Committee Stage Briefing by The Open University's True Potential Centre for the Public Understanding of Finance (PUFin) – October 2017

Data Protection Bill, clause 173: the need for collective redress in the light of Open Banking

---

This briefing has been prepared by Jonquil Lowe, member of the Open University's True Potential Centre for the Public Understanding of Finance (PUFin) and also a member of the Open Banking Consumer Forum, an informal group of consumer representatives formed to provide a consumer perspective to the Open Banking Implementation Entity.

Executive Summary

1. The European General Data Protection Regulation (GDPR) introduces welcome additional protections for consumers in the face of the rapid increase and technology-driven changes in the use of personal data. While the GDPR in general applies automatically in member states, there is discretion in some areas and these are addressed, among other matters, in the Data Protection Bill introduced into the House of Lords in September 2017.

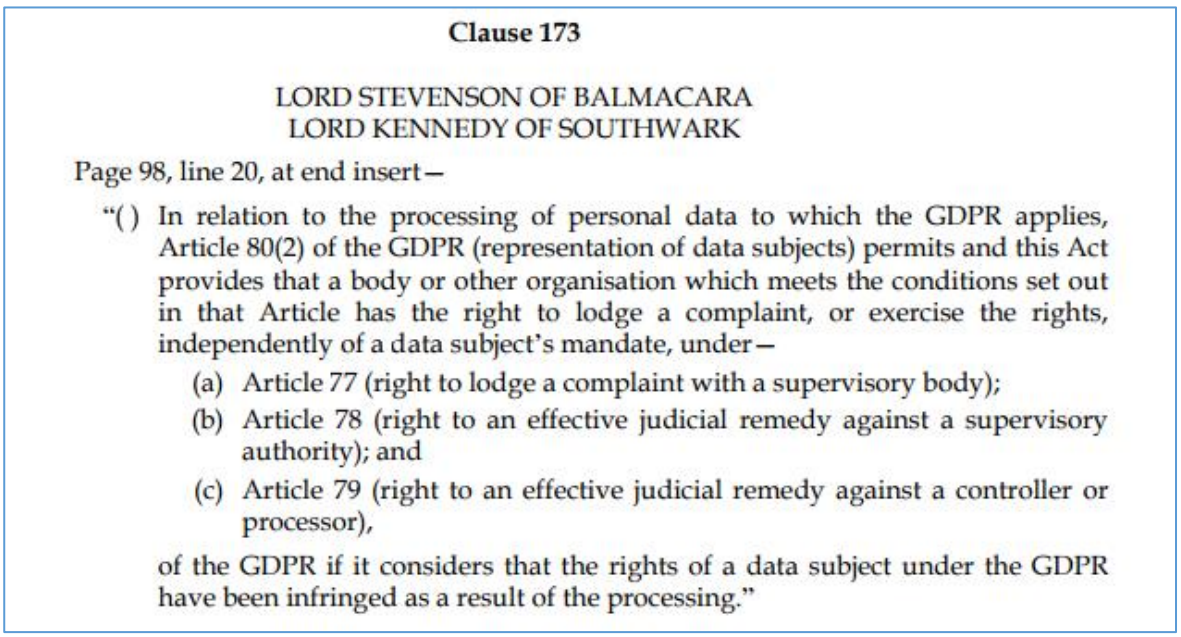
2. Open Banking is a new way of sharing bank account data (including detailed transactions information) with third parties from January 2018 onwards. Open Banking has the potential to deliver substantial benefit to consumers through greater and more informed choice and improved competition (CMA, 2017; Lowe, 2017). However, for these benefits to be delivered, it is essential that consumer trust and confidence are embedded. Therefore Open Banking must be underpinned by effective and meaningful access to redress.

3. While Open Banking does not necessarily introduce types of risk that do not currently exist, it has the potential to substantially increase personal data sharing and therefore the *volume* of people at risk (Open University, 2017 http://www.open.ac.uk/ikd/news/open-university-workshop-explores-implications-open-banking). Therefore, it will become increasingly important that: consumers have access to effective pathways to resolve problems and, where appropriate, seek redress; and the economy as a whole has efficient ways to resolve problems where large numbers of consumers are affected by the same data breach.

4. Open Banking also adds to the complexity facing consumers, since some data breaches could fall within the scope of financial regulation, while others will not. Where data has been shared with a chain of third parties, it may be difficult, if not impossible, for consumers themselves to identify which firm is at fault and thus which jurisdiction applies. Where a data breach falls outside the remit of financial regulation, under current rules, the consumer's only route for redress is to take court action. Quite apart from the difficulty of identifying which firm in a chain of third parties may be at fault, pursuing a claim through the courts is likely to be daunting, time-consuming and costly, deterring many consumers from seeking redress at all.

5. A solution to this problem would be to allow designated bodies to initiate an action for collective redress on behalf of consumers. Article 80(2) of the GDPR gives member states discretion to do this by allowing *'a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data'* to seek collective redress on behalf of all consumers affected by a particular data-protection breach, unless they opt out[1]. **We are concerned that the government has not taken the opportunity to include this collective redress solution in the Data Protection Bill and urge members of the House of Lords to support the amendment to the Bill proposed by Lord Stevenson of Balmacara and Lord Kennedy of Southwark (see Figure 1 below).**

[1] The 'opt-out' basis is important. Since group litigation became possible in the UK from 2002, only one case has been brought on an opt-in basis and fewer than 0.1 per cent of affected consumers joined the action (Norton Rose Fulbright, 2017).



Clause 173

LORD STEVENSON OF BALMACARA
LORD KENNEDY OF SOUTHWARK

Page 98, line 20, at end insert—

"( ) In relation to the processing of personal data to which the GDPR applies, Article 80(2) of the GDPR (representation of data subjects) permits and this Act provides that a body or other organisation which meets the conditions set out in that Article has the right to lodge a complaint, or exercise the rights, independently of a data subject's mandate, under—

(a) Article 77 (right to lodge a complaint with a supervisory body);

(b) Article 78 (right to an effective judicial remedy against a supervisory authority); and

(c) Article 79 (right to an effective judicial remedy against a controller or processor),

of the GDPR if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing."

Figure 1: Proposed amendment to allow collective redress on an opt-out basis (parliament.uk, 2017)

Background

6. In order to promote competition in the UK market for personal current accounts, the Competition and Markets Authority has tasked nine leading banking organisations to facilitate Open Banking, which is a method of sharing personal banking data with third party firms, through the establishment of common, openly available, free-to-use application programming interfaces (APIs) (CMA, 2017). APIs can be thought of as secure pipelines between a bank and a third party along which data (and third-party-initiated payments) can travel with the customer's consent. This will enable, for example, consumers to share their transaction data with comparison websites in order to generate personalised best deals for current accounts.

7. However, the potential scope of Open Banking is far greater than just personalised product comparisons, both financial and non-financial. It may also be used to transfer data to money aggregation providers, debt advice providers, money guidance providers, and as a way to assess affordability or creditworthiness for credit or purchase of large items. Banking data may also be combined with data from other sources, such as social media accounts, to build a holistic picture of customers in order to promote particular products or strategies. In fact, it is hard to envisage the full scope of new digital services that may result from Open Banking.

8. Two pieces of legislation are particularly important for Open Banking: the second Payment Services Directive (PSD2) and the GDPR.

9. PSD2 will be administered in the UK by the Financial Conduct Authority (FCA). While concerned mainly with payment services, it also newly extends regulation to organisations that act as Account Information Service Providers (AISPs), in other words third parties that gather account information from a consumer's bank. The FCA has provided examples of the types of firms that will be classified as AISPs (see Figure 2 below). AISPs will have to be registered by the FCA and will be covered by the Financial Ombudsman Service, but not the Financial Services Compensation Scheme.

10. Financial data transferred through Open Banking, from which (either alone or in combination with other information) a person can be identified, are likely to be 'personal data' under the terms of the GDPR. In themselves, these data will not usually be 'sensitive' personal data (to which more stringent rules apply) - i.e. about racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life or offences. However, financial data could be sensitive if they relate to, say, payment of trade union subscriptions or for health services. (Open University, 2017 http://www.open.ac.uk/ikd/news/open-university-workshop-explores-implications-open-banking)

Account information services.	• businesses that provide users with an electronic 'dashboard' where they can view information from various payment accounts in a single place • businesses that use account data to provide users with personalised comparison services supported by the presentation of account information • businesses that, on a user's instruction, provide information from the user's various payment accounts to both the user and third party service providers such as financial advisors or credit reference agencies

Figure 2: Examples of Account Information Service Providers (FCA, 2017)

The problem

11. There are a range of different ways in which consumers may engage with the digital services that will use Open Banking which have different implications for the redress options open to consumers if something goes wrong:

- **Single registered AISP**: the service, such as a money aggregator or comparison website, may itself be an AISP. If something goes wrong the consumer complains first to the firm and, if unhappy with that outcome, can take their case to the Financial Ombudsman Service (which has the power to order a firm to take a variety of steps to put matters right, including compensation up to £150,000).
- **AISP outsourced:** the service the consumer wishes to use, such as a money aggregator or comparison website, uses an intermediary firm as the AISP[2]. The data are then shared with the service the consumer wishes to use. The service itself may be regulated by the FCA, for example, if it is a money aggregator, a comparison website that is comparing regulated activities such as insurance, or a debt adviser, in which case the consumer would have recourse to the Financial Ombudsman Service if something goes wrong. However, the service might be unregulated, for example, a comparison website comparing utilities or best-buy consumer goods or offering budgeting guidance. In this case, if there was a data breach, the consumer would have access to the Financial Ombudsman if the AISP were at fault but would have to resort to the courts if the unregulated service provider were at fault.
- **Complex chains:** in practice, firms offering digital services may sit within complex chains where AISP is outsourced and the transactions data are either collated with other data from multiple sources (such as social media sites) or passed through to other firms (for example, in return for payment if that is part of the digital services firm's business model). Data may thus flow through a complex chain of firms, some regulated and some unregulated. In the event of a data breach, whether or not the consumer has recourse to the Financial Ombudsman Service will depend on where in the chain the breach occurs. This scenario is further complicated by the fact that strands of personal data that were not in themselves classified as 'sensitive' under the data protection legislation may become sensitive when combining with other data.

12. An enormous hurdle facing consumers in the event of a data breach will be how to identify where in a chain of firms the breach has occurred. Until that first step of identification is complete, the consumer will not know where to direct their complaint or whether the Financial Ombudsman can help. Assuming that hurdle can be overcome, if the firm responsible for the breach is not regulated by the financial regulator and does not respond satisfactorily to the complaint, the consumer's only recourse is to take their case to court, a daunting, lengthy and costly procedure that will deter many consumers. An additional hurdle is determining the amount of redress that the consumer should seek, given that it is impossible to know how their lost or stolen data may be misused and the consequences of that misuse.

13. While financial education may be used to help consumers become more aware of the value of their data and more careful in granting access to it (Open University, 2017, http://www.open.ac.uk/ikd/news/open-university-workshop-explores-implications-open-banking), no amount of financial education will enable consumers to overcome the hurdles outlined above. It is unreasonable to expect individual consumers to be

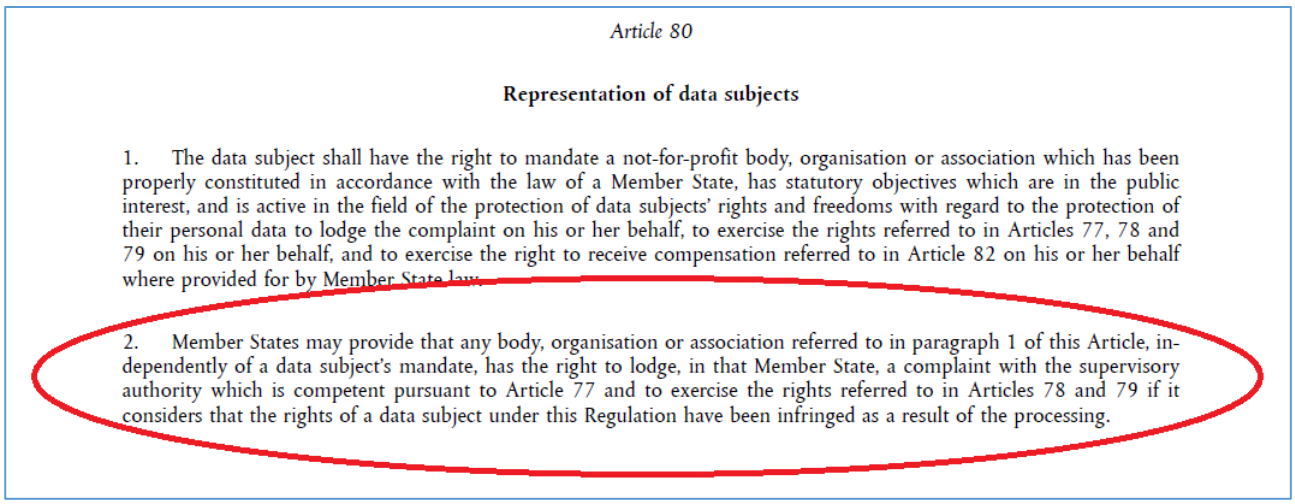
[2] An example of a commonly used intermediary is the firm Yodlee.

able to access let alone understand the information that could unravel where in a complex chain of firms a data breach has occurred.

A solution

14. The Data Protection Bill (clause 173) does allow consumers individually to appoint a suitable body to act on their behalf (enacting Article 80(1) of the GDPR). In theory, this could enable consumers to opt into a class action, though locating affected consumers – who may not even realise that a data breach has affected them – could be difficult. Moreover, even if consumers realise they could be affected, they might individually feel that the amount of loss is too small and/or effort is too great to warrant action even though the scale of the data breach in terms of numbers of consumers affected could be huge.

15. The clear solution would be to enable a designated body acting on behalf of all affected consumers to initiate action to resolve a data breach problem, including seeking redress if appropriate. The body, having resources both financial and in terms of relevant expertise, would be better placed than individual consumers to uncover where in a complex chain a data breach has occurred, thus which firm (or firms) should be the subject of action and the extent of consumers affected. The body would also be better resourced to bring a court action on behalf of affected consumers and this would most efficiently be done by representing all affected consumers as a group rather than seeking to identify each individual.[3] Article 80(2) of the GDPR allows for this pathway to redress (see Figure 3) and we urge members of the Lords to support transposing Article 80(2) into UK law. An amendment to achieve this has been proposed by Lord Stevenson of Balmacara and Lord Kennedy of Southwark – see Figure 1 above.



Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Figure 3: GDPR enables collective redress on an opt-out basis (European Parliament, 2016)

16. Governments and firms are often wary of collective redress schemes, fearing that they will open the door to widespread, speculative class actions as happens in the USA. However, Article 80(2) builds in safeguards to prevent this. In particular, the bodies that may initiate collective redress on an opt-out basis are strictly limited to *'a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data'*. This substantially reduces the risks of vexatious or speculative actions and compensation awards flowing to contingency-fee lawyers, hedge funds and similar firms, and is in line with European Commission (2013, para 4) recommendations for the introduction of collective redress subject to certain safeguards. Although those same recommendations in general favour opt-in collective redress over opt-out, they acknowledge that opt-out may *'be duly justified by reasons of sound administration of justice'* (European Commission, 2013, para 21). We would argue that opt-out is justified in this case given the complexity for consumers described above in accessing justice if they are subject to a data breach occurring somewhere in a chain of related firms. There is also a consensus that collective redress on an opt-in basis, which has been possible in the UK since 2002, has not worked. Only one case has been brought since 2002 (The

[3] As an example of the large numbers of consumers that may be affected by a single data breach, in 2017 Equifax was the target of hackers in which the data of 143 million US citizens and 694,000 UK citizens were affected, potentially exposing them to identity theft and targeted scams. (BBC, 2017)

Consumers Association v JJB Sports plc) and fewer than 0.1 per cent of affected consumers joined the claim. The global law firm, Norton Rose Fulbright, has commented: '*The requirement for claimants to 'opt-in' to any actions is considered to have been a significant impediment to collective redress'* (Norton Rose Fulbright, 2015).

17. A precedent already exists in UK law, where the Consumer Rights Act 2015, Schedule 8, allows collective redress actions on an opt-out basis to be brought under competition law. That legislation includes a safeguard against abuse requiring the Competition Appeal Tribunal to judge whether it is *'just and reasonable'* for a representative to act on behalf of the consumers affected (Consumer Rights Act 2015, Schedule 8, para 8). Only two cases[4] have so far been brought under this legislation (US Chamber Institute for Legal Reform, 2017). The safeguard set out in Article 80(2) of the GDPR and transposed in the proposed amendment to the Data Protection Bill would be even stronger by writing into primary legislation the key attributes that representative bodies must fulfil.

[4] One of these is a £14 billion lawsuit against Mastercard following a ruling by the European Commission on anti-competitive practice in setting merchant charges. The amount may seem huge at first sight but this is due to the very large - an estimated 46 million – of consumers affected and the complexity of the case. (US Chamber Institute for Legal reform, 2017) As with competition cases, data breaches may also affect millions of consumers and may be complex.

References

BBC (2017) *Equifax to be investigated by FCA over data breach* [online] http://www.bbc.co.uk/news/technology-41737241 (accessed 24 October 2017).

Competition and Markets Authority (CMA) (2017) *The retail banking market investigation order 2017* [online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/600842/retail-banking-market-investigation-order-2017.pdf (accessed 23 October 2017).

European Commision (2013) *COMMISSION RECOMMENDATION of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law* (2013/396/EU) [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013H0396 (accessed 23 October 2017).

European Parliament (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)* [online] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 (accessed 23 October 2016).

Financial Conduct Authority (2017) *Payment Services and Electronic Money –Our Approach. The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011* [online] https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf (accessed 23 October 2017).

Lowe, J. (2017) *Consumers and competition: delivering more effective consumer power in retail financial markets*, 'Think-piece' commissioned by the Financial Services Consumer Panel [online] https://www.fs-cp.org.uk/sites/default/files/fscp_consumers_and_competition_thinkpiece_finalpp_jtl_20170306.pdf (accessed 23 October 2017).

Norton Rose Fulbright (2015) *The adoption of opt-out collective actions in the UK* [online] http://www.nortonrosefulbright.com/knowledge/publications/130108/the-adoption-of-opt-out-collective-actions-in-the-uk (accessed 27 October 2017).

Parliament.uk (2017) *Data Protection Bill. Running list of amendments* [online] https://services.parliament.uk/bills/2017-19/dataprotection/documents.html (accessed 23 October 2017).

Open University (2017) *Financial capability- where we are now and is Open Banking a game changer?* Report of OU Workshop held on 21 July 2017 [online] http://www.open.ac.uk/ikd/news/open-university-workshop-explores-implications-open-banking (accessed 24 October 2017).

US Chamber Institute for Legal Reform (2017) *The growth of collective redress in Europe. A survey of developments in 10 member states* [online] http://www.instituteforlegalreform.com/uploads/sites/1/The_Growth_of_Collective_Redress_in_the_EU_A_Survey_of_Developments_in_10_Member_States_April_2017.pdf (accessed 23 October 2017).