



**Response to the Consultation paper
on
the use and sharing of Personal information in the public and private sector
by
Richard Thomas and Dr Mark Walport**

Background

About Experian

Experian is a global leader in providing analytical and information services to organisations and consumers to help manage the risk and reward of commercial and financial decisions.

Combining its unique information tools and deep understanding of individuals, markets and economies, Experian partners with organisations around the world to establish and strengthen customer relationships and provide their businesses with competitive advantage.

For consumers, Experian delivers critical information that enables them to make financial and purchasing decisions with greater control and confidence.

Clients include organisations from financial services, retail and catalogue, telecommunications, utilities, media, insurance, automotive, leisure, e-commerce, manufacturing, property and government sectors.

Experian Group Limited is listed on the London Stock Exchange (EXPN) and is a constituent of the FTSE-100 index. It has corporate headquarters in Dublin, Ireland, and operational headquarters in Costa Mesa, California and Nottingham, UK. Experian employs more than 12,500 people in 32 countries worldwide, supporting clients in more than 60 countries. Annual sales are in excess of £1.7 billion.

For more information, visit the Group's website on www.experiangroup.com.

The word 'Experian' is a registered trademark in the EU and other countries and is owned by Experian Ltd and/or its associated companies.

Experian is the largest credit reference agency ('CRA') out of the 3 consumer credit reference agencies operating in the UK¹, supplying c80% of the shared personal data used for credit underwriting by the UK financial sector. This amounts to some 150m credit enquiries each year. Experian also provides data for a variety of other purposes such as identification checks for the prevention of money laundering as required under the Prevention of Money Laundering Regulations. Under Regulation 114 of the Representation of the People (England & Wales) Regulations 2001, the CRAs are the only non-public organisations entitled by law to hold the full Register.

Version: final
08/07/08
There are c 200,000 companies registered as credit reference agencies and licensed under the Consumer Credit Act. Most do not operate any form of operation for the support of credit decisioning but a few others do supply similar services for corporate activities. There are currently just 3 agencies in the UK that operate and supply consumer data for credit referencing purposes. Page 2

The Experian response to the consultation questions

Number	Question	Response
Section 1: Background		
1	<p>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:</p> <ul style="list-style-type: none"> • 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? 	<p>As the largest credit reference agency in the world Experian collects and processes a whole range of personal data on consumers, SMEs, limited companies, directors and partnerships.</p> <ul style="list-style-type: none"> • In addition to the credit reference business Experian also operates insurance databases for the insurance industry, permission based marketing databases, fraud databases and we also operate databases on behalf of others. We collect and share <ul style="list-style-type: none"> • Public information such as voters' register, county court judgments, bankruptcy and IVAs • credit account information covering account type, limits, balances and payment history , previous names, financial links to other persons (e.g. spouse) • Marketing data will include name, and address and often age and gender and may also include preferences • Insurance data will include policy type and claims information • Fraud databases will include data on known or suspected frauds • We collect personal data from authorised public authorities such as local authorities for the voters' roll, Registry Trust for County Court Judgements, the Insolvency Service for bankruptcy and IVA data and Companies House for directors' and shareholders' data. We collect personal data from lenders, insurance companies and other organisations and from the data subjects themselves. We hold all data on secure and discrete databases. We share such data to those authorised to receive it usually via secure connections or, in the case of certain consumers by mail in plain envelopes marked "Do not redirect". • The purposes vary but are usually one or more of the following depending on the data set concerned, the recipient of the data and the associated legal

		<p>permissions:</p> <ul style="list-style-type: none"> • Making decisions about lending, or whether to continue to lend, debt collections, tracing • Prevention or detection of terrorism, crime, fraud and/or money laundering • Making decisions about whether to send offers • Creation of permission based marketing lists
<p><u>Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection</u></p>		
<p>NB: Our response covers only the services we offer</p>		
<p>2</p>	<p>What in your view are the key benefits of sharing personal information to</p> <p>a) individuals</p> <p>b) society?</p> <p>Please provide examples.</p>	<ul style="list-style-type: none"> • Access to and use of credit information is acknowledged by governments and is supported by the World Bank as being of primary importance in the development of a fully functioning market economy. It enables consumers and businesses to get access to the most competitive deals fairly, swiftly and efficiently whilst enabling lenders to make effective decisions based on the widest and most up to date information available. <p>The UK has one of the most advanced credit markets in the world, which is made possible only through balanced legislation and access to a wide range of information through credit reference agencies such as Experian. The World Bank as reported in their annual “Doing Business” report has consistently judged the UK as the best in the world. You can find out more at http://www.doingbusiness.org/</p> <p>"Where credit registries and effective collateral laws are lacking - as they are in most poor countries - banks make fewer loans."</p> <p>"Credit reporting also is more valuable where it includes both data on defaults over the past 5 years and data on on-time payments. That allows lenders to evaluate the borrowing capacity of clients. And it lets good borrowers benefit from more and cheaper lending. For banks, past payment behaviour is the best indicator of future payment behaviour." All from "Doing Business 2008" published by the World Bank.</p>

		<p>Other data sharing initiatives hosted by Experian help the insurance industry to prevent and detect insurance fraud. The database hosting the motor insurance industry information is also used by the police to check for uninsured vehicles and by the DVLA for the very popular telephone car tax system.</p> <p>Experian authentication systems are used to ID consumers applying remotely for goods and services. This enables organisations to offer a faster, and easier service whilst at the same time reducing the potential for fraud.</p> <p>Shared data can make life easier and less hassle for consumers and give them access to goods and services they might not otherwise get. It reduces or removes the need for paper evidence (which can be forged) and ensures that all applicants are treated fairly. Lenders using shared data typically report a 10% increase in consumers given credit and up to a 50% reduction in arrears.</p>
3	<p>What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.</p>	<p>One of the key risks has been amply demonstrated recently with a number of data losses occurring largely in the public sector. The risks include the possibility of data being lost but also data being incorrect, inaccurate, incomplete or misused, which might result in an individual being refused access to goods and/or services or even becoming a victim of fraud.</p> <p>However, there are many and indeed often more risk if data is not shared. All of those things are possible when information is used or provided manually on each and every occasion that it is required.</p> <p>The fact is that the risks associated with sharing data are far outweighed by the potential advantages because those risks are much more manageable than the risks that occur when the data is not shared.</p> <p>The UK credit industry is an example of how to share data properly, accurately, effectively and safely and the advantages that have flowed from doing so are manifested in the economic growth that the UK has enjoyed.</p>
4	<p>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</p>	<p>Organisations or systems with inadequate controls impose the greatest risks. Often simple controls can make a big difference e.g. not sending out post in envelopes that make it obvious that the contents might be of value.</p>

	risks? Please explain the reasoning behind your response.	The greatest opportunities are those that enable faster and easier processing removing the need to produce paper documentation, in person so whether applying for credit over the telephone or renewing one's car tax consumers that are increasingly time poor are looking for technological solutions to solve everyday issues.
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.	<p>It is our experience that public authorities frequently hold too little information or inaccurate information. A good example is the Electoral Register, which is completed annually throughout England, Wales and Scotland. Despite the fact that it is common for persons of the same name to live together within a household, date of birth is not a common part of the data collected. This makes it hard to differentiate between persons of the same name. The credit industry and the ICO recognised this as an issue in 2000 and agreed that accurate identification of individuals so that their data could be fairly processed is only possible with a full name, date of birth and address. According to some high level research undertaken a few years ago, we calculated that there are only c120,000 totally unique names in the UK. More recently we have come across a household in Wales with 5 males with the same name.</p> <p>This issue also manifests itself in court records such as county court judgements of which less than 10% have date of birth. Data should be checked more robustly for accuracy.</p>
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.	<p>We do not consider that any private sector companies in our sector hold too much information. All financial services companies and, in particular ourselves, liase closely with the ICO and have documented retention policies too.</p> <p>There are however instances where information is incomplete or more information would be of assistance.</p> <p>In particular this manifests itself where an organisation commences sharing data with us and/or another UK CRA. Before doing so they will amend their application forms to include an approved form of words to</p>

		<p>notify the consumer that their data will be shared. Henceforth the lender will share all accounts. However, accounts opened before they changed their terms and conditions will not be shared until and unless they solicit and obtain the agreement of the account holder to do so. It is for this reason that some 40 – 50m accounts are still not being shared. The credit industry has moved to share all accounts that they possibly can in order to improve the coverage of information in an effort to reduce the possibility of further lending to individuals that are already indebted. Without full coverage it is hard for lenders to be sure they have full information on an applicant's indebtedness particularly as the applicant is unlikely to tell them. (c 66 – 70% of applicants inflate their income for example and a similar number are likely to omit commitments)></p> <p>This has been the subject of extensive consultation and is still under discussion with BERR you can see Experian's response to the initial consultation at http://www.experian.co.uk/corporate/compliance/datasharing/index.html</p>
7	<p>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.</p>	<p>There have always been issues in getting access to data from the public sector for use in the private sector. Even when data is made available the purposes are often too limited and important and obvious uses are not covered.</p> <p>For example: The data held on the full version of the Electoral Register is made available to financial services companies by credit reference agencies under the Representation of the People's Act Supplementary Regulation s114. It may only be used for assessing applications for credit or that may lead to the giving of credit and for checks under the Prevention of Money Laundering Regulations. So, for example, lenders may not use it to undertake fraud investigations once an account has been opened or for activities not associated with giving credit or checking to prevent money laundering. The barrier is legislative and although a number of small changes have been made to the permissions a number of other “no</p>

		<p>brainers” are still outstanding.</p> <p>When fraud takes place it often crosses between public and private sectors and yet, the public sector do not habitually share information with the private sector.</p>
8	<p>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.</p> <p>Please describe the information sharing concerned and why you believe it should not be talking place, including the risks involved in such information sharing.</p>	<p>We are only aware of cases that have already been reported such as organisations claiming to local authorities to be credit reference agencies. The local authorities are acting correctly, the companies themselves are not.</p>
<p>Section 3: The legal framework</p> <p>The Data Protection Act (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.”</p>		
9	<p>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.</p>	<p>In our view, the legislation generally works well.</p>
10	<p>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.</p>	<p>In our view the second principle can create a barrier to data uses that arise some time after the data was collected. There should be a general position that if the consumer agrees to their data being used in a particular way then that may occur irrespective of the purposes for which it was collected. There should be more flexibility within the second principle.</p>
11	<p>What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.</p>	<p>None, if the legislation is applied properly and use pragmatically</p>
12	<p>What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA.</p>	<p>For commercial organisations that stand to lose business if they are seen to be behaving irresponsibly with personal data; the concern over reputational risk is usually sufficient. There appears to be a different issue in relation to</p>

		the public sector where people have no choice about their data being supplied to them and cannot walk away.
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.	Under 95 46 EC DPD there is a big challenge in data sharing across border with EC Commission's drive for single credit market particularly as there are different interpretations within EU e.g. France The legal issue that is creating a problem for the sharing of historic account data (as mentioned above) in Q6 is the law on Confidence.
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.	Public sector organisations have access to documents and the data behind those documents that would be very helpful in confirming ID. As mentioned above there should be more cross sector fraud data sharing.
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.	Annual DP registration – not used by consumers, cannot be used as public declaration so what is the purpose?
Section 4: Consent and transparency		
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.	Usually, but further guidance on what may be deemed to be legitimate processing (without consent) would be helpful.
17	What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.	It is not always easy to obtain consent. Leaving aside s 28. 29 and 35 provisions there are also occasions when in reality consumers would have no objection to their data being used – particularly because it would make their lives easier – but who cannot be bothered to respond to requests or read documentation. This has been amply borne out by efforts made by one organisation to solicit retrospective agreement from their customers to share data with CRAs. Less than 10% of those contacted responded, those that did agreed, with just a handful objecting, the others probably just put the letter in the bin.

		It would seem therefore that unless consumers are notified at application obtaining “consent” at any other stage is often difficult, not because consumers actually object, they just do not engage unless they see a clear and immediate benefit.
18	<p>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?</p>	<p>The Consumer credit industry already has very comprehensive fair obtaining clauses which clearly explain what will happen http://www.experian.co.uk/corporate/compliance/fairobtainingclauses/index.html furthermore consumers already have special access rights under section 9 which entitles them to a shortened report covering consumer credit. These were developed in association with the Office of the Information Commissioner by Experian. It is our view that, in general, people only question data sharing when something happens that they find surprising, at that stage they may then actually go and read the terms and conditions to try and find out if what is happening is correct. For this reason the “booklet” seeks to offer very clear signposts so that a consumer can find their way around the document. In all cases it must be remembered that consumers almost certainly feel they are presented with such a lot of information that they will read that which they feel to be most important to them at the time. Thus, in a credit application they are interested in the financial information pertaining to whether they can have the money and how much it will cost them. What happens to their data is, at best, to them, a secondary matter.</p>
19	<p>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)?</p>	<p>The larger commercial organisations, particularly in financial services, are very aware of their obligations and usually have processes in place. Generally our experience is with smaller organisations where there is low awareness of such matters. Whilst useful it is unlikely that smaller less informed organisations will become aware of this resource.</p> <p>In respect of privacy impact assessments, many larger companies, particularly such as our own, already conduct a similar exercise.</p>

Section 5: Technology		
20	What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.	In our view, technological advances have made it easier to track when data is accessed and who by. For example, in the case of data held on CRA systems, all access is tracked through the means of an auditable “footprint” and systems are in place to detect unusual activity. Data can be protected, checked, verified and properly managed far more consistently than if it was held in a paper form.
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?	In the UK, DPA longevity benefits from its technologically agnostic position, i.e. it requires best available at the time. Were the Act to be more specific it could very swiftly become out of date and would continually be playing “catch up”. Drawing on our experience the most effective solution is for the ICO to put out regular guidance based on best practice.
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?	Further to the comments in the question above, commercial companies such as our own have, for years, been performing analytics using such techniques. This is best practice and yet again, the public sector could learn a lot from closer interaction with private companies for whom data is their business (rather than a by-product, which is the case for most companies). We suggest that the ICO could interact with interested players to produce definitive guidance on a regular basis.
Section 6: International comparisons		
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.	It is a feature of UK law that it is, in general, not retrospective. However, some emerging market countries are recognising that, in certain sectors, it is more effective to facilitate a certain amount of retrospective application of the law. In our sector this has taken the form of enabling data sets collected prior to implementation of certain laws to be shared without an obligation to obtain consent.
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?	In terms of the operation of a credit reference agency the UK is considered to be the best in the world by the World Bank. Many of the controls and practices that are in common usage by CRAs could and indeed should be applied elsewhere.
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?	In our view, the UK authorities have adopted a generally pragmatic approach for the mutual benefit of all involved – in other words, unlike some other countries, there is little evidence of “privacy for privacy’s

		<p>sake”. This is right and proper as the quite correct and necessary protection of personal information should not stand in the way of the pragmatic and reasonable operation of the day to day life of the data subjects themselves. Norway goes a little further than the UK in the area of data sharing making income tax records available for public scrutiny by anyone for a set period each year. However, they do not share as much financial information as is the norm in the UK.</p> <p>Eire on the other hand, has adopted such a restrictive regime that they do not even permit sharing of fraud information without permission. France, has one of the most restrictive interpretations of the DPD in Europe where only very limited data is shared and then only between banks. They have refused permission for the operation of a CRA in France and they will not permit financial data to leave France, even to another EU member. So, for example, information on a UK resident that might also own property in France and operate a mortgage and other accounts there cannot be supplied to the UK. It is unclear whether this is for data protection reasons or for another reason such as the protection of their own markets.</p>
26	<p>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.</p>	<p>There is no doubt that public attitudes to privacy and indeed what they consider to be sensitive does vary from country to country. In the USA for example people will openly talk about their income and their credit rating. In the UK, discussions about income and indeed expenditure are far more sensitive with many married couples being ignorant of the financial dealings of their partner.</p> <p>In France, the public is even more reticent about discussing financial matters. Yet, in India by contrast, subjects that would be taboo in many EU countries are the subject of public knowledge.</p>

Section 7: Additional questions

27	<p>Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering? Do any of these issues apply specifically to your sector?</p>	<p>The UK financial services private sector is the world leader in credit management and the public sector could learn a lot by working more closely with them. Several years ago, Lord Falconer observed this and even set up a mechanism to promote closer working. This petered out after just a few meetings, but maybe the time is right to look at this again. There is no doubt that many rank and file people in the public sector continue to be resistant to the idea that they should operate in similar ways to and co-operate with a commercial organisation. Perhaps the recent troubles may serve as a wake up call that something needs to change, and fast.</p>
28	<p>Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.</p>	<p>Consumers welcome developments that they see as a benefit to them, i.e. if it makes their lives easier. The changes to the car tax system enabling renewal by telephone have, as far as we are aware, not attracted any adverse comment. Yet, it evidently relies on data sharing from the DVLA, the motor insurance industry and the MOT testing garages. There are many opportunities for the public sector to get smarter with data and reduce duplication, improve efficiency and accuracy if new technologies and greater levels of data sharing and communication were adopted.</p>