

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

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?*

Comments:

Introduction

The CBI appreciates the opportunity to contribute to the review on the use and sharing of personal information in the public and private sectors. The Data Protection Act (1998) provides a valuable single legal point of reference for businesses in their collection and handling of personal data, against which they have been able to standardise procedures. Within a new and increasingly complex online environment, however, significant changes and challenges are occurring in the way businesses and individuals are or are not able to utilise the DPA as a realistic reference point. An extensive review of the Act is timely and valuable for all companies faced with the challenge of balancing their data protection, other compliance and commercial responsibilities.

As argued below, we do believe that the DPA is increasingly ill-focused for dealing in a realistic and effective manner with the issues thrown up by developing online means of generating, processing, storing and analysing personal information. Moreover, we also consider the framing of some of the questions in this consultation document, and its general line of questioning overall, to be so abstract as to be oblivious to the real dilemmas facing business, and to the important positive relationships that usually exist in the handling personal data between the overwhelming majority of businesses and their customers. A truly constructive and non-prejudicial review of the DPA that sought to improve this relationship and regulation of areas where problems either do or might occur in relation to contemporary practices based more of risk-based better regulation principles has yet to be initiated by government. Towards this end, we do try to suggest ways in which the rights of data subjects might be able to be strengthened through technological developments, the institution of sound standards and auditing procedures, and more focused and finer-grained regulatory approaches based on dialogue between the government and private sector actors.

Background

Across various sectors, CBI members collect a vast range of personal data regarding their employees, customers and suppliers. In some cases, they are required to do this by laws (eg, money laundering, equal opportunities, health and safety, etc.) increasingly requiring internal and supply chain accountability. More generally, they are experiencing profound changes in the way they, their suppliers, employees and customers handle personal and other important information in digital and electronic forms - in different combinations for a range of purposes via various physical media (USB sticks, laptop computers, etc.)

Companies endeavour to prescribe procedures for handling personal data on mobile media, and take advantage of high quality encryption and other security technologies as they become available. But there is always a balance that has to be made between controlling processes, investing in new technologies and allowing employees and customers to engage in innovative practices. Such flexibility is vital for innovating and improving supply chain transparency and responsiveness to customer demand, and in maintaining competitiveness in the face of growing competition from lower cost overseas competitors that can access UK consumers via the internet and World Wide Web. In particular, it is necessary to build more value-added services, customised to the demands of increasingly diverse customer markets – in this sense, personal data is a vital intangible asset for UK businesses (alongside with financial, operational and intellectual property) they seek to go up the “value chain”.

In short, risk will be relative and increasingly particular to the context in which a business is operating. And in an increasingly online world, such operational and commercial processes and risks are increasingly international rather than national. In such a situation, managing risk for personal is not entirely a paternalistic responsibility on businesses but also very much a matter of shared responsibility and common interest for businesses, individuals and governments. The CBI has an obligation to identify how such responsibilities can be engaged and advanced.

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.*

Comments:

We believe this question as it stands unhelpfully invites leading and open-ended speculation as to the abstract interests of atomistic “individuals” and reified “society”. This may be appropriate regarding the en masse experience of people in relation to monolithic or law enforcement state institutions with general coercive power. But, in the context of an increasingly pluralistic society in which groups and individuals are able to exercise significant and increasing choice that can determine organisational responses, their actions in relation to specific social structures (eg. consumers in relation to businesses) will often be more telling than philosophical speculation in relation to their abstract nature.

The question avoids explicit reference to the issue of business/consumer interaction, even though a vast amount – if not the majority - of data sharing occurs in relation to such interaction. Sophisticated data sharing and storing technologies enable businesses to share information and communicate and interact increasingly quickly and more efficiently with employees, customers and business partners. This enables them (particularly SMEs in developing overseas market and international competitiveness) to deliver higher value services in ever-more customised goods and services to customers. Such interaction is overwhelmingly done through the active choice of individuals as a result of the benefits they receive. As a result, consumers can often feel empowered as proactive determiners not only of providers their own information but, increasingly with social networking technologies, of how it can be shared with others customers and businesses.¹

Two qualifications need to be noted. First, this argument is not to suggest that all individuals are similarly empowered, or that consumers have absolute determination over the choices available. For example, they may or may not choose to register and get the benefits from a store card; they cannot entirely determine the benefits they get from a store card, or **exactly** how their information will be used, but only generally - though with some new media they are getting increasing choice even in this regard.

Second, many consumers may also not appreciate the consequences and eventualities described in legalistic privacy policies and guidance. But, equally, many of the benefits to individuals - and, through businesses, to society - from sharing personal information are obscured or downplayed by the over-extensive concept of the “surveillance society” that fails to distinguish between different types of user or behavioural tracking and surveillance proper, and between beneficial and harmful outcomes. This concept (distinguished from the more specific and utilisable concept of a “surveillance state”) implicitly rejects the positive, value-adding outcomes that can - if carefully and intelligently constructed and regulated - be co-determined by individuals, businesses and governments through sharing personal information.

Both these qualifications can, of course, apply to businesses in a new, fast changing and complex environment, particularly SMEs. The key point is that it is nowadays hard to discuss “the” benefits to “individuals” or “society” from “data sharing” because there is a growing plurality of benefits, individuals, social engagement and data that is or can be shared. Some of these may still relate to crude controlling forms of surveillance, but even in the public sector, this is beginning to give way to more nuanced and positive forms of benefit provision. As a way of reaching a more carefully focused construction and regulation of data protection laws within the new and complex online environment, the CBI has suggested to the ICO that it engage with the private sector in new ways to analyse in more detail how these evolving forms of data sharing influence relate to data protection risks. We expand on this proposal below.

¹ See CBI/Google Survey of Internet Trends for Business and Consumers, 2006, for both businesses' and consumers' view that the Internet empowers the latter relative to the former. Social networking sites – both general and company run, enable consumers to provide personal information and product comment over and above that which they choose to provide in the form of company loyalty cards, etc, explicitly requested by companies.

Question 3. *What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.*

Comments:

Our comments on abstract speculation as to “the” risks to “individuals” and “society” are also applicable to this question. The risks from poor data sharing procedures highlighted by the media in relation to recent security breaches have tended to be immediate ones to individuals through thieves able to use details such as names, addresses, National Insurance numbers and bank account details to commit identity theft and banking fraud. It has also been argued that the rapid increase in handling and sharing of personal information in both the public and private sectors increases the risk of “societal harm”, such as excessive intrusion into private life or the growth in a lack of trust in organisations’ use of personal information.

Whilst increased public awareness of data protection risks is vital, the danger is that (as indicated in the framing of some of the questions in this consultation document) the best response to these risks is seen as a one-size-fits-all approach to protecting personal data. The CBI believes that, on the contrary, the most effective way of protecting personal data is through relating security procedures to the sensitivity and value of the particular data in question. Personal data can be highly varied, and its value highly contextualised and individualised. Attempts at single approaches and solutions tend to lead to a box-ticking mentality over time that can make data more vulnerable, partly because criminals and others quickly figure out the nature of such static defences, and (as recent cases in fact indicate most tellingly) partly through organisational inertia and complacency. While immediate threats must always be guarded against, these longer term ones are in many respects where the greatest dangers lie.

Assessment of security requirements is best served by focusing on long-term, risk-based and targeted approaches to data protection. The ICO could play an important role in this regard, helping to develop realistic coordination between public and private sector actors around the information sharing initiatives, to clarify risk management practices and discuss standardised good practices and procedures. To do this, though, the ICO would need to change its hands-off regulatory approach to business aimed at specialised data controllers and processors to a more proactively engaged one aimed at a more general business audience (board level and below).

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.*

Comments:

The best ways of sharing information are those where security procedures are proportionate to the value of the data being handled. Customer personal data held by organisations is increasingly varied – its value lies in its specificity and is increasingly rarely realised (and can be evaluated as sensitive or not) in isolation, but only in relation to other data sets where the overall relationships can be analysed.

In other words, the “information” that can be gleamed about an individual from data depends

upon analytical capabilities rather than the data per se. As a result, protection of this information lies best in the manner in which databases and analytical and security software programmes are constructed and encoded. In this regard, one thing that the recent government breaches have highlighted is that large general databases are more risky than smaller, more specialised but linked databases.

The high level of personalised handling of customer privacy requirements means that technological developments in the field of “user-centric identity management systems” are very important in regard to their potential to:

- provide business with flexible levels of customer authentication adequate to support current business processes and regulatory requirements;
- provide the customer with genuine choices to control their exposure to privacy risks;
- naturally reinforce organizational best practices to implement the orthodox data protection principles.

The CBI would support a regulatory approach which facilitates market adoption of innovative privacy protection technologies, mutually benefitting the privacy interests of individuals and the need for continuous improvement in business performance.

Technology will, of course, not be enough and cannot relinquish organisations of their responsibilities for good practices. Underlying the ability to securely structure and encode databases and software is sound auditing of both the data itself (its authenticity and completeness), as well as the procedures for access and utilising these. Various security standards exist at national and international levels (BS7799 and its ISO equivalent, for example). BS7799 may be particularly beneficial in allowing security stakeholders in companies to drive through process change in the face of senior management scepticism.

In terms of more formal control, tScheme (<http://www.tscheme.org>) is an important example of an organisation offering certification of auditing procedures appropriate to different types and level of risk for trust services in the UK. tScheme has two main functions. It provides a forum for establishing a consensus as to what constitutes best-practice with regard to the provision of electronic trust services, including, in this context, aspects of data-sharing outlined in the Introduction to the paper. It then provides a framework whereby these best-practice criteria can then be audited against in order to achieve 'tScheme-approved' status. tScheme is already helping both the MoD and the DCSF in providing the appropriate audit regime for access to employee data and sensitive data on children respectively.

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.

Comments:

As our response to the previous question indicates, the CBI believes the real question that needs to be addressed is not of how much or how little data public authorities hold but the way in which they gain this data and then organise its storage, handling and sharing. The HMRC and other recent data breaches seem a classic example of a systematic failure in public authorities' procedures for ensuring personal data is protected by technical or procedural measures relative to the risk of a security breach. In this regard, it is also open to question whether the large single databases that were revealed to be being held were really necessary for the analytical processes necessary for their intended purposes. Whilst government departments may have had rules in place to ensure the security of personal information, it is clear that guidelines were absent as to how these were to be implemented in practice and procedures in place to ensure that they were followed.

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.*

Comments:

In relation to the sheer variety of personal data different private sector organisations may hold (every such organisation will hold various forms of employee data at a minimum), such a sweeping question appears difficult to answer if not dangerously simplistic. Any response as to how much is too much or too little would seem to be inviting dangerously all-encompassing conclusions. As already stressed, the important question in terms of risks and opportunities is less how much or how little data is held, so much as how it is gained, stored, analysed and used. Nevertheless, a number of drivers may be identified as causes of excessive processing of personal data:

- A supposition that data must have some value, and storage is cheap, so why foreclose a free option?
- Risk management methodologies that attempt to identify high-risk groups from behavioural data
- Antiquated regulation or other legal requirements which impose vague or excessive retention periods on business process data which bear little relation to real litigation or other business risks, but which “for a quiet life” it is simpler to fulfil through conservative retention policies.

These drivers, however, can be seen as largely legacy issues for businesses as they seek to develop the focused analytical capabilities that their long term competitive survival depends upon.

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.

Comments:

We are concerned that the failure of the government to defining a governance strategy for information assurance is undermining confidence in data sharing within the public sector within the context of recent revelations of data loses, inhibiting the public sector’s ability to develop modern delivery mechanisms. We are in communication with the relevant government agencies about how jointly government and the private sector can work together to address this issue.

We are also concerned by the government’s inability to assume liability for data losses or data errors. Companies need clarity on the transparency, scrutiny and accountability of sharing personal information within the public sector. The government’s ambitions for private sector involvement with information sharing initiatives are undermined by a lack of commitment to defining a governance strategy for information assurance.

Question 8.

Comments:

Section 3: The legal framework

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.*

Comments:

The basic principles of the DPA are generally sound. The value of the DPA is that it provides a single legal framework for handling personal data that businesses can refer to irrespective of their varying sectoral contexts, simplifying business planning and development.

However, a potential problem does lurk in the second part of the second principle, namely, that data cannot be "further processed in any manner incompatible" with the previously specified purpose. The problem here centres round interpretation of the word "incompatible" in relation to

"specified". In order to avoid doing anything that may be found to be incompatible, firms can find that they need to be so general in what they specify the data will be used for that it becomes almost meaningless, undermining the value of the requirement. If the specification is made too tight and meaningful, this can restrict firms' later ability to engage in legitimate service innovation and delivery.

An example of this issue arises in the flexibility businesses can require to adapt effectively to new forms of data sharing, such as user-generated content ("Web 2.0") and social networking services. Companies providing such services on the Internet can struggle to ensure compliance with the Act as they cannot pre-determine what personal data is submitted and how it is used by the provider and others – but will need to analyse what is provided to gain any insight into it. This situation in effect blurs the distinction between data controller and data processor in the Act. These innovations have allowed consumers to have seamless access to goods and services, adding a new level of complexity to the concept of an individual's access to their personal data.

The CBI considers that changes could be made to the Act to reduce the current regulatory conundrum created for businesses in this regard. Standards-based self-regulation supported by self-certification procedures could provide a way of giving companies an alternative compliance solution. Within this context, the ICO and the private sector could work together to identify standardised good practices and procedures for public and public sector sharing of personal information.

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.*

Comments:

In general, we believe most businesses manage to adhere to the second principle of the DPA. But their ability to interpret and adhere to data protection rules needs also to balance their need to share information in 'real-time' across the global – as a result of both competitive pressures and in order to meet compliance requirements in other areas and jurisdictions. In this regard, we believe the distinction between data controller and data processor and the concept of 'personal data' itself need to be re-evaluated in light of the complex and evolving digital and electronic environment, particularly in regard to Web 2.0 and other social networking environments. We believe the ICO needs to work with and engage the private sector to identify the day-to-day difficulties businesses are increasingly having in interpreting how the second principle of the Act applies and to engage with private

sector organisation to identify ways in which businesses can either effectively **and** efficiently meet the requirements of the Act or ways in which the Act and EU Data Protection may be able to be amended.

Question 11.

Comments:

Question 12. *What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA*

Comments:

Whilst we agree that all organisations need to take data security very seriously and that proportionate sanctions should be placed on those that knowingly breach the law, we believe a broader-based and better focused debate is needed on the ICO's proposals for greater powers and criminal sanctions. We are concerned that a long-term strategy to improve public awareness and law enforcement capabilities and governance of information assurance in the UK will be sacrificed with recommendations that focus on short-term, damage/risk-limitation recommendations.

In particular, calls from the Information Commissioner to be given the power to conduct audits of companies' personal data processing procedures without prior agreement seem heavy handed and blunt. What would be more effective would be a system of initial notification of concern and an **effective** enforceable subsequent power of auditing. While such a system may already exist in a formal legal sense, the Commissioner's call indicates that the system is not effective in reality; the CBI would prefer to engage in thorough substantive exploration of ways in which the system could be made effective rather than jumping to a heavy-handed power of intervention that does not seem to be based on better regulation principles.

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.*

Comments:

UK companies face difficult and at times contradictory legal issues when sharing information within EU Member States. The absence of an EU-wide procedure for the registration of company processing means companies have to undertake a time consuming procedure of registering the same processing in different ways across the EU. For companies operating in a number of locations in the EU, negotiation with one data protection authority would be preferable to negotiating with several as is currently the case.

We are particularly concerned with proposals from the European Commission for a breach notification requirement on the telecommunications sector. We have strong concerns over breach notification law being targeted at one sector; companies would incur an extra cost no matter in which form or to whom the notification would be made, inhibiting innovation and competitive potential especially within smaller ISPs. We believe detailed proposals and clarification of how breach notification could occur efficiently within the communications sector should happen only in co-ordination with a general review of how this might occur under the Data Protection Directive, which already obliges organisations to take measures to protect data against loss, alteration and unauthorised disclosure or access.

This should not be taken to mean that the CBI supports breach notification laws – as we

indicated in our submission to the ICO's strategy consultation, a simplistic catch-all approach may be counter-productive in addition to encumbering businesses with unnecessary burdens – what we are saying is that evaluation and implementation should not occur only at a sectoral level. As we stated at the start of this submission, we believe that the value of the DPD lies precisely in providing a single frame of reference for all businesses in relation to data protection that enables businesses to standardise processes; purely sectoral approaches undermine this benefit, particularly within the context of the convergence occurring with the communications sector.

More widely, international regulatory and data protection authorities need to work towards overcoming the patchwork of different obligations faced by the private sector. SMEs developing an international presence suffer from uncertainty on how to classify reasonable protection for different types of data. In particular the current approval procedure for the EU to recognise other countries' systems as adequate is far too time consuming and restrictive. The CBI believes where other countries have passed data protection legislation the UK should be seeking to establish prompter and thus more effective "findings of adequacy" rather than the often long drawn out process that currently exist or a search for equivalence. The ICO needs to articulate this as a matter of urgency to ensure the Directive provides an enabling rather than prescriptive approach to personal information sharing.

Question 14.

Comments:

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.

Comments:

The issues discussed are very inter-connected and require shared responsibility on the part of businesses, individuals and government in order to address the practicalities of domestic and EU law. As indicated above, we believe that making businesses alone responsible for data protection in emerging online environments places an unreasonable burden on them. What is need is simplification that benefits all actors.

Specifically, data retention requirements for different categories of data and different business sectors are determined by a complex patchwork of statutes, case law and regulations. This makes compliance with the data protection principle that personal data should not be retained longer than necessary both difficult and costly, and retention periods are in general disproportionately lengthy in comparison with the modern speed of business processes. Moreover, regulatory requirements for record keeping often insist on retention of transactional details which serve no business purpose and put the privacy of data subjects at unnecessary risk.

We recommend a comprehensive review of legally determined time periods for record retention, with a view to considerable simplification and harmonisation across sectors. This will result in vendors being able to produce records handling systems to implement the personal data lifecycle which are more standardised and cost effective for businesses of all size. Simply relaxing the application of the minimisation principle could increase risks faced by data subjects whilst not rationalising the underlying causes of burdensome complexity.

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.

Comments:

At a general level, yes; in some increasing and specific circumstances in relation to social networking and Web 2.0 situations, no. Again greater practical focus and simplification might be the best response.

The available exemptions to non-disclosure provisions (especially S.29 of DPA 1998) require the controller to exercise careful judgement over matters about which they may not be fully informed. Sectoral codes of practice could be agreed with the ICO, which indicated which types of personal data could be summarily released without risk of engaging an exemption. However, data controllers would need legal indemnification against challenges to such codes given the complexity and vagueness of the exemptions. Moreover the DPA 1998 has been abused as a catch-all saving provision in many other statutes, further ramified by secondary legislation. This has created an extraordinary level of interpretative complexity.

Question 17. What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning

Comments:

In general, a requirement for consent would only be sensible in circumstances where the data subject has a genuine choice. To ask for consent in circumstances where the impact on the data subject would make it unlikely that they would not consent is likely to de-sensitise them to this aspect of justifying processing. The danger then is that they may fall into the trap of consenting as a default even when there is a genuine and valid choice to make.

However, technological innovations might allow the better focused and more fine-grained approaches to be developed. Modern methods of user-centric identity management would permit seeking consent to share data on more of a per-transaction basis, rather than solely on "box-ticking" consent at the inception of a contractual relationship. Granting individuals more convenient and fine-grained control mechanisms to authorise data sharing will improve levels of customer trust, and overall levels of beneficial data sharing. The existing data protection framework does not provide intrinsic incentives for data controllers to invest in systems which offer individuals better control mechanisms to manage consent interactively.

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?

Comments:

Sectoral codes of practice could standardise methods of data subject authentication adequate to provide sufficient safeguards against unauthorized disclosure. Modern methods of user-centric identity management could be harnessed to provide immediate online access to personal data which did not risk engaging exemptions, which in many cases would satisfy the needs of data subjects without resort to asserting the right to "full" subject access. However the existing data protection framework does not provide intrinsic incentives for data controllers to invest in systems to provide quick access to the broadest range of eligible personal data.

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:*

Comments:

The CBI welcomes the recent consultation from the ICO on sharing personal information. However, we are concerned the ICO has shifted a number of expectations onto businesses that are not easily achievable in reality. In this regard, guidance provided within and updating of the notification process might be useful. We believe a comprehensive review of the notification process is needed, including its strengths and weaknesses, to help both the ICO and businesses better understand regulatory needs relative to different and evolving on and offline practices.

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.*

Comments:

As indicated, rapid technological advances that now enable companies to share all kinds of data, particularly in digital and electronic form, are having profound implications for the protection of personal data. This technological evolution is rapid and ongoing.

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?*

Comments:

We believe the government should not mandate technical safeguards for the sharing of personal information. Such a move would stifle companies' innovative potential and is an inappropriate 'quick-fix' solution that would rapidly become outdated. The ongoing transformation of the Internet and telecommunication technologies, such as next-generation networks and greater convergence between different media, is likely to present additional problems for the management of personal data. This dilemma can only be resolved through a less legalistic, more targeted and fine-grained approach to working out practical implementation of data protection requirements by governments and the private sector.

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?*

Comments:

The use of PETs to securely share information is growing in the private sector. A recent example of PETs includes software that allows browsers to detect automatically the privacy policy of websites and compares it to the preferences expressed by the user, highlighting any clashes. There is a growing market in software that aims to provide a better balance

between security and privacy, using anonymisation technologies.

However, the issue that needs to be addressed is that there is in reality little business case for data controllers to deploy advanced PETs. The return on investment for reducing the privacy risk to data subjects needs to be made clearer if data subject risk awareness and vigilance is insufficient to engage competitive market forces. As argued in our submission to the ICO's strategy consultation, such a major awareness raising exercise requires a higher profile, better coordinated and more concerted effort involving government, the ICO, business and consumer organisations.

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.*

Comments:

The CBI, along with our partners in BIAC, the private sector representative to the OECD, has been preparing a catalogue of privacy laws within OECD countries, their overlaps, contradictions and gaps, as well as a "heat map" their relative negative impact on business. The ICO will have access to this catalogue and heat map through the OECD ICCP Working Party on Information Security and Privacy Working Party in the lead up to the OECD Ministerial meeting in Seoul on 17-18 June this year.

Question 24.

Comments:

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?*

Comments:

Despite any criticisms we may have, in comparison to many other countries, the UK is in many respects an international leader in the regulation of personal data and engagement with business issues pertaining to data sharing in the public and private sectors. The CBI is committed to continuing to improve its coordination with the ICO in furthering this capability at an international level.

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.*

Comments:

It should be noted that public attitudes to the sharing of personal data, and what is considered a matter of privacy and in what contexts, are in many ways quite distinct to different historical, national contexts. Such contextual concerns may even be changing rapidly between generations in particular countries as technological understanding and experience varies increasingly between generations within the same countries. Regulatory

approaches to data sharing by businesses and the public sector may have to consider this in relation to different user groups.

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:

