

Intellect Submission

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

February 2008

Russell Square House
10-12 Russell Square
London WC1B 5EE

T +44 (0) 20 7331 2000
F +44 (0) 20 7331 2040
www.intellectuk.org

Information Technology Telecommunications & Electronics Association

Contact: Sureyya Cansoy, Programme Manager
Email: sureyya.cansoy@intellectuk.org
Tel: 020 7331 2049

1. Introduction

Intellect is the UK trade association for the IT, telecoms and electronics industries. Its members account for over 80% of these markets and include blue-chip multinationals as well as early stage technology companies. These industries together generate around 10% of UK GDP and 15% of UK trade.

Intellect welcomes this opportunity to respond to the government's consultation on the use and sharing of personal information in the public and private sectors. This document summarises the views of our member companies and is intended to provide answers to, or comments on, a number of key questions posed in the consultation document.

2. Answers to specific questions

Question 1: Please explain what your interest in information sharing is.

Intellect members have an interest in information sharing for a variety of reasons. Member companies:

- own products that are used within the public and private sector, which enable the sharing of information across organisational boundaries
- offer security and information solutions, which involve the operation of systems that contain extensive and varied personal data
- may be interested in the relationship between evolving technology capability and policy areas (particularly systems integration companies)
- are employers that share information about their staff and associates with suppliers, customers and potential customers
- hold information about clients and consultants that is provided by individuals and companies for the purpose of advancing business, and promulgate that information amongst clients to advance their business and to assist consultants in finding assignments

As a result, Intellect can bring a broad range of cross-sector experience and expertise to bear on this issue, and is able to share insights into best practice.

Question 2: What in your view are the key benefits of sharing personal information to a) individuals and b) society?

In the view of Intellect member companies, the key benefits for individuals of sharing personal information is improved and personalised access to services, including:

- faster transactional settlements
- a better continuum of care, as a result of the improved communications
 - between professionals who are able to cross-reference of data
 - between business processes, which automatically activate associated rights or benefits thereby ensuing consistency in the treatment of individuals
- the avoidance of repeated use of unsecured media (eg, through telephone, kiosk interaction)
- the ability for individuals to update or correct data at its source eg, the DVLA vehicle licensing system, which correlates vehicle ownership with motor insurance
- the ability to utilise risk focused systems that are better able to protect vulnerable citizens or those in danger

For society the key benefits of sharing personal information include:

- a reduction in administrative costs where information on the same person, household or address can be filed once
- a reduction in social security fraud
- an improved ability to protect life, prevent serious crime or uphold national security
 - most people would have raise few objections to invoking national legislation to cover these eventualities, although that is not to say that data and information on individuals should be stored or accessible in systems that are under the direct control of central government – rather that an appropriate governance and

approval process is required that demonstrates that an individual or group of individuals poses a 'society risk' (in approved cases data can be 'pulled' from the necessary systems)

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

In the view of Intellect member companies, the key risks to **individuals** associated with the sharing of personal information include:

- the replication and ossification of error, leading to compound difficulties for the individual
 - the failure of data users to update or correct data in a timely fashion eg, London congestion charge fines being imposed on the previous owner of a vehicle when DVLA records have been slow to update
 - anonymous and untraceable errors and an inability to correct them eg, individuals recorded as deceased even when they are very much alive
 - a lack of clarity around accountability and the correcting or erroneous data
 - confusion of identities
- vulnerability to insider abuse, interception and mishandling - which can lead to associated costs for the individual, embarrassment, reputation damage, identity theft or discrimination
- through
 - the discovery or leaking of confidential information, particularly where there is no reasonable audit trail
 - the aggregation and analyse of data beyond the original need, where the data is used beyond its published purpose and there is no entitlement to do so eg, congestion charging according to vehicle ratings
 - new uses of old data eg, health check-up data which lead to increased medical insurance costs following the result of an unrelated accident or attack

For **society** the key risks associated with the sharing of personal information include:

- routine abuse that leads to common mistrust and ultimately a fear of 'authority' eg, suspicion around the apparent need for organisations to collect data about the ethnic origin of individuals during the application process for a simple service
- the embedding of a widespread culture of mistrust eg, a situation whereby large numbers of individuals feel it necessary to change their mobile phone numbers, banks and insurers on a regular basis to avoid being 'traceable'

Intellect member companies have also identified **design risk** an important issue that should be taken into consideration. Design risks can materialise when there is no clarity about information sharing procedures at the technical level (ie, in terms of rules, regulations and guidelines) on how to handle information properly and on how the individual should be treated.

- IT design is usually conducted on the assumption that the system is usually correct: where there is a divergence between the information on the database and that provided by the individual, there is a risk that data users will trust the database without giving due consideration to the needs and situation of the customer eg, the chasing of someone for payment of a student loan when the account has been paid off.
- Assumptions in system design are always difficult to legislate for.
 - The Department for Work and Pensions (DWP) 'Change of Address', for example, can identify a pensioner as an addressee even though other records show them to be mentally incapable and that a relative has assumed power of attorney. This can lead to a situation where correspondence goes astray potentially resulting in non-communication, litigation, remedial action, unnecessary costs etc. Even simple 'change of address' procedures need to be tightly defined in order to avoid a chain reaction of mistakes.
- Assumptions about data security and confidentiality risks that are made by designers and individuals need to be understood, even as they continue business-as-usual activities. Recent high profile data losses have raised concerns that government is generally too relaxed about data security, and one possible response to this would be to redefine data classifications so that one item of personal data may be considered

'private' or 'restricted', but large quantities (eg, 10,000s) of these items attract the same security handling requirements as one item listed as 'secret'. Treating bulk transfers of personal data as secret would have obviated the recent HMRC and NHS incidents.

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?

Intellect member companies consider the greatest opportunities for information sharing to be around the supporting of direct care or service provision at the local level, through the sharing of information between delivery partners and their staff for a specific event episode. This should deliver optimum value to the citizen and improve the overall improve efficiency and effectiveness of the service delivery.

For this purpose, information can be shared through secure electronic messaging based on citizen consent (rather than on volume data transfer or the exchange of paper between agencies). Indeed, a 'clearing house' method that involves an index (or token) which is exchanged between data centres and which maintains separation at the source of the data, guarantees a degree of accuracy.

On the other hand, the government's ability to authenticate information that individuals or organisations purport to be original is a major risk. The sharing of information should not, in itself, be feared if the correct levels of access are in place and the security of the original records is not at risk. However, too many organisations (public and private alike) demonstrate a lackadaisical approach to data authentication frequently leaving this to personnel who are not in a position to prove whether data is genuine or has been tampered with.

The potential impact of cumulative errors (a 'domino effect') across different systems must be mitigated at the design stage. Furthermore, information must be understood within the appropriate context and a loss of context - when a database, for example, is prepared in one domain but viewed another - can lead to inappropriate assumptions that have widespread implications.

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.

It is not, perhaps, a question of whether public authorities hold too much personal information, but rather that too much information is available to too many people, eg, departments or offices that have access to information they do not need. Therefore, the correct levels of protection need to be in place. However, there is currently widespread concern that government does not fully understand or uphold data protection principles; that data collection is excessive; and that government is ultimately unaccountable for data losses. Public concern about the tracking of council refuse collections and how this might affect other decisions is a good example, which leaves the public wondering just how much data is going to be held by local authorities, and how might it be analysed?

Conversely there are examples where a paucity of data or information creates problems. Clearly, convicted criminals should not (for example) be able to evade capture simply by changing their name - systems should enable or enforce a linkage between the police and other data sources throughout address, marriage or name changes. Another example might involve NHS patients who are frequently asked the questions about allergies etc within different departments in the same hospital when information is not shared between internally.

Central government is often perceived as developing a national integrated data management infrastructure that which holds or enables access to too much information on individuals. More

controlled sharing of data at a local level (where most citizens interact with government services) would potentially enhance the citizen experience, reduce transactional costs and significantly contribute to improved outcomes.

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.

Intellect member companies suggested the following examples of where the private sector might hold or share too much personal information.

- Banks often hold large amounts of information about their clients, and some have struggled to merge and retain this information on a central database, which has led to a proliferation of data, inaccurately targeted communications, difficulty authenticating the original data and issues related to non-repudiation.
- Emails - many organisations have been shown to retain data for longer than required and fail to recognise that emails can often contain personal data that should be carefully managed.

Member companies also highlighted the fact that many large institutions in both the public and private sectors (banks, police forces etc) have significant legacy issues associated paper-based records.

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.

Intellect member companies identified the following examples of where sharing of information would be beneficial.

- Improved information sharing across and within strategic delivery partners at the local level would improve citizen centric service delivery. Historically there has been a vertical (organisational or departmental) focus to service delivery and data management in the public sector. Organisations or departments, rather than the citizen, have owned the data, and sharing of data has involved giving access to the whole record rather than restricted access on a 'need to know' basis.
- Healthcare environments have experienced similar issues to those at the local level, but have the additional problem of ensuring that clinical context is maintained where information is shared across conventional boundaries.
- Housing associations and local councils would benefit from clear guidance or practice on data sharing, which would benefit many young people and vulnerable applicants.
- Wider sharing of benefits-related data has the potential to reduce fraud where benefit claimants, credit agencies and banks etc are capable of handling data competently.
- Outsourced services would be able to provide enhanced (rather than disjointed) services in cases where the source data for both parties is legally bound.
- Surveillance - pursuing surveillance across multiple CCTV networks is currently difficult because the networks are owned by different organisations.

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.

Intellect member companies gave the following examples of where information is shared unnecessarily.

- Electoral role details – it would seem that information can be purchased from local electoral roll officers including names, addresses, telephone numbers etc. Personal details only declared on registration forms frequently come to light on circulars of a particular nature. There are no clear control mechanisms, meaning that members of the public can be put at risk from unscrupulous individuals.

- Bank details – the selling of extended warranties provides vendors with additional data such as 'bank details for direct debit'. In these cases, bank details are to be used for obtaining payment and should not be revealed to others either accidentally or deliberately. Examples of failures can include husbands and wives who might choose not to reveal address or bank details to each other and should not have this data accidentally communicated by defective business processes.

Trust must be restored in order to provide unequivocal assurances that data captured, stored or processed will only be used for its original intended purpose, and not used to routinely discriminate against individuals or group of individuals. There should be complete transparency around the capture, storage and processing of personalised data.

Question 9: In your view, how well does the DPA work?

Although there are some cases where the Data Protection Act (DPA) is abused, members felt that the key principles of the act are sound and have responded well to the test of time. Members felt that the real issues that need to be faced are cultural and behavioural, or around the business processes of data management controls (including IT security procedures) rather than the act itself.

The DPA's main weakness would appear to be the perception that it represents a simple 'tick in the box' process. This means that organisations frequently fail to link the DPA with broader information governance and assurance policies and procedures. Personalised data should be afforded the same controls that are applied to financial systems and should be considered a key area within corporate internal control processes, with a board level executive director nominated as the accountable officer. Compliance should be monitored according to corporate audit requirements and not left to the IT function. There should also be further alignment between ISO standards on data security and management and other industry standards (ITIL, CoBIT etc).

Intellect member companies identified the following examples where the DPA was considered poorly applied.

- Phone calls to customers from private companies who ask the customer to provide personal information about themselves before the call continues.
- Situations where individuals are asked to provide a broad range of private and personal details before they are able to access information about their own accounts and records (the key here is not so much to alter the act itself but to ensure that organisations understand and interpret the act correctly).
- Insurance companies, which determine their charges according to the postcode of the customer: the charging mechanism should be openly declared to the customer.
- Where transfer of data to other countries is not necessarily covered by equivalent DPA legislation, and not necessarily declared openly to the customer.

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.

We believe that the second principle of the DPA is valid and protects the individual from the inappropriate processing of data. However, it needs to be strengthened to address the systematic and seamless transfer of data across organisational boundaries where compliance with the individual 'purpose' becomes almost impossible. The ownership of the data could, for example, remain with the individual rather than the 'government' and the individual could approve access to data on a case-by-case basis (retaining the right to withhold access without compromise or penalty).

Question 11: What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

Intellect member companies felt that the following **societal barriers** stand in the way of the effectiveness of the DPA, and that these are the same as with any other mutual transaction: trust, confidence, respect, benefits, accountability and responsibility. Member companies felt that for 'government transactions' members of the public would give low scores for these values. Members suggested that the value of data needs to be better understood in order to ensure that it is treated with the necessary respect and is not give away too easily and is stored an transferred in an appropriate manner.

Intellect member companies felt that the following **institutional barriers** stand in the way of the effectiveness of the DPA.

- The Information Commissioner is
 - (a) not always able/available to help those seeking advice
 - (b) weak in prosecuting
 - (c) has little actual power to place sanctions on offenders
- An inability to authenticate the original records held on individuals (eg, the problems that Humberside police faced in the Ian Huntley case).
- A lack of clarity around responsibility for 'Information', which is often associated with IT although the Chief Information Officer (CIO) role covers IT systems and 'all business information'. The problem is compounded across government with a lack of clarity around who decides policy – the Information Commissioner, Cabinet Office, e-Champions, The National Archives etc.
- A lack of clear ownership or accountability regarding personal information at the corporate level. It is be rare that DPA is exposed to the same executive scrutiny as any other corporate asset and Intellect member companies suggested that industry standards on Strategic Asset Management would be a useful reference point. These standards emphasise the role of board ownership, combined with robust internal controls rather than an over reliance on IT processing functions to protect data.

In terms of **technical barriers** that stand in the way of the effectiveness of the DPA, Intellect member companies noted the following points.

- The process of DPA registration is confusing and often bypasses senior management. DPA registration should be audited and fines and prosecutions should apply. Accountable individuals should be required to register in order to set up trading websites or manipulate data before informing clients.
- The government's use of online and transmitted data, as well as private sector use of the internet, frequently does not follow appropriate procedures. While clear breaches of physical data (on CDROM for example) may cause embarrassment, the public perception is of more widespread systemic failure. The government should ensure that large quantities of data are ultra-secure, rather than 'adequate' which may be sufficient for individual data items.

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

Intellect member companies felt that the DPA is 'fit for purpose' but there need to be 'additional teeth' across an array of functions which enforce compliance (eg, the Information Commissioner's Office).

Citizens must also be put at the heart of information governance and Assurance. Ownership must be clearly defined, accountability must be transparent and purposes must be clear and fully understood by citizens. Citizens must retain the right to withhold personal information, or to revoke authorisation in reasonable cases, without fear of discrimination.

One of the major issues associated with the Act is the way that organisations interpret its contents and overcomplicate validation processes.

Members suggested that an annual fee and declaration, as well as an adjustment to the checklist, could strengthen the DPA. An example might read: 'my company does not run a website that exchanges any personal information' or 'my company does not transfer personal data to any organisation based outside the UK'. The fee need not exceed the current costs, but registration should become a persistent act, like VAT or MOT (eg, all company vehicles need annual road tax).

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.

The Freedom of Information Act and Human Rights Act may have an impact on data sharing or data protection, although we are not currently aware of any legislation that will have a direct influence.

Intellect members are clearly of the opinion that the issues surrounding data protection will not be addressed by additional legislation, but rather that the underlying information governance and assurance controls should be made robust and local 'Information Supremos' empowered to monitor and enforce compliance.

There should be a widespread understanding that data should not be retained for longer than required and training should be given to data owners in organisations in order to enforce this. An amnesty should also be given, but where necessary prosecution should begin after this.

The continuing absence of any data protection provision in the third pillar of the Act, and the inappropriate scrutiny and amendment route suffered by previous proposals, produces a dangerous lack of trust in data sharing with implications for crime.

Question 14: Are there any statutory powers unavailable that would enable better and more secure sharing of personal information?

Intellect and its members believe that Data Breach and Data Authentication would enable public authorities and private organisations to determine whether information has been accessed and changed, and would enable them to authenticate the validity of the original records.

Question 15: Are there any parts of the legal framework that place an unreasonable burden on business?

The legal framework places an unreasonable burden on smaller businesses, which should be able to operate without bureaucracy and making DPA registration easier might help to address this.

We are also concerned about the ICO's interpretation of data held as 'backup' ie, data that is not intended for reprocessing except in system recovery, this should be exempt from restrictive inclusion.

Other suggestions for improvement include:

- a simplification of registration processes
- the addition of an annual declaration to confirm that guidelines have been read and understood
- the addition of audit registrations, similar to VAT inspections

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.

In general Intellect member companies believe that the guidelines around consent could be clearer. For example, if a curriculum vitae is sent by email it is not clear to what extent the authority of that individual is required to a) make that information available to a client, and b) change/tailor the content of the document that is sent to the client (eg, to ensure that it reads succinctly).

From Intellect members' experience, it is evident that guidance around explicit or implied consent is more robust within the NHS, and that it is supported by legislation around access to medical records and legal guidance in the case of young people.

The area of consent in respect of information sharing between, say, local and central government is more difficult than the consent associated with a direct intervention. Many at the local level do not fully appreciate or understand the purposes for sharing information with central government, let alone understand how this data looks with respect to the government's broader information sharing agenda.

Members also noted that consent is often perceived by industry as a relatively easy hurdle to overcome. For example, US credit card companies will process personal data worldwide but seek to get a card signatory's 'acceptance' of this as a precondition of trading.

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

Intellect member companies did not necessarily feel that gaining consent was a barrier to sharing personal information. One suggestion regarding this issue was that it is a citizen's right to give a third party approval to share information, based on understandable 'terms and conditions'. For localised interventions consent can be obtained, on an event-by-event basis, and that the 'terms and conditions' can be explained on each occasion. Therefore, a credible move towards local integrated services supported by agreed care pathways should be manageable.

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?

Intellect and its members believe that the sharing of information should be more transparent and that individuals should be given strengthened access rights. Organisations should:

- make the information that they hold about individuals available to those individuals upon request
- state with whom they have shared that information and why they have done so

Further recommendations also include:

- placing the citizen at the heart of information sharing (as in service delivery)
- making custodians of data truly accountable
- considering the much broader system and implication of that picture when thinking about information and sharing
- ensuring that the difference between legislation, executive direction, management control and systems controls are fully understood by those providing information assurance
- making information assurance a key 'item' in every corporate report

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

We recommend that government takes an up-front and open approach about what information is collected, why it is collected, with whom it is being shared, why it has to be shared and how individuals can retain control of that information. Intellect supports both the framework code and the privacy impact assessment in principle, but would stress that the crucial importance of ensuring information security is owned at the most senior level

Regulatory Impact Assessments (RIAs) on centralised policy should clearly incorporate the impact on data management, including the increased use of aggregated data across many departments. However, this does not address how the impact is communicated to the ultimate owner of the data (i.e., the citizen). Other suggestions include data management impact assessments, conducted by cross-party agencies with objective assessors, shifting accountability over to locally elected establishments.

Question 20: What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

As with service transformation, technology is an enabler: the recent data losses were not technological issues but a corporate failure to maintain internal controls across shifts in technology and changing business models. Centralised data processing, for example, creates more corporate risks that need to be visible and managed than if the organisation was directly responsible for all data management functions.

Technological advance has delivered increased protection and security functionality in the guise of: encryption, access based controls, single sign-on, disaster recovery or the ability to track individual law infringements on a global basis. However, these technical solutions alone cannot prevent losses caused by poor management and processes. A significant culture change within government is required to prevent future high profile data issues.

Both technology and citizen expectations have rapidly developed during the internet age, particularly with respect to social networking, which has created a culture in which the sharing of personal data is widely accepted. However, in these cases the citizen remains in control of what information they choose to release and with whom they share it (a state of affairs that is not the case when citizens reveal personal data to government departments or agencies).

Technology will continue to advance but where the latest solutions are implemented they need to be supported by an appropriate investment in data protection and security at all levels. Furthermore, the national aggregation of data, powerful linking and analytical tools, and the growth of 'scrutiny' forums have certainly created some challenges to the legal sharing of personal information.

The growth of the internet and advent of phishing have also made it far easier to acquire information about individuals. Because of the amount of information requested by financial institutions and government bodies, private information has been easier to obtain and the lack of security and good practice has meant that this information has been far more likely to fall into the wrong hands.

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?

The technology already exists to protect information, such as encryption and 'sealing' of data in both static and transient states. Introducing or mandating such safeguards may provide the requisite drivers to prompt government institutions to adopt this technology.

A mandate would be most effective in the form of a quickly updatable standard issued by the ICO detailing minimum expected standards dependent on the actual data elements involved, the nature of the individuals involved and the scope/number of data subjects included. The type of information being held and the device in question are both relevant to the level of protection, which is mandated. Any personal information held on a portable device should be subject to specific security measures and restrictions on its further use.

The vulnerability of the devices in question is an important factor. Personal Digital Assistants (PDAs), stand-alone home computers and databases managed across the internet all have different vulnerabilities which should be taken into account when drafting any mandate. Please note, however, that some members expressed concerns about a law that mandates to high level of detail but does not allow suppliers to encourage innovation and the freedom to shape their solutions.

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?

Privacy enhancing techniques have their merits, but also carry cost implications that should not be ignored. There are also implications for authentication and non-repudiation of information in instances where multiple users wish to access or amend data such as patient records.

There is some concern that senior policy-makers in government do not possess the necessary depth of technical knowledge to make informed decision on the use and application of differing security solutions. Improved engagement between decision-makers and expert industry figures may help to alleviate some of these concerns.

There is also a need to fully understand the technical differences between the various techniques used to 'de-personalise' data. Pseudonymisation removes person identifiable data, but requires that a link must be stored which maps the output record with the input data. This is considered acceptable, so that if there are any 'time bombs' discovered within the data, the link information can be passed back to the data owner for action including tracking down the affected citizen.

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?

The HIPAA requirements within the medical profession in North and South America are good examples of where a standard has been established for the sharing of information contained within patient records.

Question 27: 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?

Training and accreditation of professionals is an area in need of further review. Government organisations need responsible officers with the necessary training and influence within their organisation to manage information security effectively. We believe that most data lapses and the consequent public mistrust are caused by a failure of senior management, rather than the technical solutions themselves. Senior managers generally require 'finance training', and similar information management training would be very useful.

Intellect's member companies felt that there is a need to look beyond the DPA and address areas like corporate responsibility, director liability and accountability, compliance with industry standards on data management and empowerment to act locally.

The Regulatory Impact Assessments (RIAs) should explicitly address information assurance. This would require a governance forum, constituted by suitable experts, to test policy and strategy assumptions, with observations and recommendations published through an independent agency.

Question 28: Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

Intellect members also made the following suggestions and observations that we believe will be of assistance to the review.

- IT facilitates data sharing and provides more sophisticated mechanisms for the protection of information than are possible with paper based information. Most examples of information loss or unauthorised access to IT systems result from a failure to apply these mechanisms. Proper audit trails and the enforcement of data encryption enable information owners to detect and confine information breaches.
- Thorough security vetting of every person that has access to information, combined with the enforcement of appropriate management procedures, is essential.
- Most of the recent public sector data losses have resulted from ad hoc, non-transactional requests, involving 'old' technology. In transactional systems sophisticated technologies are in place to secure the records.
- Information security should be enforced by the senior managers of organisations holding and using the information. Legal obligations on senior managers to enforce security, such as those for health and safety regulations, help to ensure that those rules are enforced. Information security could be assured by giving the Information Commissioner similar powers to the Health & Safety Executive (HSE), reinforced by severe penalties for managers who do not demonstrate best endeavour compliance.
- Broadly speaking the technology (eg, specific software applications) should help support the legal framework. However, there are cases in which policy or operating procedures may restrict overall capability.
- The ICOs office should develop a friendlier advisory role, or a split between 'advisor' and 'regulator' so that trust can be strengthened.
- In the current environment where government is not trusted with citizens' information, the work of the ICO is difficult. Regulation is not easy, so identifying and supporting small initiatives and success is a crucial way to gain trust.
- A 'clearing house' approach to sharing data could be a way forward, whereby anonymous tokens between systems and each data source maintains its integrity while allowing data to pass once the index has been checked and synchronised
- It will be impossible to eliminate human error completely; instead the government should take a 'measure twice, cut once' approach.

An awareness of the following legislation/standards should be useful:

- Evidence Seals™ support Electronic Signature legislations, which are now explicitly recognised in most international law
- UK Electronic Communications Act 2000
- European Directive 199/93/EC on a Community Framework for Electronic Signatures
- US-ESIGN (Electronic Signatures in Global and National Commerce) Act 2000, which also supports the standard code of practice for legal admissibility PD0008: 'a code of practice for legal Admissibility and Evidential Weight of Information Stored Electronically'
- And they support the standard code of practice for legal admissibility: PD5000 'An International Code of Practice for Electronic Documents and eBusiness Transaction' together with the authenticating documentary evidence in line with section 8 of the UK Civil
- Evidence Act 1995
- A report by the Children's Rights Alliance for England titled 'Children and young people talk about information sharing - Children's and young people's views and comments on the Cross Government Guidance on Sharing Information on Children and Young People'