to rely on the service provider's ability to keep data secure and the regulator's capability to mitigate the consequences of any breach.

Moreover, the concern overlaps with Contributor 17's concern surrounding 'Fraud':

> I know that it's very, very easy for some criminals and outside agencies to get hold of data, by many means, whether it be accidentally sharing too much or whether it's them hacking their way into systems. So, my data for example, its security keeps me safe, as well, from losing money or having something set up in my name and used fraudulently, for example. Obviously, it has a lot of value to me in keeping my world safe, but I think it has value to other people for them to act immorally. They're less concerned about me than I am of them. [Contributor 17, female, App02B User]

Contributor 17's "world" would be compromised if the data fell into the wrong hands. This highlights the importance of keeping her financial and personal data secure.

For other contributors, it was financial loss that was the major concern associated with TPPs. Often arising from intangible fraud and data breaches, it is the loss of money that is often perceived as the most tangible outcome.

> The uncertainty of what could happen is the biggest consequence because you don't know what could happen, like someone could hack into your back account and all that's gone, it's just empty. I'd have to cancel all my cards

> and wait for new ones to come, all the bank accounts, things like that. [Contributor 12, male, App05B User]

Therefore, this illustrates that although there are concerns with the pace of technology, data breaches and fraudulent activity, the outcome which underpins each of these areas of concern is the loss of real money. When asked about data breaches, contributors were more concerned about the loss of money, than data, as money is something familiar and tangible, whereas data is somewhat unfamiliar.

For many contributors to studies 2 and 3, the belief is that a data breach will happen in the not too–distant future. When discussing data breaches, Contributor 17 said it will "definitely happen", but Contributor 23's assertion is particularly illuminating:

> … hacking is obviously a concern. The data breaches, you hear almost every day there's a new company that's saying, even Uber the other day, because Uber has got so much money and yet they can still be compromised, so that's concerning, that even a company that big and that wealthy can be compromised. That's more my concern, other than companies using my data for their own purposes. [Contributor 23, male, App02B User]

The findings from Study 1 echo many of these concerns. When participants were asked why they might not accept a company's Ts & Cs, the three most popular responses related to the sensitivity of data that was being used by the company (42.2%), when they didn't trust the company (24.2%) or when the company's reputation had been affected by negative news coverage (21.1%).

13.4 Perceived fairness of other, secondary uses of the data

The research found that consumers have some general knowledge about how apps might use (and profit) from their data, but they generally had a limited knowledge, and sometimes misconceptions, about the specific handling and use of their data by the TPPs. Consumers who are unclear about what can happen to their data are unlikely to fully appreciate the implications of their giving consent to share their financial data with a third–party provider. In particular they are unlikely to appreciate the added value that their data can provide to the TPP. This value can be found by personalising services for that customer or by selling aggregated insights from batches of customer data to interested other parties. Contributor 11 illustrated this lack of understanding in his interview:

> I kind of knew, but I'm pushing it to the back of my mind what they might be doing with my data. And I don't have any control over it, really. And I don't know how to get it deleted. [Contributor 11, male, App05B User]

In terms of these other potential uses of their data, contributors were asked what a fair use of their data would be. Many agreed that personalised and targeted marketing was a fair use of the data, with 31 contributors explicitly naming this in their response to the question. One of the reasons that many people agreed with this

data usage was that targeted advertising was frequently seen as helpful. Contributor 10 explains:

> Again sometimes it's interesting and useful, sometimes it's kind of creepy and you have to sit there going, "okay I know you're just … I'm clearly getting these ads because I've hit the criteria". A really interesting example of that would be my wife and I have been married for two and a half years, we don't have kids, half our ads on Facebook now are for fertility treatment. They've clearly gone, "right, you're you've been married for this long, you've hit all of these boxes therefore we're going to serve it to you", so it's a little bit creepy sometimes, but …
>
> Interviewer: And what's your view I guess then, about how these online providers store and then share or sell your data onto other parties?
>
> Yeah, so I think it's a bit of a difficult line to walk because my view is that, as long as it's helpful and I can see clear value in how that's coming back to me, then I'm happy with it. It is, as I say, a difficult line to walk. [Contributor 10, male, App05B User]

Therefore, for those consumers who understand the benefits of using data for advertising and marketing purposes, to help improve their day–to–day lives, they accepted that these data usages were useful. Furthermore, personalised advertising is something that is clearly visible on websites and social media platforms which consumers use. For instance, one of the contributors in the mixed–application focus group first heard about his TPP through targeted marketing.

However, when it came to uses which are much more invisible, or uses they were unfamiliar with, the extent to which consumers perceived these uses as fair was much more contested. Moreover, not all contributors appreciated that whilst the targeted messages were helpful to them, they were also a potential revenue stream for others.

In a mixed–application focus group, it became apparent that the more distant the contributors were to the type of data usage—which differed from the app's original purpose—the more uncertain they were regarding whether they considered it a fair use.

> Moderator: Offering you products?
>
> Contributor 36: Yeah. Wait, the app offering you products, or …?
>
> Moderator: Yeah. Okay, what about if it was a third–party offering you products?
>
> Contributor 36: Depends on its applicability to you.
>
> Moderator: Okay. Selling data to third–parties?
>
> Contributor 36: Questionable (Laughs).
>
> Contributor 34: It depends who.

Contributor 36: For what reason.

Contributor 35: Yeah, exactly.

Moderator: Selling information to third–parties so that they can offer new and improved services on products?

Contributor 36: I'd say again it depends on the data and depends on what company they're selling it to and whether it's going to be beneficial to me.

Contributor 34: Yes, because that sounds like it could just be beneficial to them. It could be the services they provide to other people.

Contributor 35: Yeah, if it's beneficial to you and genuinely, then that's okay.

Moderator: Brilliant. Last one. Selling data to third–parties to be used for differentiation so marketing strategies, different products or prices to different customers?

Contributor 36: You're telling me that you're going to charge me more because (Laughs)

Contributor 34: That's a no from me. Definitely not.

Contributor 36: The differentiation is … yes, that's very questionable. Is it even legal to differentiate price between customers?

This interaction shows that amongst the contributors, the perception of data usage can go from being seen as objectively fair to being perceived as subjectively immoral and even illegal.

Those contributors who had a higher level of trust and commitment in their TPP, were more forgiving of what they considered fair data use. This was shown by Contributor 13:

> I seem to benefit from getting all this budgeting health and savings tools, but they get all the impressions of not only what I'm doing and how I'm using the app and how I'm spending, but how everyone else is as well. And they can use that data to share with other companies or whatever they're doing with it, but also they can use it to update that, to make me even more committed to it, if that makes sense. [Contributor 13, female, App03B & App08S User]

Studies 2 and 3 also examined the contributors' level of data savviness in understanding how their data might be used and whether this data processing constituted a fair and ethical standard. As noted above, most contributors believed that anonymising and aggregating data, for example for targeted advertising, was the fairest and most valuable / profitable way in which TPPs should use customer data. Contributor 18 agreed that in the context of marketing, data aggregation was valuable to help work out behaviours. He said:

> Google, obviously, aggregates a lot of data to work out behaviours and preferences. Yeah, I don't have a problem with data aggregation. It's when the data is misused that it's an issue. [Contributor 18, male, App02B User]

Other contributors argued that data is only profitable when aggregated. Contributor 5 (female, App05B User) explicitly shared this sentiment, adding: "I mean that data only has value when it's gathered" and Contributor 17 agreed that it was fair to sell non–attributable (anonymised) data for aggregation purposes.

> If they are just using my data as a representative of the population and they're using it as just statistics rather than personalised, then, again, to some extent I'm happy to provide data that will allow them to see what goes on statistically, but not specifically to me. [Contributor 17, female, App02B User]

Although many contributors agreed that data aggregation constituted a fair use of the data, there is an apparent tension regarding the extent to which this fair use of data may raise unethical implications. Contributors agreed that privacy is an important factor when considering how TPPs make use of their data.

Contributors highlight a need for TPPs to be more transparent in what they do with customers' data, even when they have consent to process customer data. Although many contributors were data savvy (a majority worked in finance or technology or had an interest in data and technology), when asked about the uses of financial data, there were major gaps in their knowledge. Many blamed this on the ambiguity of the terms and conditions.

> Yes, they said—I think there is like a link that you can contact someone about your transaction history if you find something wrong with it or if you want to report anything about it. [Contributor 1, female, App10S User]

Therefore, despite being data savvy and thus possessing a good understanding of what happens to their data many contributors' knowledge is generalised.

Recognising that organisations often make profits from working with third–parties such as advertisers, or by sharing or selling aggregated information, Study 4 explored the extent to which this information is clearly presented in the Ts & Cs and privacy policies of the organisations sampled. Two–fifths of companies (42%) reported that they share or sell aggregated data with advertisers. However, only 10% of them revealed their advertising revenue model (i.e., whether they receive a commission or fee from third–parties) in their privacy policy.

More generally, the apps and services are generally clear about the purposes and limits on any data sharing. For example, more than half of the companies (58%) explicitly assure users that they will not share, sell, trade or rent personal information for any reason that is not disclosed on their privacy notices without prior consent to do so.

When the privacy notice does disclose that data will be shared with third–parties, these same companies are frequently vague and imprecise about which

third–party providers the data would be shared with and rarely specify the data that would be shared.

The lack of specificity continues in relation to the third of companies (36%) whose privacy notices mention that they will share or sell aggregated and / or statistical information with third–parties, but then fail to mention what kind of information will be included in these aggregated data sets.

Some organisations use third–parties to process personal information on their behalf but frequently make no reference to which third–parties they will be using to provide this service and which data is being processed by them.

13.5 Paid for services

A key consideration for many contributors was whether the service they are receiving is free or paid for (or a combined freemium model). Contributor 5's reasoning for using App05B was the 'no fee' (Contributor 5, Female, App05B User). Contributor 18, in contrast, is a user of App02B, a paid for service and had strong views on financial data and paid services:

> I just think I would question the motives of the people running the free app; it feels like … I think it was Chris Anderson that once wrote that "If you get a service that's free, it's not the product. You are". You're the thing being sold. [Contributor 18, male, App02B User]

This extract highlights Contributor 18's concerns about ulterior motives around the use of data and draws parallels to the bounded trust some contributors felt with their TPPs. He recognises and expresses dissatisfaction with how his data could be used if it was a free service, processes that should be clearly articulated in the terms and conditions of the free service. This is also reflected in Contributor 13's argument:

> App08S was free, but I signed up right when they had pretty much launched it, or soon after they launched it, so it was free for a while but then they started charging a monthly fee and the rationale for it was, "We don't do the targeted advertising. We don't ever want to do targeted advertising. So we're just going to charge for it". And yeah, I would rather do that. I would rather pay $3 a month for a tool that I trust and rely on and I know they're not going to promote a credit card every other day. [Contributor 13, Female, App03B & App08S User]

In Study 1, participants were asked whether they agreed with the statement: "I am more likely to share my personal information if I understand how a company makes money from it". 57% of respondents disagreed with this statement. 62% expressed some disagreement with the statement "I am more likely to sign up to new services which give financial incentives in order to use or sell my data (in the form of freebies, profit–sharing, etc.)".

Contributor 13 and Contributor 18 both argue that there is a sense of security with appointing a paid financial TPP. Contributor 47, for example, saw the service he was paying for in the same way as any other service he might pay to use, with expectations of a particular quality of service etc.

There is also a level of trust when using the paid service. Contributors highlighted that, as paying customers, they would see themselves being treated properly by the TPPs who needed to retain them as customers. Therefore, they felt that the quality of the service would be dependent on how much contributors would like to pay for the service. Some others suggested that all apps use and sell personal data anyway, so why pay them twice? Those contributors who were using apps to save money were unlikely to forego some of their potential savings in order to pay for a service that would help them save, although paid–for savings apps do exist.

13.6 Ownership of data

Some contributors saw themselves as those who possess their financial data, however others saw the TPPs and banks as "owners" of their data. For instance, Contributor 13 said that she didn't feel as if her data was hers "to begin with". Interestingly, a number of contributors believed that once their data had been shared with TPPs they were no longer owners of their data and no longer in control of it.

> … now I share it, I have shared it, the information, no, nothing is private anymore. It's private for you, I mean for people, surrounding me, but they have my information already, I share it. [Contributor 31, female, App07S User]

This highlights the ambiguous nature of data ownership and brings into question issues related to rightful ownership and access. For Contributor 47, the concept of owning data was "an impossible fact", but the ability to see what a company has access to is within a consumer's rights:

> Under law you're entitled now to a copy of your data. What you choose to do with that copy is your own right. What somebody chooses to do with their copy is set by the terms and conditions. Neither of you actually own it. You have a series of rights associated to a series of copies. [Contributor 47, male, App11K User]

The fact that there is also no limit on what data a company holds highlights the uncontrollable nature of data. Yet, the distinction between owning and controlling financial data, which is intangible, compared to owning and controlling cash, is also made apparent in Contributor 47's interview. In discussing what his motivations were for using the TPP's service, he explains that "having the ability to control cash very tightly and very closely is just brilliant". This is a feeling echoed by Contributor 1:

> I just want to make sure that at least my money is not touched anywhere. Right now, I don't really care about them seeing my transactions. It's really

more of them not getting any of the money. [Contributor 1, female, App10S User]

This is explored further in a dialogue with Contributor 11 (male, App05B User):

> Interviewer: Right. So, broad question, who owns your personal and financial data?
>
> Contributor 11: Owns? Me, I own it. But all the others, they all have access to it. I don't think they own it, I think I'm the only one that owns it. The Information Commissioner's Office would probably be able to clarify that, but I don't know. I'm assuming that I'm the owner and they're just using it.
>
> Interviewer: And who do you think is the rightful owner? Just you?
>
> Contributor 11: I think I am, yes.
>
> Interviewer: Okay.
>
> Contributor 11: There's always a 'but', though. But, if I've signed it away by signing terms and conditions, maybe they are legal owners as well. I don't know.

Doubt is peppered through this brief dialogue with Contributor 11. He separates legal ownership with the ideal ownership of the data; whereby the legal owners could be the TPPs, but the 'rightful' owner is himself. There is a mention of a regulatory body, but the specificities of what that body does for financial data is vague.

13.7 Revocation of consent

The thought of ownership of data also made contributors think about what happens to their data once their consent is revoked.

For many contributors, although they believed they could revoke their consent by stopping using the app these same contributors felt that the app would still have access to all the historical data that it collected about them whilst they were using it. Contributor 27 felt that it was a "one–way street" and once you had said yes and had provided them with your information, the TPP would always have access to that data. She adds:

> If it's the data that was previously there, then yes, the consent is there, because of when you did agree. I feel that once I delete it, it means that my consent is no longer there. It was from that time period, so whatever they had within the time period; they have my consent. [Contributor 27, female, App03B]

Similar assumptions about what happens in terms of data retention if the customer withdraws consent are found in the mixed–application focus group:

> In terms of passwords, I'd expect them to delete it, but in terms of the numerical data, I probably wouldn't expect them to delete it because it is numbers … that aren't really going to correlate to anything except to their means, doesn't really affect me too much, but as long as my passwords are deleted that's fine. [Contributor 36, male, App07S User]

Understanding both how to withdraw consent and whether data has been deleted are important pieces of the same puzzle. As users and early adopters of TPPs, many contributors in studies 2 and 3 demonstrate base–level of knowledge about their data and what happens with their data. However, there is still much uncertainty and gaps in terms of their factual knowledge of what happens, in reality, once their consent is revoked. Frequently, contributors inferred an implicit responsibility on TPPs in relation to the data that the TPPs have about them. Furthermore, as can be seen from the previous quotation, some contributors seem unaware of the implications of revoking consent to process their data and whether this meant that the firm could still extract value from the data obtained before they revoked their consent.

Study 1 also explored the situation where a participant changed their mind and no longer agreed to the terms and conditions (of a non–financial data) app or service. 77.4% would uninstall the application on their device and 73.1% claimed they would permanently delete their account, with 19.9% suggesting they would contact Customer Support.

Contacting customer support was not, however, considered a realistic option by some contributors in studies 2 and 3:

> Call and try to talk to somebody? Short answer, no. Long answer, I'm sure they are obligated to somehow tell you that, but it would be a nightmare probably to get the right person on the phone or whatever it took. [Contributor 13, female, App03B & App08S User]

14 Empirical findings: Regulatory environment

A common reason given for why contributors do not read Ts & Cs was due to the pre–existing assumptions a contributor has before reading the Ts & Cs, including assumptions about the regulatory environment within which the service operated. If these assumptions are incorrect then they will fail to understand what actually happens with their data and how they might be protected. These pre–existing assumptions cloud the contributors' opinion and therefore they compromise the importance and weight of the Ts & Cs. As noted above, these pre–existing assumptions can include behavioural constraints that affect decision making (see section 6.2), as well as a general awareness of the regulatory environment within which the service operates (see section 8.1).

The empirical research revealed how closely assumptions about the effective operation of the data and financial regulatory environment were related to decisions to skim read / ignore terms and conditions. In particular, there was considerable evidence that consumers simply expected the regulatory environment to work smoothly and easily address any issues that might arise, including actions that they had consented to on the basis of what was presented in the terms and conditions. The findings are discussed in more detail below.

14.1 Relationship between Ts & Cs and the regulatory environment

Over half of the research contributors in studies 2 and 3 were aware of the existence of some form of regulation to safeguard their rights in relation to their data. For many, the extent of their awareness of regulation was largely quite general and limited to naming the laws and not the detailed role of the laws and regulations. For example, when discussing what regulations they were aware of, Contributor 16 (male, App05B User) said, "I don't know what it's called, but I think there is like a regulation around protection of financial data". Similarly, when asked the same question, Contributor 23 added the following:

> I think there's actually an act of legislation, isn't there a data privacy act, so I think there's probably, they have to abide by that and I'm sure there's provisions from the FCA and other regulators that make sure that they keep customers data secure and safe. [Contributor 23, male, App02B User]

Despite the distinctive profile of contributors (educated to degree–level, some involved in financial or information technologies), only a small number of contributors were very aware of the specificities of data protection laws and regulations and the level of protection that they actually give in relation to their data. For example, a number of contributors spoke explicitly about the Data Protection Act or the GDPR. Contributor 17 (female, App02B User) said that data protection law is "quite specific about the fact that you can't, you mustn't keep data once it's no longer needed". Contributor 28 (male, App05B User) reported that as a result of the Act, an app isn't "allowed to use my name, basically any information that will be

able to link the data they have to me personally. I know it has to be anonymised" and Contributor 10 (male, App05B User) suggested "the Data Protection Act and the new stuff {GDPR}[4] will give the app the right to go in … and access a copy of everything that they have. I don't know whether it will allow me to make them delete it". A related concern was about how effective any regulation would be. For example, Contributor 4 (female, App01B user) mentioned that she thought that "regulation doesn't really have much say. I mean, on paper or like as an overview is like a company can look like very decent and like protecting one's data. But you never know what's happening".

In fact, when contributors were asked 'What does Regulation mean?' the answer, 'to protect', was frequently used, although Contributor 11 (Male, App05B User) didn't think it could provide a great deal of protection as it was "fairly weak".

> I know that the tax preparation stuff probably has tighter regulations than other random financial services apps, so that made me have more confidence in using this service but I don't know specifically what regulations are like because there isn't any money tied up in it, so it's not like the FDIC {Federal Deposit Insurance Scheme} where they're on the hook for that money. So I don't really know what it would be. [Contributor 13, female, App03B & App08S User]

Contributor 13 anchored her knowledge in tax regulations, as her knowledge on financial regulation is minimal. She was unaware of any governing body or regulation to protect her financial data. Nevertheless, Contributor 13's response also raises an apparent tension in the context of regulation. Despite there being a plethora of regulation to protect consumers in the event of a data breach, for example, the extent to which consumers have faith in the regulator's ability to protect their financial data is uncertain. A number of contributors expressed the view that regulatory oversight was not developing quickly enough in comparison to the speed of technology.

> I think the technological world that we live in extends beyond the … Or in terms of the production of technological advances and the production of regulation to protect one against those technological advances. So, from that aspect I suppose there is an aspect of vulnerability. [Contributor 19, female, App04F User]

Similarly, Contributor 3 likened the pace of regulation to police officers who are behind the "new drugs on the market" and are unable to keep up with developments. Thus, although there is comfort in knowing that there is a system of checks and balances for insurgent TPPs—which allows users to feel they are more trustworthy because they are monitored by authoritative bodies—this comfort is somewhat superficial.

[4] {} indicates explanations added, not part of the original quotation

14.2 Expectations that the regulatory environment will provide protection

Most contributors chose to ignore Ts & Cs deliberately. The phrase "ignorance is bliss" was common throughout the focus groups and interviews. Contributor 7 (male, App06P User) assumed that the terms and conditions "will be standard and generic to a banking app. It's not like a selling one. I thought it would reflect the FCA regulation and route". Contributor 11 (Male, App05B User) argues that he "pushes {financial and personal data usage} to the back my mind". Without considering the repercussions of how data could be used, Contributor 11 conveys Ts & Cs as "threatening".

This point was also made by Contributor 24 in the following exchange:

> Interviewer: And in your opinion, do existing Ts & Cs help to make informed choices?
>
> Not on these sorts of websites I don't think, because they're pretty standard I think. So, it's a UK financial services website, it's not going to be particularly exotic, put it that way. [Contributor 24, male, App02B User]

This interaction echoes Contributor 20's sentiments regarding Ts & Cs; that they are "bog standard" in nature and are believed to be grounded in a common or shared regulatory environment for data protection and financial services.

Additionally, contributors tended to rely on their knowledge of previous terms and conditions to understand the current Ts & Cs of the TPP. Consequently, they anchored their knowledge into pre–existing Ts & Cs as they cannot comprehend, or become familiar with, what happens to their data. Pre–existing thoughts about Ts & Cs become a barrier to understanding the implications of a new service. This was reiterated in Contributor 30's opinion, expressed after an exercise in the interview and focus groups that allowed contributors to read through the Ts & Cs of their service again (or for the first time).

> Interviewer: I'll ask you just a couple of questions following on from that. After reading the Ts & Cs, how did you find them generally, as you were reading them?
>
> I found them pretty sort of boiler plate Ts & Cs, so didn't find anything unexpected from my looking at them. [Contributor 30, male, App02B User]

Interestingly, some contributors differentiated between the Privacy Policies and Ts & Cs of the service. Those that did found the Privacy Policies to be more important (and potentially more likely to be read) than Ts & Cs.

> I think the privacy policy was probably the first thing I looked at with both of them, because again it's that sort of okay, how are you actually going to be sharing this data? Ts & Cs, glanced through, but again, as with most people, I don't have time read 20 pages. [Contributor 10, male, App05B User]

When many contributors spoke about this aspect they referred to "others" to support their view. They rely on the consensus of those around them. This line of thought is prevalent within Contributor 12's opinion:

> Privacy policy, yes, because I do understand the difference of Ts & Cs and privacy policy, so I do read private policies because I am concerned about how App05B themselves will use my data, so I will read that. Ts & Cs, I know can just be very generic as well and quite vague, but the privacy policy I do pay attention, no matter what I'm signing up with, how that data is going to be used. [Contributor 12, male, App05B User]

This emphasis on the Privacy Policy over the Ts & Cs and the focus about how the data can be used seems to underlie a common concern held by many contributors and highlighted a sense of control or perceived possession over their data.

Thus, although many contributors felt "they really should" take into account Ts & Cs and privacy policies, many did not. Contributor 6 acknowledged the importance of Ts & Cs when reminiscing about her uncle's circumstances.

> For example like my uncle—this is not really related to it—but my uncle went over his limit when he used the {mobile phone} roaming. And he didn't read the Ts & Cs of the company and then he got charged for that. And he was charged like £100—which is like for a seven–day period. [Contributor 6, female, App01B User]

The financial harm suffered by a close relative made her sensitive to the significance of complying to the Ts & Cs of any company. This is especially important as it seems Contributor 6 understands the importance of Ts & Cs through negative enforcement. Unlike Contributor 6, many contributors showed a disconnect between thinking and doing. When asked, they acknowledged the importance of privacy and Ts & Cs, but this rarely translated into reading them.

15 Treating customers fairly

Although data protection regulations are based on principles that seek to treat data subjects fairly when organisations wish to process their data, the term has a specific meaning in the context of the work of the Financial Conduct Authority (FCA). The FCA has three principles that particularly inform the work of the FSCP in relation to the notion of treating customers fairly. These principles are given in Table 9:

6 Customers' interests	A firm must pay due regard to the interests of its customers and treat them fairly.
7 Communications with clients	A firm must pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair and not misleading.
8 Conflicts of interest	A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.

Table 9 The Principles (Financial Conduct Authority 2014)

There is a close relationship between the three principles taken together and the FSCP concerns about consent and the environment within which the giving of consent takes place.

FCA principle 6 Treating Customers Fairly (TCF) requires that any firm regulated by the FCA "must pay due regard to the interests of its customers and treat them fairly". The aim of this principle is to:

- help customers fully understand the features, benefits, risks and costs of the financial products they buy; and
- minimise the sale of unsuitable products by encouraging best practice before, during and after a sale.

The FCA also specifies six "desired outcomes" arising from the principle of ensuring fair treatment of customers:

- Outcome 1: Consumers can be confident they are dealing with firms where the fair treatment of customers is central to the corporate culture.
- Outcome 2: Products and services marketed and sold in the retail market are designed to meet the needs of identified consumer groups and are targeted accordingly.
- Outcome 3: Consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale.
- Outcome 4: Where consumers receive advice, the advice is suitable and takes account of their circumstances.

- Outcome 5: Consumers are provided with products that perform as firms have led them to expect and the associated service is of an acceptable standard and as they have been led to expect.
- Outcome 6: Consumers do not face unreasonable post–sale barriers imposed by firms to change product, switch provider, submit a claim or make a complaint. (Financial Conduct Authority 2015).

The desired outcomes encompass activities throughout the customer journey and experience. Treating customers fairly includes giving them general confidence in an organisation's integrity and continues through the purchase of a financial product and on to any post–purchase relationship with the firm. The principles aim to improve the conduct of financial institutions as well as public trust in the industry.

For example, Outcome 1 requires organisations to act in such a way that reflects responsibility of customers' interests and fair treatment as core to the entire organisation. Customer privacy and data protection, as well as instilling trust in handling and safeguarding of customer data, should be some of the principles relevant to the fair treatment of customers.

As a consequence, some companies explicitly state that their Data Protection Policies reflect their approach to adhering to the FCA principles for TCF and ensuring the outcomes—see, for examples, the Inter–Credit International (2018) and CCLA (2015) Treating Customers Fairly policies.

Three of the FCA outcomes are particularly relevant in the context of this study. The research has highlighted concerns with both the content and understanding of privacy policies and terms and conditions. The general lack of clarity about data–gathering, –storing, –sharing and –utilisation could be seen to be in conflict with outcome 3 ("consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale") and outcome 5 ("Consumers are provided with products that perform as firms have led them to expect"). This lack of clarity could also be seen to be in conflict with outcome 1, which expects fair treatment of customers to be central to the corporate culture.

These issues also relate closely to FCA principles 7 and 8 and they reveal some of the "hidden" ways in which customers might experience unfair treatment or even not realise its existence.

Although firms that want to access customer financial data through Open Banking need to be authorised and appear on the FCA Register, they are regulated via the Payment Service Regulations rather than the Financial Services and Markets Act 2000 (which defines the work and purpose of the FCA). The Payment Service Regulations specify conditions that must be satisfied for a firm to receive authorisation as a payment institution but not all these firms are also subject to the requirement to satisfy the FCA's Treating Customers Fairly principles.

16 Conclusions

In commissioning this research, the FSCP was particularly keen to better understand four key questions:

a. The concept of consumers "owning their own data";

b. The type of consent they have given to the Account Information Service Providers (AISPs) to make use of their data;

c. The terms and conditions of the service they have signed up to (with regard to the consent they have given); and

d. The 'cost'—implicit and explicit—of the service and whether this represents good value for money / data.

The answers to these questions are summarised below.

16.1 What types of consent do consumers give to third–party providers to make use of their data?

Although data protection law including the GDPR requires consent to be freely given, unambiguous and informed, the evidence from the empirical research suggests that this is frequently not the case. Over half of the contributors to study 2 and 3 claimed not to read any terms and conditions for products and services that they sign up for, including the specific services that access their financial data (section 11.1). When the comprehension of privacy policies was explored in study 1, only 7% of participants correctly answered a question about a detail in the policy even after having an opportunity to re–read the policy (section 11.1).

A common explanation given by contributors to studies 2 and 3 was that the privacy policies were full of 'legal jargon' and not written with consumers in mind (section 11.2). Moreover, as found in study 4, not all the information a consumer might require would necessarily be found in the privacy policy (section 10).

In the absence of an ability or willingness to consent to the processing as described in the privacy notice, many respondents drew on alternative support when assessing whether or not to provide consent. For a small number of technologically sophisticated early adopters, this would involve detailed research into the operation of the service (section 11.3) and might also include trials with less sensitive accounts (section 13.1). Others would rely on proxy assurances such as adverts, reviews on app stores or the recommendations of friends and colleagues (section 12).

For some, consent would be given regardless of what was specified in the terms and conditions because they had already decided to use the app or service. A final approach was to give consent and simply rely on the regulatory environment, including data protection and financial services oversight, if problems arose (section 14.1).

16.2 How well do consumers understand and appreciate the terms and conditions of the service they have signed up and given consent for?

Given the poor comprehension of the basis on which consumers were giving consent, it is perhaps unsurprising that few research contributors fully appreciated the consequences of the terms and conditions they had signed up to.

Whilst contributors generally understood that they were giving consent for the service to access their personal and financial data in order to perform the primary processing that the service was based on, some believed that they hadn't even given consent for that data sharing to take place (section 11.3).

In terms of additional uses of personal and financial data covered in the terms and conditions, there was a general acceptance, or resignation, that, as customers, they would be likely to be subject to personalised marketing messages and associated online tracking (section 13.4). There was far less appreciation of other things the service provider might do with (aggregate) level analysis of their data, or whether the benefits of this aggregation might be shared with consumers or simply improve the profitability of the service provider (section 13.4).

16.3 How do customers understand the concept of "owning their own data"?

The empirical evidence highlights the challenges of this concept. For some contributors personal data and financial data were very different, with different levels of risk associated with each. For others they were all examples of data that were sensitive in light of the risks that would arise if the data were mishandled (section 13.3).

Complications arise around whether the data are shared with, or just accessible to, the third–party provider. Data that are shared, some felt, became even more uncontrollable. This ambiguity about ownership is heightened for contributors who hadn't fully appreciated the implications of the terms and conditions they had agreed to. For example, the Ts & Cs may permit the service provider to undertake statistical analyses on aggregate consumer data. Arguably this resulting aggregate data is as much a product of the service provider, who has created value by doing the analysis, as it is something that should still be owned by the individual customers (section 11.3).

16.4 How do customers understand the implicit and explicit costs of the services they are using and do they think this represents good value for money / data?

Some of the apps and services used by the contributors to studies 2 and 3 were paid for services, whilst others were offered for free. There was a general recognition that services that were not paid for directly were still being paid for indirectly, typically through targeted marketing etc. (section 13.4).

In general, however, there was limited appreciation of other ways in which consumers might be "paying with their data" (section 13.5). A small number of participants had recognised that some free (and paid for) services might be using the data for statistical analysis purposes and selling these insights to generate revenue (section 13.4). Few, if any, fully appreciated the risk that these analytical insights might result in price discrimination or sub–optimal recommendations.

For some services, such as savings apps, it seemed paradoxical to some contributors to pay for the service using money that could, instead, be saved (section 13.5).

16.5 Reconsidering the relationship between terms and conditions and consent

The literature and empirical evidence considered in this study highlights the relational nature of the link between privacy policies of an online service and the customer who is seeking to give consent for that service to access their personal and financial data.

Ensuring that "when consumers consent to share their financial data with a third–party they are able to do so in an informed way and without being subject to behavioural manipulation" requires an understanding of the limitations associated with both the privacy policies and consumers natural behaviours. The research has highlighted the limitations with existing privacy policies and terms and conditions as well as the increasingly common tendency to not bother to read (unhelpful) terms and conditions.

This suggests two related responses. First, it is important that efforts to improve the clarity of terms and conditions continue. There is a need to ensure that the presentation of Ts & Cs addresses the information requirements of customers. They should no longer be seen as just satisfying a legal requirement to notify customers of the legal basis for processing their personal data. Second, there is an urgent need to change consumer attitudes so that Ts & Cs cease to be something that they don't bother to read and instead become a key means by which they learn about what will happen to their personal data. Effective terms and conditions can also provide clear guidance about what protections the regulatory environment provides as well as what decisions the customer is responsible for.

Thus, whilst Table 10 and Table 11 highlight particular issues that should be addressed to improve the consent process, they must be seen in a holistic and relational manner for sustainable improvements.

Privacy Notices issues for consumers	Description	Research evidence
Not clear	Even if read, ordinary consumers struggle to understand the privacy notice	Presented in section 11

Not complete	Some users may not find the information they require to help them decide which service to use	Presented in section 10

Table 10 Limitations of privacy notices

Consumer's issue with Privacy Notices	Description	Research evidence
No choice	For some services, choices may not exist or be realistic	Presented in section 12
Not read	Most consumers have adopted an attitude of not reading Ts & Cs	Presented in section 11.1
Not understood	Even if they are read, Ts & Cs are rarely written with the consumer's needs in mind	Presented in section 11.1
Not appreciated	Frequently, the implications of the Ts & Cs are not spelled out for consumers	Presented in section 11.3
Not relevant	For some consumers, a decision to use the service has already been made and won't be changed by reading the Ts & Cs	Presented in section 12
Not necessary	Some consumers assume that the service is covered by the existing regulatory environment	Presented in section 14.2
Not useful	Some consumers might not appreciate the (potential) usefulness of Ts and Cs and therefore not bother to read them, thus reducing the likelihood that they will come to know their usefulness until it is too	Presented in section 14.1

	late.	

Table 11 Natural consumer behaviour in relation to privacy notices

16.6 Treating customers fairly

As noted above, the FCA principles around treating customers fairly do not necessarily apply to all the firms authorised to access customer financial data through Open Banking. It is helpful, nevertheless, to identify additional evidence from the research that addresses more implicit aspects of the three principles that can be seen to relate to personal data, principles 6, 7 and 8 as these underping the work of the FSCP.

FCA Principle 6 states that a firm must pay due regard to the interests of its customers and treat them fairly. Alongside the findings about consent and terms and conditions, the study also explored behavioural constraints that can affect decision making around consent, the role of individual privacy attitudes on the decision to use particular apps and services and the broader role of the regulatory environment. These are summarised in Table 12.

Literature	Research findings
What is the evidence around behavioural constraints affecting decision making about giving consent?	
Section 6.2 presented examples from the literature that showed how the ability to make informed decisions is often hindered by a variety of factors. Because individuals tend to value short–term rewards over long–term goals, they often click through presentations of a service's terms and conditions in order to obtain the immediate benefits that arise from using an app or service. Research also shows how decision biases like loss aversion and endowment effects can be used to either nudge people toward consent or to dissuade people from acting fully on their privacy rights. These influences may also play a part in the way customers view their data at the point of choosing to engage in a third–party service or product.	The empirical findings (section 12) provide examples of how these behavioural constraints affect the consent process. For example, some contributors found the service proposition so appealing that they didn't bother to examine the terms and conditions of the service before using it. Others, who found that they were unable to rely on established reputations, were able to research the service or take advantage of free trial periods to determine whether to use the service on a regular basis. Another strategy used by some research contributors was to rely on crowdsourced evaluations such as reviews found on app stores.
How do individual privacy attitudes, knowledge, awareness and risk appetites affect the decision to take up apps and services?	

The literature reviewed in section 7.1 helps explain the factors that affect an individual's privacy attitudes and relationship between espoused privacy attitudes and behaviours. Thus, those who value their privacy more are more likely to be sensitive to the risks of disclosing personal data online. Other individual factors affecting the disclosure of personal data include the trust relationship between the discloser and recipient.	The research contributors provided many examples of their varying privacy attitudes and associated risk appetites in relation to sharing their financial data with third party providers, discussed in section 13.1. Some revealed their attitudes by only providing access to some of their accounts. Others demonstrated a quite nuanced account of the perceived sensitivity of different kinds of data, with some data types being considered more sensitive in terms of privacy than others.
What is the role of an effective regulatory environment?	
The regulatory environment for the apps and services covered by the research includes the existence of appropriate data protection laws coupled with effective, independent oversight. It also includes the Financial Conduct Authority. The regulatory environment is particularly important for addressing existing concerns around the handling of data (presented in section 8.1). The General Data Protection Regulation (GDPR) that enters into application on 25 May 2018 is intended to strengthen the data protection environment, especially around consent, see section 8.2.	Over half of the research contributors in studies 2 and 3 were aware of the existence of some form of regulation to safeguard their data rights, although this knowledge was often fairly general and may have been a by–product of the fact that many contributors worked in the technology industry. This general sense that the regulatory environment would provide protection was used by some contributors to justify their decision to ignore the terms and conditions of the apps and services they were using, see section 14 .

Table 12 Additional evidence on TCF Principle 6

Customer interests include having clear demarcations about what elements of data processing can be reasonably assumed to be covered by the terms and conditions of the service being used and which choices they need to be responsible for as this can help minimise the sale of unsuitable products. The best interests of customers will also be affected by their individual attitudes to privacy and risk as well as the extent to which other behavioural factors affect their decision–making practices. At the very least, these items need clearer exposition when the benefits and risks of using a particular service are introduced.

FCA Principle 7 states that a firm must pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair and not misleading. The discussion in sections 16.2 to 16.5 about improving the

presentation and understanding of terms and conditions can be complemented by consideration of information that underpins other aspects of the decision to use a particular app or service.

Literature	Research findings
What other factors affect how customers choose to use particular apps and services?	
The literature discussed in section 6.3 highlighted the role of the customer experience in influencing the choice of apps and services, noting that unnecessary and unexpected delays in the online experience can affect customer trust and the long–term relationship with the service provider. Whilst "positive frictions" in the user journey may be valuable, excessive delay can be problematic. As discussed in section 7.2 they may disrupt adoption by customers who have already decided they want to use a convenient app or service.	In studies 2 and 3 contributors expressed a range of concerns about sharing personal and financial data, including relative risks associated with different data types. Thus how the service asked for access to this data affected perceptions and take up of the service, see sections 13.2 and 13.3. These perceptions also affected the extent to which customers were more forgiving in terms of what additional uses of the data might be undertaken by the TPP, see section 13.4.
How effective are the existing revocation practices?	
The ability to revoke consent is an important additional requirement under GDPR, see section 5.3 and the option to do so needs to be clearly explained to customers.	In studies 2 and 3 discussion of the effects of revocation of consent typically arose out of discussions about the ownership of the data, although many contributors were uncertain as to what happens to the data that has already been shared once consent is revoked, see section 13.7.

Table 13 Additional evidence on TCF Principle 7

In addition to the general improvement in terms and conditions, the implication of treating customers fairly in terms of their information needs includes balancing appropriate information posting and other positive frictions with the need for a well–designed user journey. The introduction of the GDPR introduces a new element around the ability to easily revoke consent. This additional requirement is not widely found in existing policies and only emerged in the research study in relation to discussions about data ownership.

FCA Principle 8 is around conflicts of interest. It states that a firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client. In the context of open banking and related financial

services, the issue concerns the additional uses a TPP might make of the customer's financial data and the extent to which the customer understands that they are agreeing to this additional processing. This is particularly important when these additional uses might not benefit the consumers directly.

Research findings
What are customer views on other, secondary uses of data?
Section 13.4 describes the extent to which the research contributors perceived secondary uses of data to be reasonable. There was a general recognition that the TPPs would do things with their data beyond providing the service the customer had signed up for, although most understood this to be little more than receiving targeted advertisements. Research contributors often sought greater clarity about how the TPPs were benefitting financially from these other uses of data, such as selling aggregated statistical profiles to other companies. Most participants expressed unhappiness with any uses of their data that would not directly benefit them and the services provided by the TTPs.
What are consumer attitudes to paying for financial services?
Customer attitudes to paying (explicitly) for services was discussed in section 13.5. For some, the availability of a "free" service was a key factor. Others, however, recognised that if the service was not paid for explicitly, the TPP would be extracting value in other ways. Thus, some explicitly chose to pay for the service to avoid, for example, targeted advertising. Others, however, resented the idea of possibly paying twice: once for the service and once in terms of their data. Those customers who did pay for their service often felt they could expect a higher level of service from the TPP than those customers who were not paying.
How is ownership of data understood?
The ambiguous nature of data ownership was discussed in section 13.6 with some contributors distinguishing between ownership, simple access to the data and control over what could be done with the data. A further dimension relates to the additional value that a service provider can add to the consumer data.

Table 14 Additional evidence on TCF Principle 8

With data playing a central role in open banking, consideration of Principle 8 highlights a number of areas where potential conflicts of interest around the use of personal data can arise. In particular, to avoid the perception of conflicts of interest, third–party providers need to make clear what the regulatory environment permits and does not permit in terms of secondary uses of data, what the consumer is paying for when using a paid–for service and what alternative costs exist when using a free service as well as a better understanding of how data ownership is managed across the data shared by the customer and any value–added analysis undertaken by the service provider.

17 Methodology Appendix

17.1 Research design and methods for studies 1, 2 and 3

This appendix provides more detail about the mixed methods research design adopted for the project.

Participants for Study 1 were recruited online through the LSE Behavioural Research Lab (BRL). A description of the study was sent out to members of the BRL participant pool inviting them to participate in the study. To be eligible for the study, participants had to be over 18, own a personal smartphone and have not had exposure to open banking mobile applications. Participants were selected using stratified sampling. Including the pilot stutdy, 206 participants agreed to take part in the study. Of those, 15 individuals cancelled, leaving a total of 191 participants who completed the survey.

The average age of participants was 23 years (SD=5.00) with ages ranging from 18 to 58 years. Of the respondents, 69% were females and 31% were males.

Following an examination of existing published literature on consent, privacy and smartphone usage (Buchanan et al. 2007; Chin et al. 2012; Joinson et al. 2010; Malhotra et al. 2004; Xu et al. 2008) a computerized survey was developed using Qualtrics Software.

The survey consisted of basic demographic questions such as family and personal income social class and employment. Novel questions about online companies and their access to user data were also created to garner an understanding of the general attitude towards reading the terms and conditions of online service providers and the comprehension of how one's data is used by these companies. The survey also included items about participant responses to breaches in these statements and fears about online companies using personal data.

Additionally, items were drawn from the literature and adapted for use regarding mobile applications. Seven items of computer-efficacy measures, developed by Compeau and Higgins (1995) were adapted with wordings to specifically capture "mobile efficacy" and included in the survey. A 7–point Likert scale (1—not at all confident to 7—totally confident) was adapted and used to measure participant's competence in using mobile applications.

Three items of disposition to value privacy measures, adapted from Malhorta et al. (2004) were used to measure perceived privacy risks again rated on a 7–point Likert scale (1—strongly disagree to 7—strongly agree).

Privacy control was measured with 5 items also rated on a 7–point Likert scale. Four of the items were taken directly from Xu et al. (2008) and one privacy awareness measure, taken from Malhotra et al. (2004), were used as an indicator of one's awareness of the agents in control of their data.

Privacy concern was measured using 4 items also taken from Malhotra et al. (2004) and an additional item was created in order to emphasise and measure the level of trust individuals have towards online data sharing companies.

A timed exercise, which required participants to read the terms and conditions of a fictional online social media company, was created to measure the length of time that individuals spend reading the terms and conditions. This was followed by a comprehension task consisting of three questions that tested participant's understanding of what they just read. The text provided was an adaptation of Facebook's online terms and conditions, but was shortened to allow for completion of the rest of the survey.

The survey also explored participant's reactions to different avenues of consent, including whether the tendency to provide consent was affected by peer influence and whether consent for the use of online services depended on the type of data that was requested. The following scenarios were implemented in the survey:

Opt–out pre–ticked box scenario. One feature of the forthcoming General Data Protection Regulation is the decision to ban of the use of pre–ticked boxes as a means of obtaining consent and arose in response to the controversy surrounding the influence of this strategy in engineering the consent decisions of consumers (BBC News 2011). Questions surrounding participants' thoughts of the practice were included, particularly examining the helpfulness of pre–ticked boxes and ratings of caution were included in the survey.

Attitudes towards Health Records Data Sharing. Participants were given a hypothetical scenario that detailed a family member wanting to install a mobile application to track their health and were asked how they would advise them to gather information the applications health–records sharing policy and rated the level of caution towards this type of application on a 5–point Likert scale from 1—extremely cautious to 5—not at all cautious.

Attitudes towards financial data sharing. Participants were given a hypothetical scenario detailing their interest in a mobile application that tracks their spending. They were then asked to identify their initial reaction towards its request of access to their financial history, as mentioned in its terms and conditions, from a choice of options. They also rated their level of caution towards this application on a 5–point Likert scale from 1—extremely cautious to 5—not at all cautious. This was followed by questions about sharing financial data and what would make them feel comfortable with sharing data.

Open Banking Information. Information about Open Banking as a solution to combat the lack of competition between banks was introduced to the participants, followed by questions that focused on their reaction to the legislation, their concerns and positive remarks.

A pre–test of the survey was conducted with 10 people, including academics and research assistants at the LSE. Respondents provided feedback on the wording of questions and the overall structure of the questionnaire. A copy of the final survey is available at https://lse.eu.qualtrics.com/jfe/form/SV_3gz4ftWpimiKcuN.

The BRL has 20 computer terminals available for study participants. A pilot study was conducted in 2 sessions on 18 October 2017 to test the time taken to complete the survey and to gain additional feedback. It was found that the average

time of completion was 10 minutes, creating scope to add more questions and scenarios relevant to the research question and this was incorporated into the revised instrument. The main survey was completed in 11 30–minute sessions on 20 October 2017.

On arrival at the BRL, participants were greeted and were reminded that they were to complete a survey lasting no longer than 30 minutes. Once the study commenced participants were shown an information page informing them about the survey. Participants were also informed of their right to withdraw at any point during the study, should they wish their data to be excluded from the analysis. At the end of the study a debrief page was displayed to participants detailing the premise of the study in relation to consent giving for online data applications. No participants withdrew from the study.

The survey took an average 20 minutes to complete and participants were paid £5 for their participation.

Studies 2 and 3 consisted of interviews (Study 2) and focus groups (Study 3). In total 39 individual interviews were undertaken: 18 Females and 21 Males. Contributors were aged between 18 and 70 years. 21 participants were British and 26 had resided in the UK over 5 years. 27 participants were students, 20 participants worked full–time, one participant worked part–time and one participant was retired. All participants had attained A–levels or equivalent and the majority of participants had attained at least an Undergraduate Degree.

Scheduling problems meant that it was only possible to arrange two focus groups with 11 participants in total. The first focus group was made up of three participants: two females, who were both users of App05B and one male, who was a user of App07S. The three participants were current Master's students, classified themselves as lower–middle class and worked part–time. They had sufficient characteristics in common for the group not to feel threatened or intimidated. Bringing together a mixed, yet aligned group allowed for the exploration of different perspectives, and encouraged debate. This is a highly useful technique for an under–researched area.

In contrast, the second focus group was made up of eight participants, who were all of ethnic and national Chinese identity. They were all users of App09F and were all LSE Master's students. The decision to hold a largely exogenous and issue homogenous focus group was decided to see how the dimension of the focus group related to the focus group topic, which in this case was how users interacted with App09F, a leading Chinese–based financial services app.

Unlike participants in Study 1, participants in Studies 2 and 3 were existing users of third–party financial apps and a qualitative methodological framework was used to better understand their attitudes to sharing financial data with these third–party providers.

The use of qualitative data in interviews and focus groups provided some beneficial insights. First, it enabled insights into ideas which may have not been considered before. Our understandings, as researchers, provide limited perspectives

on what it means to share financial data with third parties. Good qualitative research harbours an element of surprise. The essence of surprise cannot be achieved solely through quantitative research. Therefore, there is room for an innovative scope, which may not have been discussed by researchers prior to the collection of data.

Second, participants could discuss and debate ideas existing within themselves. Many times, participants espoused many competing—sometimes even conflicting—ideologies, often known as 'Cognitive Polyphasia' or 'Cognitive Dissonance' (Jovchelovitch 2008). Through qualitative data, it is possible to discover conflicting opinions about sharing financial data held by the same person and discover them across people.

Third, the language participants use tells a lot about their sense–making processes. It helps to understand what their understanding is of financial data, security, consent and ownership of data. Rather than presupposing their views, most of the Research Questions began with a 'How' or 'To what extent'.

One–on–one interviews facilitate a relaxed environment for the participant to speak about a potentially sensitive topic: their finances. The interview enables a strong rapport between participant and researcher. Furthermore, the data collected through interviews provide a 'thick description' related to a topic. The ideas are given contexts and issues surrounding the topic are discussed. The answers to questions are in–depth, which facilitate points being explained fully.

In contrast, focus groups allow for group dynamics. As Whitley et al. (2012) suggest, answers to questions may facilitate debates around a set topic. Participants then have the power and the ability to interact with these debates. Moreover, these participants are set in pre–defined groups whereby they are all share their financial data with third party apps and services. This relaxes the environment, as a common group identity is achieved. However, it would be wrong to argue that all users have the same perspective and experience. A plurality of perspectives is studied in focus groups. Therefore, we are able to assess where consensus and a lack of consensus lies in understanding consent to sharing financial data.

Before the interview or focus groups, participants were asked to read an Information Sheet and complete an Informed Consent Form and Demographic Information Form. The interview or focus group then began following the structure outlined in the topic guide. When the activity had finished, participants received a debrief and were paid £20 for their participation.

Topics guides were produced (and updated) to explore the identified project research questions. Different versions of the topic guides were produced for the focus groups and interviews respectively. Similarly, as interviewees had specified the services they used in advance, it was possible to tailor the questions accordingly, e.g. asking different questions to users of paid–for services than those asked of users of free services. The topic guides comprised of a warm–up, questions, exercises and a cool down. The warm–up was needed to ensure that participants became

comfortable with being asked questions relating to financial data and consent. The exercises enabled there to be engagement between the researchers and participants.

All interviews and focus groups were recorded (audio and, in some cases, video). Many took place in rooms at LSE but others took place over the telephone or skype. All interviews and focus group recordings were transcribed by a professional transcription service.

After the recordings were transcribed, the data was anonymised and password protected. The data was coded in ATLAS.ti 7.5.16. A hybrid approach to thematic analysis was adopted, with the research questions comprising the overarching themes and further divided into the individual codes derived from the data which provided the suitable response.

All empirical aspects of the project were approved by Behavioural Research Laboratory Ethical scrutiny process and the self–certification procedures for LSE's Research Ethics Committee in 2017. These processes included providing informed consent forms, debrief documents and a data management plan to address the storage of empirical results including survey results and transcripts. Participation in the research was voluntary and this was emphasised in the study promotion and during the process. Consent was obtained prior to the data collection from participants' ensuring they were informed about how data would be collected, analysed and disseminated. They were told that they could withdraw from the study at any time without consequence.

17.2 Insights and limitations

Interviews and focus groups were extremely beneficial to the study at hand. They helped to provide a deeper level of understanding about the consent participants had given to TPPs, what they had given consent to and how they felt about the services. The interviews and focus groups also explored their trust in the TPP (and other partners in chain). It allowed an exploration of their views and experiences in an open and frank environment. As those interviewed were already users of TPPs, it also provided greater insight as to how their experiences, beliefs and motivations could relate to the later and potential experiences that may face consumers in light of Open Banking.

This could be seen as a limitation of the study. This pool of participants were early adopters of TPPs and had consented to granting them access to their data through screen scraping. As a result it was likely that their level of knowledge on data related issues would be higher than average. Additionally, most of the participants were made up of individuals who fell into a higher socio–economic and educational background. Considering, however, that the findings point towards consent being not very well informed, it can be argued that such results would also apply to a larger set of the population. Nevertheless, future research could explore how informed consent is given by contributors of all socio-economic levels and once TPPs become more common.

17.3 Interview topic guide

Present Information Sheet, followed by Consent Form (printed) and demographic information (iPad)

Set up Video/Voice Recorder

Hi (name), thank you for attending this interview.
My name is (interviewer) and I will be conducting this interview.

This research project (funded by the Financial Services Consumer Panel - "An independent voice for consumers of financial services") is looking to interview people who use third party mobile phone apps and websites that interact with their banking data to manage their personal finances and savings as part of Open Banking.

As part of this interview, you will be asked questions relating to how your financial and personal data is used.

This information will be used for advising the Financial Services Consumer Panel. When this discussion is typed up, data will be stripped of names. Nothing said will be related back to you. This interview will be video / voice–recorded for transcription and analysis purposes.

You have the right to leave this interview, skip a question, stop and take a break.

Do you have any questions for me to begin with?

Warm Up + understanding why they use this / these apps(s)

What apps or websites do you use to help manage your personal finances and savings?

In what way does this service you are receiving from the app differ from what your bank offers?

How do you benefit from this service?

How did you come to the decision to use such financial app for managing your money? What were your motivations?
a. Did the adverts for (name of app) have an influence over your decision making for joining the app?

b. Did somebody recommend you this app?
c. What other factors influenced your decision to use (name/s of app)?

Are you someone who is open about their finances, say to
a) family?
b) friends?
c) work–colleagues?

How did (this app) gain your trust to share your financial data?
a. PROBE: from the company, from word of mouth, friends etc.

Did you compare apps offering similar services? If so, why did you choose to use this one? Can you tell me what criteria did you use to compare?

How long have you been using this app?

How has your experience been so far with this app?

Was their consent informed? – Do they read Ts & Cs and privacy policies?

What information in the app/website did your read, if any, to take your decision to use it? Did you look for details or did you just decide to give it a try? Why?

What was the most important factor that helped you to make this decision?

Do you generally read carefully the terms and conditions and privacy policies before clicking "accept" when signing up to online services, or social media? Why?
a. As an example, did you read the privacy policy on your bank's annual privacy notice when you received it in the post, or on the website?
b. If you have a social media account, such as Facebook, did you read the terms and conditions when signing up?

We know that many people do not read the Ts & Cs before signing up. We were wondering if you remember reading the Ts & Cs and privacy policy of (name of the app) when signing up?
a. YES: If so, how did you find them in general?
i. Were they clear and concise?
ii. What do you think about the language used in the terms and conditions and privacy policies in this app?
iii. Did you find them reassuring? Or did you find any surprising, concerning or unexpected terms and conditions and privacy policies? Or any reference to uses of your data that you don't particularly like?
If so, why did you accept the Ts & Cs anyway (if they were concerning)?

b. NO: If not, why didn't you read them?
i. Did you assume they would be overly complex / long?
ii. Did you assume they would not be informative? Did you think there wouldn't be any useful / surprising / concerning information?
iii. Did you assume that reading Ts & Cs would not make you change your decision to use the app? Why? (You trust it, you have no other choice than accepting the Ts & Cs …).

In your opinion, do existing terms and conditions help you to make informed choices? Why / Why not?

Do you have any views or suggestions in terms of how to improve them? What wording and content would you prefer to see in an ideal terms and conditions statement?

Views & concerns on privacy and data sharing, and their current practices
What sort of social media do you use? Do you usually share personal information on social media? What sort of information?

Is privacy important to you? In what sense?

When you use let's say Facebook or Google, do you know if they collect data? What sort of data?

Do you know what happens to the data that you have shared, let's say, with Facebook or Google, or any other online service that you have used?
a. Do you know what is the value of the data that let's say Google or Facebook collects? Do you know if they benefit somehow from your data and the data of other users? How exactly?
b. Do you know if they share or sell your data with other parties? For what purposes? Is this legal?
c. What is your view about online service providers storing and selling data to third parties?
d. Do you have any concerns about how your data might be used? (PROBE: if they refer to hacking, security issues, etc., ask: and do you have any concern about how your data might be used legally?)

To what extent do you think there is a difference between consenting to sharing personal and financial data?
a. For example, if you share data on Facebook how is that different to using (the app)

Was their consent informed? – Did they understand the Ts & Cs? Do they understand the specific uses of data by the app?

Different apps might use and share data differently. We are interested in understanding the specific uses of your data by the app you use. We have experienced that some people don't necessarily know how their data is used, but we want to understand what your perception is. For instance…

How do you think the app uses your data? How else do you think it can be used?

How do you feel about consenting to sharing your personal and financial data with this app?

What do you think can happen to your data once you consent to share it with this app?

Have you thought about what kind of data is stored by the app?

What rights do you think the app has to use your data?

Do you think there is some data the app has access to which you're unaware of?

How long do you think the app has access to your data?

How do you think the app benefits from providing you with this service? / How do they make money? (Prompt: Targeted advertising, new products, selling data)

Are you aware as to how specifically your data might be used in the future by (this app) or other parties? (PROBE: personal data vs financial data)

Do you think your data is valuable? In what sense? Do you know or could you imagine how your data might be used by (this app) or by others?

Do you know if (this app) shares your data with or sells your data to other parties / organisations?

If this or a similar app were to share or sell your personal and financial data to third parties, do you know for what purposes these third parties might use your data? If you don't know, what is your guess? (PROBE: personal data vs financial data)

If this app were to share or sell your personal or financial data to third parties, do you know how your data could be aggregated with other data sets and with what purposes or consequences?

Do you have any concerns over how your data might be used by your app or other parties?

Do you know if you have the right to access and correct the data that they have collected from you?

Who owns your personal and financial data? And who should own it?

Do you have control over your data? Do you know if you have the legal right to exert control over your data? In what sense? How?

Do you know if you have the right to access, inspect, and correct your personal data that they have collected?

If you decide to stop using this app, what are the steps you will take?

Do you know if and how you can revoke your consent to the Ts & Cs that you agreed to? Or how you can withdraw? Will your data be erased by the app and any other organisation that might have stored / used your data?

How can you check that this has been done and your data has been deleted?

Are you concerned about possible data breaches (hacking, fraud, stolen / lost data)?

What could the consequences be of a data breach? That is, can you imagine how fraudsters could use your personal or financial data? For what purposes?

If something goes wrong with your financial data (fraud, hacking & stolen data), who do you think has responsibility? What steps would you follow to find a solution? Who would you contact?

Are you aware / have you heard of any regulations that protect your financial data?

What do you think regulation does?

To what extent do you think regulation is able to protect you from misuse of your financial data?

Do you know the extent to which current regulation protects your rights in terms of data privacy and control over your data?

You shared your data with this app. Is it because you think is in good hands because you trust the company? Because you believe regulation is protecting you?

Or you are not very much concerned about how your data might be used by the app or third parties other than the app?

Is consent freely given?
I am not saying that this is the case, but how would you feel if you realised that your data serves to other companies to provide targeted marketing, for instance advertising different products or different prices to different costumers?

If you had the opportunity to decide how your data is being used, what would be a fair use of your data be.
(*GET PARTICIPANTS TO DISCUSS THEM ONE BY ONE*)
1) improving services of the app;
2) offering new products;
3) selling the data to third parties;
4) selling the data to third parties so that they can offer new and improved services or products;
5) selling the data to third parties for targeted advertising;
6) selling the data to third parties to be used for differentiation marketing strategies (i.e. different products or prices to different costumers);
7) selling the data to third parties which then can aggregate this data with other data sets to gain further insights on you.

If you were (this app) how would you make sure clients are informed of how they share their financial data? What measures would you take to gain your clients' trust?

Would you prefer to pay for the service that does not share your data?

How much would you be willing to spend to protect financial data from being sold in the future?

Having discussed your perception about how data is being used by the app and third parties, we would like you to read again the Ts & Cs and see if there is any new information about it that you haven´t noticed before (interviewer shows Ts & Cs to participant).

a. After reading these terms and conditions, how did you find them?
b. Have you noticed any new information about how your data is being used?
c. Do you think the terms and conditions are clear about who the partners are?

Cool Down
Would you recommend (this app) to friends and family?

Have you heard about 'open–banking'?

(In early 2018, Open Banking will be launched in the UK. This is an initiative which enables personal customers and small businesses to share their data securely with other banks and with third parties, allowing them to compare financial products)

What do you think about this initiative?

Is there anything else you would like to add or any concluding comments?

Debrief sheet
Switch off recordings
Guide participant to payment desk

18 References

Accenture (2017). Accenture Research Finds Lack of Trust in Third-Party Providers Creates Major Opportunity for Banks as Open Banking Set to Roll Out Across Europe, (available at https://accntu.re/2fBLKj4).

Acquisti, A., and Grossklags, J. (2004). Privacy Attitudes and Privacy Behavior, in *Economics of Information Security* , Springer, Boston, MA, 165–178 (available at https://link.springer.com/chapter/10.1007/1-4020-8090-5_13).

Akamai (2017). Akamai Online Retail Performance Report, (available at https://www.akamai.com/uk/en/about/news/press/2017-press/akamai-releases-spring-2017-state-of-online-retail-performance-report.jsp).

Alcorn, W., Frichot, C., and Orru, M. (2014). *The Browser Hacker's Handbook*, Wiley Indiana.

Aldemore Bank (2017). Less than one in ten UK SME bosses understand new data protection regulations, (available at https://www.aldermore.co.uk/about-us/newsroom/2017/09/less-than-one-in-ten-uk-sme-bosses-understand-new-data-protection-regulations/).

Awad, N. F., and Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization, *MIS Quarterly* 30(1), 13–28.

Barocas, S., and Nissenbaum, H. (2009). On notice: The trouble with notice and consent, Presented at the Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information, Cambridge, MA (available at http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf).

BBC News (2011). EU bans pre-ticked website boxes, (available at http://www.bbc.co.uk/news/world-europe-15260748).

Bechmann, A. (2014). Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook, *Journal of Media Business Studies* 11(1), 21–38.

Biddle, S. (2017). Stop Using Unroll.me, Right Now. It Sold Your Data to Uber., *The Intercept* (available at https://theintercept.com/2017/04/24/stop-using-unroll-me-right-now-it-sold-your-data-to-uber/).

Birch, D. (2017). Open Banking Revolution, (available at http://www.chyp.com/open-banking-revolution/).

Borghi, M., Ferretti, F., and Karapapa, S. (2013). Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK, *International Journal of Law and Information Technology* 21(2), 109–153.

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).

Buchanan, T., Paine, C., Joinson, A. N., and Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet, *Journal of the American Society for Information Science and Technology* 58(2), 157–165.

Carey, R., and Burkell, J. (2009). A heuristics approach to understanding privacy-protecting behaviors in digital social environments, in *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* I. Kerr, V. Steeves, and C. Lucock (eds.), Oxford University Press Oxford, 65–82 (available at http://idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_01.pdf).

Cate, F. H., Cullen, P., and Mayer-Schönberger, V. (2013). Data protection principles for the 21st Century, (available at http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf).

CCLA (2015). Treating customers fairly policy, (available at https://www.ccla.co.uk/our-policies/treating-customers-fairly-policy).

Chin, E., Felt, A. P., Sekar, V., and Wagner, D. (2012). Measuring User Confidence in Smartphone Security and Privacy, *Proceedings of the Eighth Symposium on Usable Privacy and Security* , 1:1–1:16.

Compeau, D. R., and Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test, *MIS Quarterly* 19(2), 189–211.

Connington, J., and Murray, A. (2018). Open banking: how to keep your data safe and avoid being scammed, *Daily Telegraph* (available at http://www.telegraph.co.uk/personal-banking/current-accounts/open-banking-keep-data-safe-avoid-scammed/amp/).

Curren, L., and Kaye, J. (2010). Revoking consent: A "blind spot" in data protection law?, *Computer Law & Security Review* 26(3), 273–283.

Davidson, S. (2017). How to keep your money and identity safe after Open Banking: Comments, *This is Money* (available at http://www.thisismoney.co.uk/~/article-4944932/index.html).

Davies, S. G. (2014). A crisis of accountability: A global analysis of the impact of the Snowden revelations, *The Privacy Surgeon* (available at http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf).

DDCMS (2018). Cyber Security Breaches Survey 2018: Preparations for the new Data Protection Act, *Department for Digital, Culture, Media and Sport* (available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018-preparations-for-the-new-data-protection-act).

Digital Banking Report (2016). 2017 Retail Banking Trends and Predictions, (available at https://www.digitalbankingreport.com/dbr/dbr245/).

Doubleclick (2016). Mobile speed impacts publisher revenue, (available at https://www.doubleclickbygoogle.com/articles/mobile-speed-matters/).

EU (1995). Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, No. L 281, (available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en).

EU (2011). Opinion 15/2011 on the definition of consent, *Article 29 Data Protection Working Party* (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf).

EU (2016). Regulation (EU) 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), No. L 119/34, (available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN).

European Commission (2015). Special Eurobarometer 431: Data protection, (available at http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf).

Facebook Business (2016). Improving Mobile Site Performance, (available at https://en-gb.facebook.com/business/news/improving-mobile-site-performance).

Financial Conduct Authority (2014). PRIN 2.1 The Principles - FCA Handbook, No. Release 23, January 2018, (available at https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html).

Financial Conduct Authority (2015). Fair treatment of customers, (available at https://www.fca.org.uk/firms/fair-treatment-customers).

Finextra Research (2017). Banking on frictionless customer journeys, (available at https://www.finextra.com/blogposting/14328/banking-on-frictionless-customer-journeys).

Greenleaf, G. (2012). Independence of data privacy authorities (Part I): International standards, *Computer Law & Security Review* 28(1), 3–13.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach, *Journal of Management Information Systems* 24(2), 13–42.

Hayer, R. (2017). GDPR compliance – financial services firms are amongst those in the lead, *PWC* (available at http://pwc.blogs.com/fsrr/2017/11/gdpr-compliance-financial-services-firms-are-amongst-those-in-the-lead-.html).

Hedaya, J. (2017). We Can Do Better, *Unroll.me blog* (available at http://blog.unroll.me/we-can-do-better/).

Heidegger, M. (1937). *Being and time* (J. Macquarrie, tran.), Basil Blackwell Oxford.

Heimer, C. A. (2012). Inert facts and the illusion of knowledge: Strategic uses of ignorance in HIV clinics, *Economy and Society* 41(1), 17–41.

Hickey, S. (2018). "Open banking": radical shake-up, or a threat to your private data?, *The Observer* (available at http://www.theguardian.com/money/2018/jan/08/open-banking-bank).

Hill, R. (2018). EU bods up GDPR ante: Threatens legislative laggards with "infringement procedure," (available at https://www.theregister.co.uk/2018/01/25/eu_bods_up_gdpr_ante_with_threat_of_infringement_procedure_for_legislative_laggards/).

Hoeyer, K. (2009). Informed consent: The making of a ubiquitous rule in medical practice, *Organization* 16(2), 267–288.

Hoofnagle, C., King, J., Li, S., and Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, SSRN Scholarly Paper No. ID 1589864, , Rochester, NY: *Social Science Research Network* (available at https://papers.ssrn.com/abstract=1589864).

Hunt, R. (2017). New Survey Reveals GDPR Readiness Gap, *Varonis* (available at https://blog.varonis.com/new-survey-reveals-gdpr-readiness-gap/).

Hutchinson, A. (2015). Convenience Vs Privacy: The Latest Study in the Data Tracking Debate, *Social Media today* (available at

https://www.socialmediatoday.com/technology-data/adhutchinson/2015-06-05/convenience-vs-privacy-latest-study-data-tracking-debate).

Information Commissioner's Office (2015). Direct marketing, (available at https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf).

Information Commissioner's Office (2016). Privacy notices, transparency and control, (available at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/).

Information Commissioner's Office (2017). The conditions for processing, (available at https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/).

Information Commissioner's Office (2018a). Key definitions of the Data Protection Act, (available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/).

Information Commissioner's Office (2018b). GDPR consent guidance, (available at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/).

Inter-credit international (2018). TCF Policy, (available at https://www.intercred.com/ici-treating-customers-fairly.pdf).

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.

Jolls, C., Sunstein, C., and Thaler, R. (1998). A Behavioral Approach to Law and Economics, *Stanford Law Review* 50, 1471.

Jovchelovitch, S. (2008). The Rehabilitation of Common Sense: Social Representations, Science and Cognitive Polyphasia, *Journal for the Theory of Social Behaviour* 38(4), 431–448.

Kahneman, D. (2012). *Thinking, Fast and Slow*, Penguin London.

Karwatzki, S., Dytynko, O., Trenz, M., and Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization, *Journal of Management Information Systems* 34(2), 369–400.

Kerr, I., Barrigar, J., Burkell, J., and Black, K. (2009). Soft surveillance, hard consent: The law and psychology of engineering consent, in *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* I. Kerr, V. Steeves, and C. Lucock

(eds.), Oxford University Press Oxford, 5–22 (available at http://idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_01.pdf).

Kolodinsky, J. M., Hogarth, J. M., and Hilgert, M. A. (2004). The adoption of electronic banking technologies by US consumers, *International Journal of Bank Marketing* 22(4), 238–259.

van Lieshout, M. (2014). The value of personal data, in *Privacy and Identity Management for the Future Internet in the Age of Globalisation. Privacy and Identity 2014* J. Camenisch, S. Fischer-Hübner, and M. Hansen (eds.) (Vol. 457), Springer Verlag London, 26–38.

Lindley, D. (2014). Innovation in Banking: Personal Financial Management - Credit Sesame and Money Dashboard - Empowering consumers to monitor their finances and get the best deal, *New City Agenda* (available at http://newcityagenda.co.uk/innovation-in-banking-personal-financial-management-credit-sesame-and-money-dashboard-empowering-consumers-to-monitor-their-finances-and-get-the-best-deal/).

Loewenstein, G., and Elster, J. (Eds.) (1992). *Choice Over Time*, Russell Sage Foundation New York, NY (available at https://www.russellsage.org/publications/choice-over-time).

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research* 15(4), 336–355.

Manthorpe, R. (2017). To change how you use money, Open Banking must break banks, *Wired* (available at http://www.wired.co.uk/article/open-banking-psd2-regulation-banking).

McClure, S. M., Laibson, D. I., Loewenstein, G., and Cohen, J. D. (2004). Separate Neural Systems Value Immediate and Delayed Monetary Rewards, *Science* 306(5695), 503–507.

McDonald, A. M., and Cranor, L. F. (2008). The Cost of Reading Privacy Policies, *I/S: A Journal of Law and Policy for the Information Society*.

Metzger, M. J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce, *Journal of Computer-Mediated Communication* 9(4), 00–00.

Moores, T. (2005). Do Consumers Understand the Role of Privacy Seals in e-Commerce?, *Communications of the ACM* 48(3), 86–91.

Morley, K. (2018). "Open banking" revolution could lead to scams and pricing rip-offs, experts warn, *Daily Telegraph* (available at http://www.telegraph.co.uk/news/2018/01/07/open-banking-revolution-could-lead-scams-pricing-rip-offs-experts/).

MSE Forum (2017a). Money Saving Expert Forum: Yolt App, *Money Saving Expert Forum* (available at http://forums.moneysavingexpert.com/showthread.php?t=5720844).

MSE Forum (2017b). Money Saving Expert Forum: Digital banking, *Money Saving Expert Forum* (available at http://forums.moneysavingexpert.com/showthread.php?t=5758951).

MSE Forum (2017c). Money Saving Expert Forum: Authorised Online Third Party Provider Access, *Money Saving Expert Forum* (available at http://forums.moneysavingexpert.com/showthread.php?t=5733825).

Nienaber, A.-M., Hofeditz, M., and Searle, R. H. (2014). Do we bank on regulation or reputation? A meta-analysis and meta-regression of organizational trust in the financial services sector, *International Journal of Bank Marketing* 32(5), 367–407.

Nissenbaum, H. (2011). A contextual approach to privacy online, *Daedalus* 140(4), 32–48.

Nussbaum, E. (2004). My So-Called Blog, *New York Times Magazine* (available at http://www.nytimes.com/2004/01/11/magazine/my-so-called-blog.html).

Open Banking Implementation Entity (2017). Open Banking Consent Model, (available at https://www.openbanking.org.uk/wpcore/wp-content/uploads/2017/12/Consent-Model-Part-1-Implementation-Guide.pdf).

Open Banking Implementation Entity (2018). Open Banking, (available at https://www.openbanking.org.uk/).

Orlowski, A. (2015). Silicon Valley now "illegal" in Europe: Why Schrems vs Facebook is such a biggie, *The Register* (available at http://www.theregister.co.uk/2015/10/06/silicon_valley_after_max_schrems_safe_harbour_facebook_google_analysis/).

Orlowski, A. (2017). Schrems busts Privacy Shield wide open, *The Register* (available at https://www.theregister.co.uk/2017/10/03/schrems_busts_privacy_shield_wide_open/).

Ortendahl, M., and Fries, J. F. (2002). Time-related issues with application to health gains and losses, *Journal of Clinical Epidemiology* 55(9), 843–848.

Parliament (2018). Data Protection Bill 2017-19, (available at https://services.parliament.uk/bills/2017-19/dataprotection.html).

Pew Research Center (2014). Public Perceptions of Privacy and Security in the Post-Snowden Era, (available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/).

Preibusch, S. (2015). Privacy Behaviors After Snowden, *Communications of the ACM* 58(5), 48–55.

Reynolds, F. (2017). Open Banking – A Consumer Perspective, (available at https://www.openbanking.org.uk/wpcore/wp-content/uploads/2017/12/Open-Banking-A-Consumer-Perspective.pdf).

Rudgard, O. (2018). Open banking will only mean more bad deals for the most vulnerable, *Daily Telegraph* (available at http://www.telegraph.co.uk/news/2018/01/08/open-banking-will-mean-bad-deals-vulnerable/).

Salmon, F. (2016). Privacy is an afterthought when convenience is king, *Splinternews* (available at https://splinternews.com/privacy-is-an-afterthought-when-convenience-is-king-1793853823).

Schaub, F. (2017). Nobody reads privacy policies – here's how to fix that, *The Conversation* (available at http://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932).

Schaub, F., Balebako, R., and Cranor, L. F. (2017). Designing Effective Privacy Notices and Controls, *IEEE Internet Computing* 21(3), 70–77.

Schrage, M. (2016). Why User Experience Always Has to Come First, *Harvard Business Review* (available at https://hbr.org/2016/09/why-user-experience-always-has-to-come-first).

See-To, E. W. K., and Ho, K. K. W. (2016). A study on the impact of design attributes on E-payment service utility, *Information & Management* 53(5), 668–681.

Smith, G. J. (2018). Data doxa: The affective consequences of data practices, *Big Data & Society* 5(1), 2053951717751551.

Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma, *Harvard Law Review* 126, 1880.

Steeves, V. (2009). Reclaiming the social value of privacy, in *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* I. Kerr, V. Steeves, and C. Lucock (eds.), Oxford University Press Oxford, 191–208 (available at http://idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_01.pdf).

Thaler, R. H., and Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth and happiness*, Penguin London.

Thaler, R. H., Tversky, A., Kahneman, D., and Schwartz, A. (1997). The Effect of Myopia and Loss Aversion on Risk Taking: An Experimental Test, *The Quarterly Journal of Economics* 112(2), 647–661.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, *Information Systems Research* 22(2), 254–268.

Turow, J., Feldman, L., and Meltzer, K. (2005). Open to Exploitation: America's Shoppers Online and Offline, *A Report from the Annenberg Public Policy Center of the University of Pennsylvania* (available at https://repository.upenn.edu/asc_papers/35/).

unroll.me (2016). Unsubscribe from emails, instantly., (available at https://unroll.me/legal/privacy/).

Westin, A. (1967). *Privacy and freedom*, Atheneum Press New York.

Whitley, E. A. (2009). Informational privacy, consent and the "'control'" of personal data, *Information Security Technical Report* 14(3), 154–159.

Whitley, E. A., and Kanellopoulou, N. (2010). Privacy and informed consent in online interactions: Evidence from expert focus groups, TBC (ed.), Presented at the International Conference on Information Systems.

Whitley, E. A., Kanellopoulou, N., and Kaye, J. (2012). Consent and Research Governance in Biobanks: Evidence from Focus–groups with Medical Researchers, *Public Health Genomics* 15(5), 232–242.

Whitley, E. A., Willcocks, L. P., and Venters, W. (2013). Privacy and Security in the Cloud: A Review Of Guidance and Responses, *Journal of Information Technology and Information Management* 22(3), 75–92.

Winograd, T., and Flores, F. (1986). *Understanding computers and cognition: A new foundation for design*, Addison Wesley Reading, MA.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative view, Presented at the

International Conference on Information Systems (available at http://aisel.aisnet.org/icis2008/6/).

Zachariadis, M., and Ozcan, P. (2017). The API Economy and Digital Transformation in Financial Services: The case of Open Banking, *The Swift Institute* (available at https://www.swiftinstitute.org/papers/the-api-economy-and-digital-transformation-in-financial-services-the-case-of-open-banking/).

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology* 30(1), 75–89.