



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

INFORMATION COMMISSIONER'S RESPONSE TO THE CABINET OFFICE CONSULTATION ON 'TRANSFORMATIONAL GOVERNMENT: ENABLED BY TECHNOLOGY'

Introduction

The Information Commissioner welcomes the opportunity to comment on the Cabinet Office's consultation documents on Transformational Government and the vision and strategies that are set out. The proposals engage a number of data protection concerns and this response sets out the data protection considerations that will need to be taken into account together with the opportunities that the proposal creates for strengthening public confidence in how their personal details are handled by government.

Background

The Information Commissioner's Office is the UK's independent public body set up to promote access to official information and the protection of personal information. The Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this paper are primarily from the data protection perspective.

The Information Commissioner has been actively consulted on various existing separate programmes for change, including Connecting for Health, reform of the Criminal Justice System and Child Indexes. In past years his

Office has also been consulted on many aspects of the existing systems that may be the subject of change under a transformational government programme. It is important for the Commissioner to have input to new initiatives to ensure that data protection implications are considered and compliance measures built in to programmes from an early stage in order to avoid any data protection non compliance issues once the schemes are implemented.

General Comments on Paper

In general, the Commissioner does not see any fundamental data protection obstacles to using technological advances to increase government efficiency and to improve and facilitate services available to the public. He can see that there are benefits to both the general public and to government itself. However, in order to benefit both groups it must not just be done to be in accordance with the law, it must be done in a manner that inspires individuals to have confidence in what is going to happen to their personal information and that any privacy risks to them are minimised. Just as the opportunities provided by new technology and new ways of working can be used to transform government services, these also provide opportunities to introduce a more privacy friendly approach to information handling, putting individuals more in control of what happens to their personal information.

The Data Protection Act 1998 provides part of the legal framework within which any such changes will have to be implemented and should help to ensure that such a programme maintains the trust of individuals in terms of how their personal information will be handled. Research by the ICO shows that most individuals (58%) feel that they have lost control over their own information and are increasingly concerned about what organisations do with it.

Whilst the document makes much of the fact that technology provides an opportunity to transform the business of government through solutions to

economic productivity, social justice and public service reform it should be recognised that just because the technology is available, it does not necessarily mean that it is always advantageous for the individual. Any new developments should include a proper consideration of the potential impact on an individual's privacy, the risks associated with this and how the technology can be best used not only to transform the business of government, but at the same time to protect the individual. As suggested in the recent Council for Science and Technology report on Better Use of Personal Information – Opportunities and Risks, the use of privacy enhancing technologies should be deployed where possible and their use should be considered throughout implementation of the strategy.

It is important, in data protection terms, that the mere technological capability to process personal information in new ways, such as wider information sharing, is not the sole driver for change. The desire to process personal information should be driven by substantial business need and compelling cases should be made out for the wider use/disclosure of individuals' personal details.

The consultation document itself makes reference to the fact that many current systems are structured around the "product" or the legislation rather than the customer (para 14); that systems have previously failed to provide the right information to the right person at the right time (para15); that public confidence in government's ability to deliver technology projects reached a low point by the late 1990s (para 17); and finally, that new risks to information assurance now exist: terrorists, organised criminals and hackers, theft of identity and personal data (para 19). Ensuring that data protection and privacy safeguards are built in to systems from an early stage would help address these issues.

In order to ensure that developments are taken forward in a way that considers their impact on privacy and thereby fosters public confidence the use of formal privacy impact assessments should be a feature of all such new developments. These are common in other countries such as the USA,

Canada, Australia and New Zealand and provide a way of assessing privacy impact at an early stage when policy makers and technicians have an opportunity to take developments forward in a more privacy friendly way whilst at the same time realising the business objective. In particular the US E – Government Act requires that all new developments involving the use of personal information go through such a rigorous assessment process. Adopting a similar approach with transformational government initiatives would help bring the UK up to the good practice standards that exist in other countries in similar contexts.

Although data protection only applies to personal data, building compliance in at the system design phase could have a positive impact more widely. For example, a requirement to hold personal data securely is one of the data protection principles (7th Principle). This principle recognises that as security technology and new threats develop security measures need reviewing regularly to make sure they are still appropriate. The principle also requires proper consideration of the potential harm which could arise from an unauthorised or unlawful processing of information or accidental loss or damage to information and to take into account the nature of the information to be protected. Assessing the risk and therefore the appropriate security measures needed at the start of a project allows security measures to be incorporated which are adequate for data protection compliance purposes and which also benefit the overall system helping build trust in that system.

The proposal to create a Service Transformation Board (in paragraph 29) to steer and coordinate the work of others is welcome. The proposal is that this should include officials from the wider public sector who run major services and consideration should be given to extending this to include those with substantial data protection and privacy expertise, perhaps including a representative of the Information Commissioner's Office.

Paragraph 30 mentions that this Board will signpost the potential of technology as well as promoting best practice and setting the overarching service design principles. The Board should also consider data protection and

privacy implications aspects of technology. In particular it could encourage an exploration of the possible use of privacy enhancing technologies as outlined in the recent Council for Science and Technology report. Just as technological possibilities have advanced in information handling so have more privacy friendly information handling techniques. Much work is still going on in this field and these developments, such as more privacy friendly ways to secure identity management, should be considered by the Board and be available to be deployed during new developments.

Paragraph 39 outlines the 'Shared Services' approach. This is broken down into eight areas to which particular attention should be paid. Given the Information Commissioner's statutory responsibilities and expertise he would expect to be involved in any discussions around data sharing, information assurance and identity management in particular.

Providing a single gateway to a wide variety of information held by the public sector may have some attractions both for individuals and government. However this is not without risk. Enabling staff, perhaps in a shared service call centre, to access a very wide range of personal information does run the potential risk of misuse by the staff concerned. There is already a thriving market in personal information and government held personal information is often the target of what has become known to some as 'information blagging'.

There have been a number of cases resulting in prosecutions by the Commissioner and cases have recently been reported in the media involving the acquisition of a substantial amount of personal information in order to commit fraud involving the tax credits system. Putting a wider range of information at the disposal of staff increases the likelihood that they will become the target for those who seek to misuse it. Whilst it is essential that adequate security precautions are deployed, including ensuring the reliability of staff, there is also a pressing need to strengthen the offence provisions at Section 55 of the Data Protection Act. At present these fall well short of a serious deterrent to the misuse of personal information as they do not include

the possibility of a custodial sentence. It is essential that these provisions are strengthened before a wider shared service approach is implemented.

In terms of identity management, transformational government activities represent an ideal opportunity to take forward many of the suggestions in the Council for Science and Technology report such as the potential for anonymisation/pseudonymisation of personal information where appropriate to minimise intrusion and privacy risks.

In the references to data sharing it is stressed that privacy rights and public trust must be retained. The recognition of this is welcome. The newly established Cabinet Committee Misc 31 will be considering issues related to information sharing between government departments and the Commissioner would expect to be consulted as part of this committee's work. Any personal information sharing between government departments must be in compliance with the Data Protection Act. Amongst other things consideration should be given to what information it is necessary to share, who has access to that information and what the individual understands about what will happen to their information when it is collected. As mentioned previously, the desire to share personal information should be driven by real need not mere capability. It is essential that the appropriate safeguards are put in place to ensure not only that data protection compliance issues are addressed but that systems of work foster public confidence rather than add to fears held by individuals that they have lost control of their own information.

Other Comments on Detail from the Paper

In paragraph 33(7) improving use of online access to personal records and data is suggested. Whilst this proposal may have benefits for the individuals, it does give rise to the possibility of 'enforced subject access'. This occurs where an individual uses their access rights when compelled by another to do so, being required to reveal their personal details to them for the other party's

purposes. For example, an individual may be forced to access their health information by a potential employer as part of the job application process. It is important that scenarios such as this are considered to prevent abuses of such services. At present the offence provisions at s.56 of the Data Protection Act which are aimed at dealing with enforced subject access through criminal sanctions have yet to be implemented. This should be remedied to provide a safeguard for individuals before wider access is available.

In paragraph 39(7) it is suggested that there should be wider use of the national insurance number. The Commissioner has significant concerns whether the existing national insurance number is robust or secure enough to be used as a single identifier for all government transactions. The number was originally generated for use in connection with benefits and taxation and with these particular purposes in mind. Whilst the number may still be fit for these limited purposes, it has its limitations and there has been no tradition of individuals keeping the number secure. If the number becomes a single reference to gain access to a wider variety of personal information held by government this poses a significant security risk. In any event if this number is to be used more widely than for purely tax and benefits purposes then it should be specified as an identifier of general application under Schedule 1, Part II, s. 4 of the Data Protection Act together with necessary safeguards.

In paragraph 46(4) the establishment of a Government IT Academy is suggested. This provides an opportunity to educate professionals in terms of data protection, including examining privacy enhancing technologies. Ensuring that this is part of the professional education and ethos of the Government IT Profession would be a significant step towards data protection compliance becoming second nature to those with responsibility for developing programmes that involve personal information.

In paragraphs 48-50 issues dealing with project delivery and supplier management are examined. The Commissioner is concerned that at present there is the potential for the need to incorporate data protection safeguards to be overlooked as they are not specified by government departments during

procurement and the supplier does not proactively suggest them. This runs the risk that systems may be non compliant with expensive remedial action required as happened in past cases. It may also mean that opportunities to develop more privacy friendly systems of work from first basics are lost. Ensuring that data protection matters are included in procurement arrangements is essential.

Conclusion

The proposals for transformed government by better use of technology do engage data protection concerns but these two public policy objectives do not have to be mutually exclusive. Ensuring data protection compliance and appropriate respect for an individual's privacy is an important objective, not just in terms of compliance with the law but also as an opportunity to foster public confidence in government information handling at a time when the citizen is increasingly worried over what happens to their information. It is essential that developments such as wider information sharing amongst government and shared service centres proceed on the basis of well justified need rather than available technological capability. Just as advances in technology mean that much more is possible in terms of information handling, the very same technology can be deployed in ways that enhance privacy such as through deployment of privacy enhancing technologies and identity management tools. Ensuring that data protection and privacy issues are considered at the outset is important and ensuring that privacy impact assessments are undertaken is a reliable way of achieving this objective. Strengthening data protection safeguards in areas such as more effective offence provisions to deter and properly punish the misuse of personal information is also vital. The Information Commissioner stands ready to assist with advice and guidance and looks forward to be invited to play an active role as the Cabinet Office takes the transformational government programme forward.