The Information Commissioner's Office response to HM Treasury's Call for Evidence on Data Sharing and Open Data in Banking

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003.

He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to this call for evidence on data sharing and open data in banking. The Information Commissioner recognises there may be economic benefits to consumers, businesses and other organisations arising from the publication of open data sets and increased data sharing in banking. There are, however, a number of important privacy concerns to be considered.

The ICO has previously provided advice and guidance on the data protection issues arising from the transfer of financial transaction data to the authors of the report, *Data Sharing and Open Data for Banks,* which precedes this call for evidence. We take this opportunity to reiterate some of the submissions made whilst that report was being researched and drafted. The ICO's response to this call for evidence relates only to those questions that significantly impact upon information rights issues.

Question 3
Who should play a role in the development of an open API standard and who should be able to make use of it and how?

There should be a wide range of stakeholders involved in the development of an open API standard, including consumer representatives and other groups interested in privacy issues.

Question 5
The government would like to deliver an open API standard in banking as quickly as possible. Are there practical issues which could affect quick delivery? Would 1 to 2 years be a reasonable timescale for delivery?

We understand the Government's desire to move quickly in developing a standard, but suggest that the speed of development should not be at the expense of ensuring personal data is protected to a high level.

Sufficient time and resource should be provided to ensure the ancillary issues that will be essential for successful adoption by consumers and business, for example measures to ensure consumer trust and confidence when sharing data, can be successfully delivered.

Question 6 (&9)
What issues would need to be considered in terms of data protection and security, and what is the best way to address these?

Obtaining information about an individual's spending habits presents a powerful way in which to build a very detailed profile about that individual and the way in which they choose to lead their life. This position is exacerbated following the growth in contactless payments for small transactions which might previously have been undertaken, in cash, with relative anonymity. Profiling in this way is potentially very privacy intrusive and careful consideration needs to be given to ensure the risks arising are identified and appropriately managed.

Whilst in most cases financial transaction data is not likely to be sensitive personal data according to the strict legal definition[1], we suggest that information about an individual's financial affairs and standing is a matter that many people would consider to be confidential. In 2014 the ICO issued civil monetary penalties against two organisations which failed to take appropriate technical and organisational security measures to protect payment card information in what amounted to a serious breach of the Data Protection Act.

It should be appreciated that whilst access to financial transaction data is intended to improve competitiveness in the personal current account market and facilitate development of fintech products, both of which are entirely laudable objectives, the danger is that this is a case of "opening Pandora's box" with consequences for individuals' privacy extending beyond the envisaged applications. It is not something to be entered into without sufficient thought being given to what the implications are for individuals' privacy.

[1] Data Protection Act 1998, Section 2

Individuals can currently download a copy of their personal current account statements through online banking services, or receive a paper copy on demand. It is expected that the public will soon be able to download a copy of their personal current account (PCA) 'midata file' containing a partially redacted version of their transaction history in a standardised CSV format which may, in turn, be uploaded to an online price comparison service.

In the existing cases it should be more readily apparent to the individual what data they are sharing because they can physically inspect it. Conversely, where an API is used to access and share data there is less visibility and this creates a challenge in terms of ensuring any consent given by the individual for the processing of their data is specific, informed and freely given. The issue is exacerbated when the access provided is ongoing, i.e. does not require future action from the individual, and is more than simply a "one time" permission. Individuals need sufficient control of their data and an informed understanding of what organisations are doing with it.

The Open API standard should also address the fact that financial products and transactions can relate to more than one individual. Current accounts and mortgages can be held in multiple names and transaction histories can include details of payments made direct to family and friends.

It is foreseeable that the introduction of an open API standard will lead to the development of new products and services which seek to utilise the data which becomes accessible. It will be essential that organisations, and regulators, understand the risks arising when processing individuals' personal data in such volumes and with such variety. It is important to understand that analysis of financial transaction data to make conclusions about individuals, and then to use this data to make decisions has the potential to be unfair (or unethical), and appropriate care should be exercised.

In relation to the financial transaction Midata download previously described, the data is partially redacted to ensure that the price comparison service only receives the information that is needed to make a comparison of PCA options. This element is integral to the scheme and helps safeguard against processing of excessive and unnecessary data. Consideration also needs to be given as to how granular any permission might be and whether any privacy enhancing features can be built in.

It will be essential that organisations, supported by government, are able to build consumer trust and ensure that individuals can make informed decisions about whether to share their data, and on what terms. Taking

steps to build consumer trust and confidence should be an integral part in development of the standard.

The ICO advocates the adoption of 'privacy by design' principles and privacy impact assessments (PIAs) to ensure privacy risks are identified from the outset, and that measures to address these are built in to any projects and not 'bolted on' at a later stage.

Question 7
What are the technical requirements that an open API standard should meet?

An open API standard should ensure that access to the data is secure from unauthorised access during transfer (i.e. an encrypted transfer protocol such as TLS) and also provides an assurance of who the data is being shared with (e.g. third-party API key applications must be rigorously checked). The open API standard should also ensure there is appropriate verification of identity of the data subject before any third-party access to the data can be granted.

It should be recognised that granting access to an individual's account information is not the same as a third-party making use of that permission. Therefore the open API standard should have a comprehensive audit trail mechanism to inform users about who and when access has taken place including examples of the data which has been accessed.

The Open API Standard should also support the principle of data minimisation such that third-parties are only given access to the information strictly necessary for a previously defined purpose. The individual should be given a granular level of control such that they can choose precisely which data the third-party can access and be given effective mechanisms to revoke that access in a simple and effective manner.

Question 10
What are the other risks or costs of publishing more open data in banking and how can they be addressed?

Anonymised open data sets may pose privacy risks if they are combined and aggregated with other data sets. This can lead to the re-identification of individuals, or allow for a more intrusive analysis of an individual's private life. For example, if the payment description field in an individual's transaction history contained a code relating to a specific ATM, and an open data set of ATM codes and the location of the ATMs in question was subsequently released, then this may enable an organisation to identify not only the date that the account holder makes a withdrawal, and how

much for, but also where the individual was at the time. The ICO's Code of Practice on Anonymisation[2] sets out the steps that should be taken to assess and mitigate the risks of re-identification. The ICO agrees that fully open datasets should always be considered, to enable maximum transparency and the greatest benefits from re-use, but consideration should be given as to whether certain types of datasets have to be made available using specific user agreements and to identified users to mitigate privacy risks.

The ICO has published a paper, *Big data and data protection*[3] which identifies some of the challenges for organisations seeking to use big data analytics which may prove instructive. We identify the use of privacy impact assessments, privacy by design, and transparency/privacy information as some of the tools available to organisations to meet these challenges.

Question 12
If so, what action do they think is required by the banks and the Government to bring them about?

The Government needs to work with a wide range of interested stakeholders to explore the wider implications of releasing financial transaction data, assess the privacy risks and identify ways in which these may be appropriately dealt with.

In relation to the Midata programme, the ICO has regularly highlighted the point that there needs to be a sufficiently robust framework in place for ensuring consumer trust and confidence, including provision for an overarching Consumer Charter or Code of Practice.

We find ourselves in a position, however, where financial transaction data is shortly to be released by banks as a download without any overarching code being in place. The banking industry and comparison providers have worked together to agree an industry code which may go some way towards addressing some of the risks, but there is no obligation on any bank or comparison provider to follow its requirements and no direct sanction if it is breached.

February 2015

[2] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
[3] https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf