

BBA response to a consultation paper on the use and sharing of personal information in the public and private sectors

The British Bankers' Association is the leading UK banking and financial services trade association and acts on behalf of its members on domestic and international issues.

Our 225 banking members are from 60 different countries and collectively provide the full range of banking and financial services. They operate some 130 million accounts, contribute £50bn to the economy and together make up the world's largest international banking centre.

Executive Summary

The financial institutions represented by the BBA hold 130 million accounts. This represents a significant share of the total volume of data held on computer systems in the UK. Financial institutions work closely with credit reference agencies (CRAs) and data relating to the credit records of customers is shared across the finance industry via the three agencies.

Members of the BBA welcome the opportunity to provide an industry response to this consultation. This response represents the collected views of members although some members will be submitting their own individual response.

The extent of data sharing already taking place is discussed in this response and we refer to the views of the industry already noted in response to the BERR consultation on whether or not the Government should introduce specific legislation to enable the sharing of non-consensual credit account data with CRAs. This is data not currently shared with CRAs by many lenders because 'consent' may not be held. We consider legislation which expressly permits such data sharing would be of great benefit to the industry and greatly assist their obligations to lend responsibly, although we are of the view that there is a strong argument to suggest that such data sharing can occur under the legitimate interests provision within Schedule 2 of the Data Protection Act 1998 (DPA). However, we are also aware that the law relating to a banker's duty of confidentiality means that in the absence of customer consent, a bank has very little discretion to disclose information. This is covered in more detail later in this response.

In addition to credit data, we discuss in this paper the need to share information between the public and private sector relating to fraud and crime. This already takes place but we call for greater clarification and extended powers. For example:

- We call for greater sharing of electronic information on fraudsters between the UK Identity and Passport Service, the DVLA and the financial services industry.
- We believe S29 of the DPA could be clarified so that reporting of crime between financial institutions is enabled to assist the Police in taking on more fraud cases.

Fundamental to any debate about data sharing is the DPA. In general we support the DPA and consider it provides sensible protection for data subjects without creating unnecessary difficulties for data controllers and processors. However in our response we detail a number of areas we consider the law or guidance relating to the law could be improved. e.g.

- Greater sharing of data held by public authorities relating to their records of debt should be encouraged and enabled.
- The law relating to cross border data sharing needs to be reviewed.
- Guidance concerning data sharing with UK and overseas regulators needs to be clarified.
- S29 of the DPA should be reviewed
- We express concern about the potential for abuse of subject access rights and refer to helpful judgments contained in recent legal cases.
- The law on banking confidentiality means that the disclosure of customer data to public authorities or, indeed other banks, may have to be enabled by statute law or regulation where it is unrealistic to obtain consent and where banks do not consider the 'own interests' qualification applies.
- We seek greater clarification of the status of undertakings requested by and given to the ICO.

Bankers are very mindful of their duty to keep customer records confidential and they are very supportive of the DPA. It is considered that the DPA works very well and does not cause undue restrictions in relation to data sharing. In general we think its main strength is that it strikes the right balance between being suitably prescriptive and protective of the rights of individuals whilst at the same time leaving data controllers the flexibility to decide the most appropriate way for them to comply.

As discussed there are areas of law and practice that would benefit from revision in the light of technological developments and the enormous scale of data records held by UK companies and the UK Government. We believe it is important to hold regular consultations between the private and public sectors and we and our members will be pleased to contribute our expert knowledge and experience to this process.

We attach submissions made by the BBA to recent consultations carried out by DTI (BERR) and ICO.

Appendix 1: Response to ICO on DP strategy

Appendix 2: Response to ICO on information sharing

Appendix 3: Response to Consultation by DTI (BERR) on sharing non consensual data

Yours sincerely

Section 1: Background

Question 1

Please explain what your interest in information sharing is.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- What kinds of personal information do you collect, hold and share?
- How do you collect, hold and share such personal information?
- For what purposes do you collect, hold and share such personal information?

The Banking Sector's principal interests in data sharing are for credit control and fraud prevention purposes.

Typically, in the context of customer information banks collect and hold an individual's name, address, telephone, date of birth, employment, income and bank details. Many will also collect and hold information about an individual's nationality as part of their Anti-Money Laundering procedures. Additionally, they collect and hold information about the conduct and characteristics of customer accounts. Some information is held in its raw form, whilst other information is derived and held for use, such as for credit scoring purposes. For the purposes of fraud prevention, banks maintain information, within the confines of existing industry agreements, on the victims and perpetrators of fraud.

Information comes from different sources, including the individuals themselves, credit and fraud prevention agencies and other companies within the same group (group companies). Initially, individuals provide information through credit applications, (paper, telephone or online) although at later stages of a banking relationship, it may be supplied during review conversations and other interactions. It is collected periodically from credit reference agencies and other group companies, often as a result of a 'trigger event', such as a loan application or unauthorised overdraft.

Information is collected, held and shared to allow banks to carry out risk assessments (identity checking, credit and fraud risk management) and general account management, as well as simple customer servicing.

Financial crime information may be derived from analysis of transactional activity through an account or a linked account. It may also be collected through suspicions of employees and other individuals. It is then shared with relevant law enforcement agencies in accordance with the law. Information for fraud prevention purposes is shared, for example via the Fraud Intelligence Sharing System (FISS) maintained by APACS. As with credit reference and fraud prevention agencies, FISS is a database onto which subscribers from the banking sector input data as well as retrieve it.

Much of the information collected is shared with other relevant companies in the same Group for credit risk and financial crime control purposes. It is shared with credit reference agencies for credit scoring and assessment purposes, as well as to meet legal and regulatory obligations regarding identification. Behavioural information is shared with credit reference agencies, as is default data. Elements of this information are further shared, via the credit reference agencies with other financial organisations following strict protocols laid down in SCOR's (Steering Committee on Reciprocity) 'Principles of Reciprocity'. The level of sharing will depend on a number of circumstances, not least the size of the bank and its own internal policies. In view of this, it is not possible to provide a specific response in respect of sharing activity that applies to all BBA members equally.

New customers are advised about banks' use of credit reference and fraud prevention agencies as well as more general data sharing via application and terms and conditions fair processing notices. Consent is obtained before initial searches are undertaken. Many banks will also collect consent at the same time to make periodic searches of such agencies

and, where relevant, other group companies. This includes an explanation of the implications of such searches on the applicant and any 'associated' individuals. In the event that applicants refuse to give their consent, the application is unlikely to be able to proceed as failure to make appropriate searches would put banks in breach of certain financial services regulations. Banks would be unwilling to provide financial services to individuals about whose credit or possible fraud history they knew nothing or where permission to share credit data is withheld.

Obtaining consent from some long-standing existing customers is unrealistic and is the subject of a DTI (from here on referred to as BERR) consultation on the 'Removal of Barriers to the sharing of Non-Consensual Credit Data'.

Information is held in operational systems for decision making and may be archived into analytical databases for future strategy development and for the provision of management information. Banks often obtain anonymised information from credit reference agencies for scorecard development.

All information held is subject to stringent organisational and technical security safeguards.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2

What in your view are the key benefits of sharing personal information to a) individuals and b) society? Please provide examples.

Key benefits include:

- Identifying ID theft and protecting genuine customers, individuals and assets;
- Identifying known fraudsters and preventing infiltration into the organisation (employees and customers);
- Minimising the risk of distress to genuine customers by reducing the risk of false suspicion;
- Improving fraud prevention capability and assisting in the reduction of crime and terrorist funding and making society a safer place;
- Improving the accuracy and quality of banks' investigations;
- Reducing the capability of criminals to launder the proceeds of their illegal operations by depriving them of banking facilities;
- Proactively intervening minimises the potential financial impact to organisations and the UK economy as a whole;
- Reducing the need to re-key the same information into multiple systems, which in turn reduces the risk of typing errors and subsequent inability to accurately 'match' records;
- Minimising the risk of inconsistencies and errors across different bodies;
- Providing banking services that are appropriate to an individual's circumstances, including product availability and relevance;
- Assessing responsible levels of credit to be granted;
- Facilitating responsible lending by enabling lenders to identify and decline applications which could otherwise result in/exacerbate financial difficulty;
- Setting appropriate pricing levels and reward schemes.

Question 3

What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

All processing carries risk. Whilst the following key risks have been identified as applying to data sharing, it is important to understand that they may apply equally to other processing activities. They should not be regarded as risks that apply to data sharing in isolation.

Key risks include:

- The theft or loss or subsequent inappropriate use of information, whether accidental, opportunistic or via targeted organised crime; (This includes the loss of information from third parties, within or outside the EEA);
- Corruption of low-paid individuals who have access to sensitive information.
- Loss of trust in data controllers following compromise;
- Perception of a 'nanny state';
- Inappropriate or inaccurate processing of personal information. For example, Sharing of inaccurate information, compounding problems for individuals who are having decisions made about them based on inaccurate information
- Information falling into the wrong hands through poor control of either the provider of the information or the recipient;
- Misinterpretation and resulting accidental misuse of shared information by the recipient;
- Wilful misuse of the information by third party recipients; For example, information shared for credit or fraud prevention purposes is subsequently used for direct marketing purposes;
- Errors and omissions by the provider of the information may have an adverse impact on the decision-making capabilities of the recipients of the shared information.

Question 4

As mentioned in the introduction, there are wide variations in the scope and methods of personal information sharing. What scope and what methods, in your view, pose the greatest opportunities or risks? Please explain the reasoning behind your response.

This response explains the scope of data shared by financial institutions and the controls exercised by such bodies as SCOR as evidenced by the Principles of Reciprocity produced by SCOR. Data sharing in respect of financial management is conducted in an open and transparent manner. Customers are notified about the extent of data shared and the appropriate consent is obtained from them. The Principles of Reciprocity are published.

This paper explains the benefits and opportunities the financial institutions and their customers gain from data being shared in respect of monitoring financial exposure and controlling fraud.

We believe that the principles and procedures adopted by financial institutions are a model of responsible behaviour. The DPA can be perceived as a threat and we believe that if a more positive and knowledgeable view is taken of the DPA by many public and private bodies, significant gains can be taken from data sharing and all within the constraints of the current law.

Question 5

Please provide examples of where, in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.

We make some reference to the public sector sharing information with the private sector in relation to fraud and crime prevention and to debt management. Other than that we do not consider it appropriate for us to respond to this question.

Question 6

Please provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.

The third data protection principle obliges data controllers to process personal information that is adequate, relevant and not excessive. Therefore, we would not expect our members to hold too much or too little information.

Use and sharing of personal information in the public and private sectors

Question 7

Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.

Please explain as fully as possible why information is not being shared, detailing what the barriers to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.

(a) The BBA believes that the sharing of electronic information on fraudsters between the UK Identity and Passport Service, the DVLA and the financial services industry would significantly enhance the ability to identify individuals in compliance with UK anti-money laundering requirements and reduce the opportunities for and incidences of fraud. The banks are only interested in the data held by the IPS and DVLA that relates to fake and fraudulent passports and driver's licences. There is no suggestion the bank would seek to receive genuine or clean data held by these bodies.

The banking and financial services industry has well established processes to manage and share personal information on individuals seeking to access financial services. This information is maintained and stored in strict accordance with current data protection laws and principles, and with due regard to customer confidentiality.

The vast majority of this information relates to individuals and companies with no connection to fraud or other criminality. However, the sharing of confirmed fraud data across the industry has been recognised as an effective tool in maintaining the integrity of the UK financial sector. The Government Fraud Review highlighted that effective sharing of data on actual and suspected frauds across the public and private sectors is the key to improving the UK's response to financial crime, estimated to cost the economy at least £14bn a year.

The sharing of information on fraud and financial crime not only reveals the full extent of criminality but also provides an additional resource to facilitate successful investigations and prosecutions. It also provides the platform to make more informed decisions in the processing of applications for products and services preventing potential fraud losses.

It is acknowledged that fraudsters target any weak link, whether in the private or public sector, or in the relationships between the two. They will often commit fraud against many different Government departments and private sector firms at the same time. In the majority of cases, criminals rely upon documents and other tokens fraudulently obtained from Government and its agencies to support attempts to defraud the banking and financial

services sector. In particular, the driver's licence and passport are, by being widely held across the UK population, two of the main tokens for establishing customer identity.

(b) It is worth noting that the rules on the sharing of information between two financial institutions in order to complete a police report appear under the Counting Rules introduced under the Fraud Act 2007. Under these rules, customers are required to report a suspected fraud to their financial institutions, rather than to the police, which means that the financial institution has to complete the preliminary investigation and make the decision, where it considers there is a strong enough case, to pass it to the police.

A 'pack' is then prepared for the police with all the evidence that is available to enable the police to make a decision on whether to proceed to further investigation and prosecution. In many cases of payment card, cheque or on-line fraud, the 'pack' for the police needs to include information from more than one financial institution. In some instances, financial institutions are concerned that s29 of the DPA does not give them explicit authority to do so whilst others believe they may be able to justify releasing information to another financial institution for this purpose under the s29 exemption.

This results in the police not being able to take on fraud cases that otherwise may have led onto a successful prosecution. Clear guidance on s29 would be beneficial. The Counting Rules, as described above, should also be clearer about the legal basis for data sharing between banks and this may reduce banks' reliance on s29.

(c) Turning to credit data and the industry's desire and obligations to lend responsibly there are currently a number of credit data sources which are not currently available to financial institutions. These include public records, such as utility bills, i.e. Council Tax arrears, council rent arrears, student loans, gas, water and electricity bills and information relating to Child Support Agency payments. Knowing whether customers are in arrears in relation to these payments is information that could usefully be shared with financial institutions to aid more responsible lending. Lack of information could disguise an inability to repay a loan. This might lead to a lender providing a loan in good faith, resulting in over-commitment by the customer, which would not be in their best interests. This demonstrates where inability to share data is likely to result in harm to the individual.

Other issues could be where two individuals are financially linked and one party has consented to the sharing of their financial information, but the other has not, so the information cannot be shared. Knowing about fines imposed by the Courts, where an individual pays a monthly payment to the courts could, again, help the lending decision process. These potential barriers can be overcome by a willingness on behalf of the controller to begin to share data (after obtaining appropriate consent) but better still by introducing enabling legislation so that all credit data can be shared. This is discussed in our response to the BERR consultation on the sharing of non-consensual data.

Question 8

Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.

Please describe the information-sharing concerned and why you believe it should not be taking place, including the risks involved in such information-sharing.

We have no comments to make in response to this question.

Section 3: The legal framework

The DPA regulates the processing of information, including its obtaining, holding, use and disclosure.

The second principle of the DPA is as follows:

“Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.”

Question 9

In your view, how well does the DPA work? Please outline the DPA’s main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

Overall our members are very supportive and think the DPA works very well and does not cause undue restrictions in relation to data sharing. In general we think its main strength is that it strikes the right balance between being suitably prescriptive to enable data controllers to understand their obligations whilst at the same time providing them with the flexibility to decide the most appropriate way for them to comply. As an industry, our members find that in general they are able to share data to the extent necessary whilst acting in accordance with the spirit of the DPA. Instead, we generally find that it is other laws that act as a barrier to data sharing. It would help if there were more statutes enabling government bodies to share information, such that the ‘legal obligations’ conditions and exemptions (contained in section 35 and schedules 2 & 3 of the DPA) could be further relied upon. It is often the common law duty of confidentiality that restricts our members from sharing information rather than the DPA, as the DPA has a number of grounds and exemptions which permit data sharing (e.g. s29).

However, there are a few areas where we think that clarification / additional legislation or guidance would be helpful, as follows:

Schedule 2 & 3 Conditions for Processing

The conditions within Schedules 2 & 3 of the DPA that provide for the legitimate processing of personal data and sensitive personal data are in our view too limited. Whilst the additional conditions in the Data Protection (Processing of Sensitive Personal Data) Order 2000¹ have assisted, there are still occasions where it is hard to share information where it would be beneficial to the wider public to be able to do so. In particular, an additional processing condition to enable non-consensual credit data to be shared for the purposes of fraud prevention and credit risk purposes (as outlined in our response to the BERR consultation, (see Appendix 3)) would be welcomed by our members.

We feel that either clearer provisions in the DPA are needed or more practical guidance on the scope of the processing conditions in Schedules 2 & 3.

There is also a disparity between the legal advice / legal obligation conditions that can be relied upon depending on whether personal data or sensitive personal data is being processed. Under Schedule 2 section 3 personal data can be processed where “*necessary for compliance with any legal obligation to which the data controller is subject*”. However there is a wider condition contained in schedule 3 section 6 relating to legal rights/obligations, whereby sensitive personal data can be processed where “*...necessary for the purpose of, or in connection with any legal proceedings...necessary for the purpose of obtaining legal advice...or, is otherwise necessary for the purposes of establishing, exercising or defending legal rights*”. It would often be helpful to be able to rely on this latter condition to enable data sharing when dealing with personal data in general rather than just sensitive personal data and as such would be helpful to have the schedule 3 wording also included in schedule 2. This would give our members increased legal certainty to share data both generally and more specifically with fraud prevention agencies such as CIFAS or organisations such as APACS that maintain fraud prevention databases for the banks, to defend their legal rights and those of their customers against fraud.

¹ Statutory Instrument 2000 No. 417

Under Schedule 2, paragraph 6(2), the Secretary of State may by order specify particular circumstances in which the condition in Schedule 2, paragraph 6(1) is satisfied. We believe that data sharing for the purposes of fraud prevention and responsible lending to reduce over-indebtedness is in the legitimate interest of society at large. Using this power, already enshrined in the DPA would seem to be a relatively simple and, hopefully, swift way of enabling banks to share data for these purposes without the need for individual consent.

Another difficulty related to these Schedule 2 and 3 conditions applies to obligations imposed on our members, and other organisations, to share personal data with regulatory bodies. Some of these requests are based on legal requirements, whilst others are made in the spirit of co-operation. Controllers face uncertainty as to what personal data they can and should disclose to regulators on this co-operative basis, where non-provision of the data may be considered as un-cooperative behaviour.

An additional layer of complexity is added where the request comes from an overseas regulator, which is a real issue our members who are global financial services organisations face. Section 35 as currently drafted doesn't enable a data controller to rely on a non-UK legal requirement as grounds for sharing/disclosing information. Also, would such a disclosure be covered by the legitimate interests condition contained in Schedule 2, paragraph 6(1) of the DPA?

Data sharing of “non-consensual” account information

Again, we refer to the 2006/07 BERR consultation on the sharing of non-consensual account data. The consultation recognised that the legal position is unclear as to the extent to which customer information can be shared between lenders via the credit reference agencies, for long-standing customers that may not have specifically indicated their “consent” for their information to be shared with the agencies.

We would recommend for the sake of clarity that regulations be introduced to enable non consensual account data to be shared with the agencies without the opportunity for consumers to opt-out. Such data sharing is in our view necessary within the financial services industry in order for businesses to satisfy their obligations for responsible lending. We are, however, of the view that such data sharing is, in any event, permitted under Schedule 2, paragraph 6(1) of the DPA, as it provides an adequate balance between the interests of lenders and those of consumers, without prejudice to consumers' rights and freedoms. However, more clarity in the law or guidance from the ICO relating to this section of the DPA would be helpful, particularly around when the processing of personal data prejudices the rights and freedoms of data subjects is considered ‘unwarranted’. For example, if the processing will expose the data subject as having committed fraud or another crime or acted dishonestly, or being over-committed to debt, would that be unfairly prejudicial?

The crime and taxation exemption (Section 29 of the DPA)

Some additional clarity would also be welcomed as to the scope of this qualified exemption. At present there is a lack of understanding as to exactly what falls within the scope of s29 and as such it may be inconsistently applied by data controllers. Further guidance from the ICO of the circumstances in which this exemption can be relied upon would be helpful. This would improve consistency of application across our sector, enabling organisations to all share the same levels of information for fraud prevention purposes. (See our response to Q7).

Subject Access Request Fees

Although not related to data sharing. We would also refer you to the response to the Information Commissioner's Data Protection Strategy document in relation to amending the fees chargeable for responding to complex subject access requests (Appendix 1, page 3).

Definition of personal data

Our members would benefit from clarification of what constitutes “personal data”. We appreciate the ICO’s revised guidance on personal data and look forward to the new guidance on what is “data”. However, in light of the *Durant*² case and more recently the *Ezsias*³ case there is a suggestion that the courts are not interpreting the DPA in the same way as the regulator and perhaps it would help if the DPA itself offered a more definitive classification. The courts appear to be interpreting more narrowly than the ICO.

We are of course mindful of the European Data Protection Directive (95/46/EC) and that any changes to UK legislation made to address any of these issues would need to be compatible with the provisions of the Directive.

Question 10

In your view, how well do public authorities and private organisations adhere to the second principle of the DPA? How valuable do you believe the second principle is? Please provide examples and the reasoning behind your response.

Principle 2, which is an expression of Article 6, 1 (b) of Directive 95/46 EC, provides valuable safeguards for individuals. The limitation of purposes for which personal data may be processed set out by Principle 2 supports the fair and lawful processing provisions in Principle 1.

Principle 2 is not, in our view, an unnecessary barrier to the disclosure and sharing of personal data.

Question 11

What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

As we have highlighted earlier in this paper, we believe that the main barriers that stand in the way of the effectiveness of the DPA lie around areas of interpretation and application (see our response to question 9). We have already commented on the recent developments in the courts on relation to *Ezsias*, and previously of *Durant*, which appear inconsistent with the interpretation of “personal data” by the ICO and would again call for clearer definition. Whilst this poses a challenge for our members it can only lead to further confusion for individuals themselves.

We are aware that the interpretation of certain areas of the DPA, particularly s29, can vary among data controllers which can cause barriers to legitimate data sharing, where there is a fear of “breaching the DPA”. We would support further guidance in key areas of the legislation, such as this to ensure that both public and private organisations act consistently and in compliance with individuals’ rights. Whilst our members are typically of the size where they have the ability to seek expert legal advice on complex issues, we recognise that this is not a feasible solution for all data controllers who could instead benefit from the publication of clearer guidance by the ICO.

We believe that, in respect to the nature of data sharing carried out by our members, data subjects are aware of how their data is shared (as we have explained in our response to question 10) and are receptive to data being shared in this way. We do, however, see barriers in relation to the sharing of non-consensual credit account data with CRAs.

² *Durant v FSA* [2003] EWCA Civ 1746

³ *Andrew Ezsias v The Welsh Ministers* [2007] All ER (D) 65

Question 12

What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA?

The ICO's enforcement powers

We are generally supportive of the Information Commissioner's recent call for the additional powers of inspection and enforcement. We fully supported the ICO's request in 2007 for the introduction of prison sentences for serious breaches of s55 of the DPA. We understand the ICO's desire to have the power to audit and inspect data controllers' DPA compliance measures without first having to obtain their consent. However, we would want to ensure that if such a power were introduced it would contain restrictions to ensure the protection and privacy of personal data that the controller is custodian for (e.g. customer records). We would also wish for there to be a further amendment to the DPA such that any information copied or removed from a controller during such an audit would not be disclosable under a Freedom of Information request – in the way that much information provided to the FSA is exempt (an absolute exemption).

We do believe it is important that the ICO is given the powers and resources in order to oversee and enforce the Act effectively. Particularly to enable it to take action against those organisations which deliberately flout the rules. We would not want to see the powers used against those organisations that are genuinely trying to comply with their obligations under the DPA.

Should the ICO at some point in the future receive the power to fine data controllers who contravene the DPA, we think the model the FSA have could be replicated (i.e. a reduction in the volume of the fine for co-operating with the regulator). We welcome his stated vision (in the ICO's Data Protection Strategy consultation) of adopting a responsible, measured and risk-based approach to data protection risk management.

We have seen an increase in the use of undertakings by the ICO over the last 12 months and would appreciate some clarification on the power to request undertakings, the circumstances in when undertakings will be used and when enforcement notices will be issued and the duration of such undertakings.

Security breaches

In light of the numerous security breaches involving personal information that have been well documented in the media in the past year or so, we support the Commissioner's call for reckless or repeated significant security breaches to be made a criminal offence in itself. However, "reckless" and "significant" will need to be defined clearly within the legislation for it to be effective. We are not sure whether volume of data, monetary value or risk of the data being used for fraudulent purposes would render breaches 'significant'.

Breach reporting legislation

Should such legislation be introduced, it is critical that a "reportable breach" is defined within the legislation. Our members would prefer to see guidance on when the ICO (and/or other regulators) would like to be informed of incidents where discretion on the part of the organisation is required, rather than a very prescriptive law.

We would have some reservations about the introduction of US-style breach reporting legislation, which would require organisations to notify the ICO, affected individuals and/or the media in situations where personal data are lost or stolen. Our view is that such legislation will only be of value if they offer real protections to individuals, for example where there is a real possibility that they will be exposed to fraud or identity theft or reputational damage. Otherwise there is a risk that a blanket requirement for organisations to report breaches to those affected will create unnecessary concern for those individuals affected, in situations where (a) the risk of fraud or identity theft or reputational damage etc is negligible,

and (b) the organisation has implemented measures to protect those consumers. Lessons can be learned from the US and looking at how the breach notification laws have developed over time. As each State introduced legislation, it learnt from the lessons of States that had already implemented such requirements.

We think that a harm based test would be appropriate. Please see our response to the ICO's Data Protection Strategy consultation for our discussion of a harm based approach (Appendix 1, page 2).

Our members would hope that there would be wide consultation on the introduction of any legal requirement to report breaches and would welcome the opportunity to contribute to that consultation.

Use and sharing of personal information in the public and private sectors Consultation

Question 13

Are there any other aspects of UK or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Please provide examples.

General

In the financial services sector the anti money laundering regulations, the banker's common law duty of confidentiality, the absence of consent from pre-existing customers, contractual arrangements with CRAs and various sectoral codes of practice all impact a bank's ability to share personal data. Much of this impact is negative in that it does not adopt a harm-based assessment and sets out a 'one-size-fits-all' approach. Many of the restrictions, if lifted, would enable responsible data sharing to take place without harm to the individual. Indeed, sharing often enhances an individual's ability to obtain a service they apply for, through more up-to-date and comprehensive information being available to lenders.

The law of confidentiality

The law of confidentiality adds another layer of data protection in the banker-customer relationship. However, the exemptions have been interpreted historically and narrowly to date. The obligation to retain confidentiality predates data protection legislation by 60 years and is a duty which is taken very seriously by Banks. The comments in this response are not intended to suggest that this duty of confidentiality should be watered down. There is no doubt that the DPA provides strong safeguards to protect the individual, but as discussed in this paper there are also areas which could be amended or conflicts clarified to the benefit of society in general.

As is well known, the legal case which defines a banker's duty of confidentiality is *Tournier v National Provincial and Union Bank of England* [1924]⁴. The case defined four areas where a duty of confidentiality is qualified. In the words of the Banking Code, which is based on this case law, these are:

- If a bank has to give information by law;
- If there is a duty to the public to reveal information;
- If the bank's interests mean we must give the information (for example to prevent fraud);
- If the customer asks the bank to reveal information or if the bank has permission.

As data sharing for fraud prevention and credit risk assessment purposes are recognised in the modern world to be of public benefit, it would be helpful if such data sharing were expressly permitted.

⁴ 1924] 1KB 461 CA

The greatest restrictions are around where there is a lack of consent. Specifically, as regards those customers where at the initial opening of the account, consent was not gained, as industry data was not widely shared at that time. This has led to an incomplete picture on a number of individuals' existing financial commitments. If schedule 2 para 6(1) were to be extended to include data sharing for the purposes described or if it were to be formally interpreted as to permit such sharing, it would have a positive impact on data sharing.

Human Rights Act 1998

In addition, where data-sharing is undertaken on the basis of Schedule 2, para 6(1), in considering the rights of the individual the ICO or the court would take into account the Human Rights Act 1998. The right to private life is qualified such that it can be interfered with where to do so would be, amongst other things, "in accordance with the law".

This has been interpreted, at European level, to mean that that there must be a specific legal basis for the interference - rather than that the interference itself is not prohibited by law. In the context of data-sharing between banks for fraud prevention purposes or for responsible lending purposes, there is no specific law setting out the basis upon which such data-sharing is permitted.

Public Sector Data

In the public sector, data sharing is inhibited by the various statutes that restrict the powers and activities of public sector bodies and on the whole this prevents the sharing of relevant data with the private sector. There is a great deal of public sector data which would greatly increase a lenders ability to fully assess an individual for credit (see Question 7 for details) in the majority of cases current legislation and the lack of will to obtain the necessary consent restricts the sharing of this data with the private sector.

Conclusion

Considering the fact that the government is challenging lenders to make changes to ensure they lend more responsibly, and given that the industry has made a number of changes to align with this and optimise its current use of available data, it is disappointing that legal restrictions and lack of public sector data being made available inhibits our ability to ensure a complete and accurate financial view of an individual.

Question 14

Are there any statutory powers unavailable that would enable better and more secure sharing of personal information– for example for identity authentication purposes – between a) public authorities and b) public authorities and private organisations? If so, what are they?

Please provide examples and any steps you believe could be taken to improve matters.

Please see our answer to question 7 and other comments in our response

Question 15

Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples. Please outline your proposals for streamlining the legislation to ensure that such burdens are minimised.

(a) Section 7 of the DPA relating to data subject access requests (DSAR) is, in our members' view too general and wide ranging. This has enabled the right of access to be exploited and abused to suit other interests, such as third party companies acting on someone's behalf in a claim or complaint. It has also enabled individuals to make requests that are not related to the identification of whether an organisation holds information about them and the accuracy of such information.

Banks have no wish to restrict the rights of individuals, particularly their right to access their own information. However, they do believe that such access rights granted under the DPA should be limited to relevant data protection or privacy purposes. If access to information for non-data protection or privacy purposes is required it should be enshrined in other laws more suited to the purpose.

The fee that can be charged for responding to subject access requests should also be reviewed and, perhaps, be set on a sliding scale. Our members accept that any fee must be realistic so that it does not prevent poorer members of the community from exercising their right to access their information, but the £10 fee has remained unchanged since the 1984 DPA and does not reflect the true cost of providing the information. Nor does it discourage frivolous or vexatious requests.

We recommend that any sliding scale should take into account whether the same information now being requested has already been provided free of charge previously. Any repeat requests for identical information should permit data controllers to charge a fee that more realistically reflects the costs to them.

(b) The 8th DP Principle is based on national legal boundaries and was drawn up when the internet was in its infancy. In today's electronic communications world, where the internet has no physical boundaries, it can be difficult for data controllers to comply with the 8th principle's requirements with confidence.

(c) We believe that the Information Commissioner should continue to maintain a Register of Data Controllers, but the current 'Notification' process is burdensome for the benefit that it delivers to the public. A much simpler register, limited to data controller's name and contact address ought to be sufficient. If there is still a need to specify processing purposes, it could also be simplified and limited to non-obvious purposes. However, we do not believe the current level of detail adds value to individuals and we realise it adds a considerable amount of work and expense to the ICO's already-stretched budget.

(d) There is a modern and recognised need to share personal data for credit risk assessment purposes as recognised by the House of Commons Treasury Select Committee in the context of responsible lending in 2004/2005. As already described, this causes conflict and confusion.

Similarly there is little case law on the public duty exemption to the law of confidentiality and this can create doubt where banks want to share data for fraud prevention purposes, either amongst the banks or with law enforcement agencies.

As already discussed in our response to the BERR consultation on the sharing of non-consensual data, if the purpose of the data sharing is for combined benefits to both the individual consumer and lender and it is supplied securely and in line with current industry best practice, the unrealistic obligation of gaining specific consent for pre-existing accounts should be relaxed.

To conclude, therefore, for the purposes of fraud prevention and responsible lending, current legislation should be broadened or clarified, with data-sharing being expressly permitted.

Section 4: Consent and transparency

Question 16

Is it clear whether and when you need individuals' consent to share information about them? Are you clear about the form that consent should take? Please provide examples.

Please provide details of any initiative you have been involved in that has been based on consent.

The First Data Protection Principle, together with Schedules 2 and 3, set down the conditions that need to be met in order to process personal data fairly and lawfully. It is clear

from Schedules 2 and 3 that consent is only one of the bases on which the processing of personal data can be legitimised and that an individual's consent is not required if one of the other processing conditions apply including:

- where such processing is necessary for the fulfilment of a contract
- where such processing is required by law
- where the processing is necessary for the purposes of the legitimate interests of the data controller provided such processing does not prejudice the rights, freedoms and legitimate interests of the individual

Although the DPA itself does not define consent, guidance can be found both in the definition contained in Art 2 (h) of the Directive, in the guidance provided by the Information Commissioner and in the decisions made by the Data Protection Tribunal. For example, it is clear from the guidance available that valid consent cannot be obtained through silence and the data subject should do something to communicate their consent such as returning a form or using an account.

The fact that consent can be withdrawn at any time means that it is not always practical for organisations to rely on it as the basis on which to legitimise their processing. For example, whilst individuals are likely to be happy to consent to their information being filed at a credit reference agency whilst the information is positive, it is likely that they would want to withdraw their consent as soon as the information starts to become adverse.

There are however, some examples of organisations relying on consent to share and use information. For example, the carrying out of a credit search (and the subsequent leaving of a footprint) by banks when individuals apply for credit is based on consent, as is the use of personal data for marketing purposes.

Fair processing notices vary greatly between organisations. There is some helpful guidance on the Experian web site at:

<http://uk.experian.com/corporate/compliance/fairobtainingclauses/index.html>

Question 17

What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.

Making it compulsory for organisations to gain consent to the sharing of personal information could be problematic for a couple of reasons. Firstly, as mentioned in the response to Question 16, the fact that consent can be withdrawn at any time means that it is not always appropriate for organisations to rely on it as the means of legitimising their processing. In the financial services sector our members regard 'consent' as an individual's agreement to the terms and conditions of a product and service, including the processing (including sharing) of personal data as described.

Secondly, as we mentioned in our response to the Consultation on the Removal of Barriers to the sharing of Non-Consensual Credit Data in January 2007, introducing a requirement for organisations to retrospectively obtain consent from existing customers is not practical for the following reasons:

- The great majority of customers would fail to respond or would respond unfavourably, probably because of mistrust of any form of data sharing.
- IT development would be needed to provide an indicator to show which customers had consented or had not. Depending on the circumstances, the lack of consent could lead to individuals having to be treated differently.

Question 18

Do you have any suggestions on how to make the sharing of information more transparent?

For example, should individuals be given strengthened access rights? And if so, how? Should organisations be expected to do more to explain their use and sharing of personal information to the public? And if so, how?

In order to comply with the First Principle of the DPA, data controllers are already obliged to give individuals a fair processing notice advising them how their information will be used and shared. Under the DPA and the Freedom of Information Act 2000 individuals have rights to see or receive information.

For example, when a customer applies for credit, all reputable financial organisations will tell customers how their information will be used, in their data protection statements and in the relevant terms and conditions. In addition, many will also provide documentation via their websites or branches on how customer data is used, where it is shared, and customer rights to access and correction.

UK banks advise customers that they will send regular account performance data to one or more UK based credit reference agencies, and this data is aggregated to show a customers total credit commitment when applying for credit. Individuals can apply to each of these agencies to see a copy of their information, and request correction or deletion where this is found to be incorrect.

We believe that there are already adequate and sufficient access rights to data for individuals in the UK with appropriate processes in place to correct or delete inaccuracies.

**Use and sharing of personal information in the public and private sectors
Consultation**

Question 19

How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?

For example:

In your view, how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information (http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf)?

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December (www.ico.gov.uk)?

Financial organisations are aware of their obligations under the DPA, and have processes and practices in place to ensure these obligations are complied with. Where data sharing takes place for example, with credit reference agencies, frameworks such as the Principles of Reciprocity are in existence to help ensure accountability. Good Practice is an essential requirement in all successful organisations, and one that has to be continuously assessed and updated to changing circumstances.

We welcome any initiatives that will assist data controllers in their compliance with the DPA. The Information Commissioner's Information Sharing Code of Practice converts elements of the DPA into clear usable processes, and can be used by all financial organisations to check and improve their own data sharing practices.

We believe that Privacy Impact Assessments (PIA's) could be used as part of an organisations best practice, to ensure that new initiatives address data security and privacy as part of any development plans. We do not believe this should be a legal requirement or compulsory across the industry, but used as a set of guidelines within each organisation's information sharing framework.

Section 5: Technology

Question 20

What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

Technological advances have overcome geographical and logistical constraints on sharing data, which means business can be conducted globally with speed and ease. The result has been a huge increase in worldwide data sharing. Wider, faster data sharing, arguably, means more opportunity for loss, corruption and disclosure of data, placing considerably more responsibility on data controllers to keep personal data secure.

Whilst there are dangers as outlined above, there are also a lot of positive outcomes from advances in technology. These include encryption technology and general electronic security measures built into programs and systems. The ability to share information electronically reduces the reliance on traditional transportation methods involving third parties, such as Royal Mail or courier. At the same time, the ability to store significant volumes of data on CD-ROMs or similar, whilst beneficial in itself in terms of reduced storage space can increase the risk of loss simply because of the minimal size of the storage vehicle.

On the whole, we believe that technological advances have had a positive effect on the sharing and protection of personal information. It is weaknesses in the corresponding operational controls that are the biggest threat to security rather than the technology itself. As long as appropriate policies are set and robust procedures are implemented and controlled, then it is possible to exploit the advantages of technology, whilst minimising the corresponding risks.

Question 21

Should the law mandate specific technical safeguards for protecting personal information?

For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?

Question 22

How, in your view, could 'privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research?

Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

The issues raised by these two questions are closely interlinked, so our response covers both questions:

The speed of technological change would make setting minimum standards in statute an unrealistic approach. It would also be self-defeating as in a relatively short time such a minimum standard may have become an unacceptable standard. If enshrined in law, that standard would give some irresponsible data controller's protection, but there would be potential harm to individuals.

Technical safeguards are widely available and affordable: there are commercially-available methods for secure file transfers that are robust yet easily implemented. A variety of simple yet effective 'privacy enhancing techniques' exist which, when used along with these technical safeguards, ensure a good level of security for personal information. Good security builds public and industry confidence, which in turn supports the expansion of activities involving the use of personal information.

Information and advice about using 'privacy enhancing techniques' and technical security measures are also widely available, and the current BS/ISO standards provide an excellent security framework for organisations choosing to adopt, or refer to them.

Commercially-available technical security measures are already widely used across a variety of industries, as are other 'privacy enhancing techniques'. Whilst the introduction of mandatory minimum standards would compel all Data Controllers to make use of them and provide a 'level playing field' of privacy and security, it would lead to the risks identified above.

The seventh Data Protection Principle, which allows a controller to take a responsible view of what are appropriate technical security measures are suitable, based on an analysis of the harm which could arise owing to unauthorised access offers flexibility, but lacks clarity.

The flexibility allows Data Controllers to balance security with practicality, but it is open to wide interpretation, something that could clearly be mitigated by the provision of more detailed guidance. Such guidance would be welcomed to provide greater clarity, but without being so prescriptive as to be restrictive either on large multi-national organisations or on very small organisations. Although there is a common need to protect personal data, there are very real practical differences in business need and capability between data controllers. A fine balance will be required to achieve the former while still allowing the latter.

Section 6: International comparisons

Question 23

Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Please provide examples.

We have mentioned on a number of occasions the industry response to the BERR consultation on the sharing of non-consensual data and the role the Credit Reference Agencies play in holding shared data. Emerging markets desirous of developing a robust consumer credit market all set up credit reference capability and make data sharing mandatory, (e.g. India, China, Japan). Likewise a number of more established economies are also adopting this model such as Greece and Italy. Spain has recently changed its position on positive data sharing to enable the credit bureaux to collect more data and the subject is also under discussion in Australia.

Use and sharing of personal information in the public and private sectors

Question 24

Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

See Q 23

Question 25

Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?

The approach taken in the rest of Europe can be very different from the UK. This is not necessarily as a direct result of DP laws, but stems in part from historical cultural differences where individuals have greater expectations of privacy than is perhaps seen in the UK as well as the effect of other legal obligations such as banking secrecy. The management/administration of credit files are very often, by law, decreed to be the responsibility of the central bank of the particular country and are not operated on a commercial level or available for use in a way not related to the granting of credit.

We are not aware of a particularly permissive country in the EU but think that several may be viewed as being more restrictive.

Generally personal data relating to offences, alleged offences etc can only be processed pursuant to the penal code or equivalent. In some countries individuals carry identity cards and are able to obtain certificates of good behaviour (effectively a police report) which can be used for identity verification/background checking.

Many countries include specific provisions within their laws regarding the 'interconnection' or 'combination' of personal data. If for example two databases created for different purposes are to be combined by one or more data controller, prior approval has to be obtained from the relevant Privacy Commissioner. (e.g. Austria, Luxembourg, France, Portugal,...) who will assess specific risks to the rights and freedoms of individuals.

Similarly, prior approval has to be obtained from the relevant Commissioner for processing personal data for purposes relating to the credit status and solvency of an individual unless carried out pursuant to law.

This report prepared by CNIL may be of interest, it refers to 'Bad debtors and fraudsters, central databases in respect of personal data protection' and can be found at:

<http://www.cnil.fr/fileadmin/documents/uk/CNIL-Blacklist-2003VA.pdf>

It is something CNIL have commented on more than once and 'blacklists' have been refused. On 13 April 2007, CNIL announced that it had refused a request from Experian to build a comprehensive database on the credit history of French consumers and firms as it was felt that the database would violate French banking secrecy and privacy standards.

Spain have recently amended their DP law (not yet in force and currently only available in Spanish) and there are now provisions relating to bad debts and credit reporting databases: "It reinforces protection of debtors by requiring that contracts contain far more specific information regarding the purposes for which the information shall be collected, processed and transferred; expanding liabilities for data controllers who use inaccurate information; obliging data controllers to delete records on debts after they have been paid; and generally banning the recording of information on non-performing loans before the debtor has been properly informed.

Furthermore, starting on the effective date of the GDPR such recording of information shall be linked to a claim (before a court of justice or otherwise)." (Comment by DLA Piper).

In October 2002, the Article 29 Working Party adopted a paper entitled 'Working Document on Blacklists', (WP65). WP65 looked at the establishment of databases for the purposes of debtor records, solvency and credit, criminal offences, fraud detection, etc., including the differences between countries and the applicable requirements of the Directive. [Essentially all of the databases that banks would like to see created/enhanced through data sharing.] Two fundamental conclusions were drawn "the incidence, prejudicial effects and consequences of this kind of joint file for individuals' private (and social) lives, and the existence of clear discrepancies in how this kind of file is regulated and used in the Member States." The Working Party called for harmonisation in this area. The paper is still of relevance.

Question 26

Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

Section 7: Additional questions

No specific examples. The differences are often cultural as stated above. For example we understand that in India individuals will be more open about discussing their financial affairs and this means that third parties will often discuss the financial affairs of others.

Question 27

Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering?

See response to Q28 as we believe these questions are the same in essence.

Do any of these issues apply specifically to your sector?

No

Question 28

Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

There should be a cross reference to the Justice Committee Report on the Protection of Private Data to ensure that any proposals for data sharing are aligned with that report as well as making reference to previous consultation exercises in particular sharing of non-consensual data, information sharing and data protection strategy as there is an obvious overlap.

The public's perception is that we live in a 'nanny state' and will see the prospect of increased data sharing as 'big brother' watching them. If the Government wishes to allow a greater flow of data between the public and private sectors there needs to be an educational programme to inform the public why there is a need for it including the benefits to individuals, organisations and to society as a whole i.e. reduction in financial crime, responsible lending etc.

[Ends]

Appendices (submitted as additional papers)

Appendix 1

BBA APACS joint response dated 28 September 2007 to the Information Commissioner's Data Protection Strategy consultation draft

Appendix 2

BBA response dated 1 October 2007 to the Information Commissioner's Framework Code of Practice for Sharing Personal Information consultation draft

Appendix 3

BBA response dated 11 January 2007 to the DTI (BERR) Consultation on the Removal of Barriers to the Sharing of Non-Consensual Credit Data (URN06/1357)