Information sharing in e-government initiatives: issues concerning Freedom of Information and Data Protection

Luciano Batista[1] and Marc Cornock[2]
The Open University Business School
[1] Lecturer in Operations Management, L.Batista@open.ac.uk
[2] Lecturer in Law, M.A.Cornock@open.ac.uk

Abstract
In e-government initiatives, the sharing of information is crucial for empowering citizens and boosting joined-up services. The lack of clear guidance on how to share government data can potentially harm Freedom of Information and/or Data Protection rights. This article addresses this issue by drawing from the main concerns governments have when dealing with Freedom of Information and Data Protection issues. As illustration, we comment on the findings of a case study we have conducted in a Local Authority in the United Kingdom (UK). Our findings show that local government managers might be struggling to adequately implement Freedom of Information and Data Protection aspects. Cultural aspects are subtly present in this context, as managers' values and beliefs regarding public access to information might be biased toward either information disclosure or information withholding.

Key words: Freedom of Information; Data Protection; information ownership; information classification; information sharing.

1. Introduction

The advent of new information and communication technologies (ICT) has opened the way for organisations around the world to establish new forms of communication with stakeholders. These new forms of communication are based upon electronic means and Web-enabled technologies such as the Internet and its variations (like the Intranet and the Extranet). By adopting these technologies, companies are increasingly becoming more available and responsive to their stakeholders, for Web-enabled technologies allow communication in a 24-hour seven days a week basis.

Being responsive is a fundamental issue for governments. Starling (2007) argues that responsiveness for government is more than to merely react to popular demands; it also means that government can take the initiative in the proposal of solutions for problems previously identified. Furthermore, governments seek to improve responsiveness in order to change the popular criticism that most public institutions are bureaucratic, slow, and incapable of taking immediate actions. Starling (2007) also argues that enhancing relationships with stakeholders is crucial for allowing government's prompt acquiescence of popular demands. These relationships comprehend initiatives such as providing information to the public, creating input channels for listening to the public, and improving the quality of public services according to the received inputs.

Governments around the world are deploying ICT in order to enhance the quality of their services as well as their responsiveness. In general, the use of electronic means by the public sector, in particular the Internet, in order to deliver public services in a more convenient and cost-effective way is termed 'e-government' (Holmes, 2001). The boundaries of e-government are not limited to the Internet realm, different authors mention that the territory of e-government covers both the administrative structures of the back-office and the points of access via electronic channels; hence, e-government involves modernisation of back-office procedures as well as modernisation of communication means in order to facilitate the delivery of services and enhance access to government services through increased availability of electronic channels (Dean, 2000; Harman and Brelade, 2001; Hoenig, 2001; Moulder, 2001). The Internet plays a major role in this context and it is changing the way people interact with the government. Public sector organisations are increasingly focusing on e-government initiatives in order to bring traditional services online. E-government initiatives are also empowering citizens and organisations in general to conduct transactions themselves, without the need to visit a government office or speak with a government employee (Sood, 2001).

A critical aspect to be considered is that e-government initiatives are opening or broadening access to government information, as they usually involve information sharing with the public and amongst public bodies. It may be argued that for e-government initiatives to be successful, information sharing is crucial for empowering citizens and boosting services jointly delivered by government agencies or departments. One important issue that emerges from this is that the lack of clear guidance on the legal framework for information sharing might potentially lead to two opposite scenarios: 1. the difficulty for accessing government information might act as a barrier against successful implementation of e-government initiatives; or 2. the open access to government information might pave the way for sensitive data to be shared without prior consent. Additionally, there are also cultural aspects subtly present within the two scenarios presented.

In this article we address the issues above by drawing from the main concerns governments have when dealing with Freedom of Information and Data Protection issues. First, we provide an overview of the main issues concerning Freedom of Information and Data Protection aspects. Following on from this, we address the fundamental concepts regarding information ownership and access to government information before discussing the differences between government managers' values and beliefs concerning information sharing. For this, we are going to comment on the findings of a case study conducted in a Local Authority in the UK. In this case, we have found that government managers might be having some difficulty to implement Freedom of Information and Data Protection requirements due to lack of clear guidance on the matter and also due to biased positions toward one aspect to the detriment of the other. Finally, before concluding, we discuss some practical implications of the issues addressed in the article.

2. Freedom of Information and Data Protection aspects

Freedom of Information and Data Protection represent two perspectives concerning information sharing. When addressing issues related to access to government information, different people and segments of society might express opposite interests, values, and opinions concerning Freedom of Information and Data Protection. They might also see the legislative provision for information sharing and protection, namely the Freedom of Information Act 2000 and the Data Protection Act 1998 as being mutually exclusive and contradictory with each other.

The purpose behind the Data Protection Act 1998, which as may be deduced is the earlier of the two, was to make legislative provision for the regulation of personal information. Personal information being taken to mean information that relates to individuals and, within the terms of the Data Protection Act 1998, is capable of leading to their identification. As will be seen below, there are different classes of personal data and the classes reflect how the data may be processed. According to the Data Protection Act 1998, section 1, processing of data refers to '*obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:*

(a) *organisation, adaptation or alteration of the information or data,*

(b) *retrieval, consultation or use of the information or data,*

(c) *disclosure of the information or data by transmission, dissemination or otherwise making available, or*

(d) *alignment, combination, blocking, erasure or destruction of the information or data'*

In addition, a number of rights were established for data subjects, that is, those individuals who are the subject of the personal data being processed.

The provisions with the Data Protection Act 1998 are based upon a set of principles that are designed to ensure that personal data is processed fairly and lawfully, this includes: the data being obtained for a specified purpose and not being processed outside of that purpose; that the data obtained is not excessive for the purpose for which it is obtained; that the data is accurate and up-to-date; that the data is kept only for as long as it is necessary to satisfy the purpose for which it was obtained; that adequate levels of protection re in place to ensure the data remains secure and prevent unauthorized use or against loss or destruction as well as providing for the protection of the rights of the individual whom the data concerns.

By its turn, the Freedom of Information Act 2000 provides for individuals and organisations to request information held by public authorities. The term public authority has specific meaning under the Act but may be taken to encompass all aspects of government both local and national and associated bodies. It does not cover privately owned organisations unless they are undertaking a role associated with a public authority.

Subject to the request being made in the prescribed format, unless the information is exempt from the provisions of the Act, the public authority has to confirm the existence of the information being requested and supply it within a given timeframe.

Information may be exempt from the provisions of the Act if they fall into one or more of a number of categories stipulated within the Act, these include: national security; personal information; defence, economic information; legal proceedings; and information accessible by other means.

Some exemptions are qualified which means that the public authority must make a decision as to whether the public interest in using the exemption outweighs the public interest in releasing the information. As a matter of principle, it is not assumed that information is automatically exempt because it relates to a category that is exempt if there is a greater public interest argument in releasing it.

Where an information request has been made but the public authority has not complied, the Information Commissioner's Office may issue an enforcement notice, a legal order requiring the public authority to address it's not compliance.

An interesting point relating to the provision of the Freedom of Information Act 2000 is that it is fully retrospective meaning that it does not just cover information that has been held since its commencement date. Rather, it applies to all information held by public authorities.

It may be seen that whilst the Data Protection Act 1998 is concerned with the safeguarding of personal data and preventing unauthorised access to it, the Freedom of Information Act 2000 is concerned with the disclosure of information held by public authorities and guaranteeing public access to information held by the government. Thus giving rise to the view that the two legislative provisions are contradictory and that it is not possible to fulfill obligations under both at the same time.

However, from a legal perspective the background and purpose behind the two legislative provisions are co-operative and not contradictory. Together the two pieces of legislation provide a mechanism whereby information may be shared with the public but that information deemed to be sensitive may be protected. Whether this protection is through exempting the right of access to it or by providing mechanism under which the use of data is regulated including preventing unauthorized access.

3. Freedom of Information and Data Protection concerns

The new ICT resources currently available in the market have brought with them an enormous capacity for information sharing and accessibility the humanity has never seen before. On the other hand, it is becoming increasingly difficult to protect sensitive data. In the rise of the digital government, the public sector is increasingly espousing Freedom of Information principles while at the same time restricting access to information held by different government bodies (Perrith and Rustad, 2000). One of the greatest promises of new e-government initiatives is to greatly improve public access to government information; however, the Internet has made the protection of personal data a particularly difficult task. Addressing this issue, Holmes (2001) warns that the Internet gives the government the potential to collect and connect much more information about people, posing new risks for personal privacy. He argues that it is necessary to promote a balance between people's right to privacy and the need for public and private-sector access to information on which they can base decisions and provide services. This balance varies from country to country, as each country has its own regulations, values and cultures. Cultural differences regarding this issue may arise when public preference for information disclosure outweighs public preference for the data privacy, or vice versa (Murphy, 2002).

3.1 Freedom of Information concerns

Freedom of Information issues are inherently present in e-government initiatives. For the government, they represent an opportunity to improve transparency and democratic processes by providing information to the public, enabling citizens to register their views on public issues, and allowing the voices of citizens to be heard by each other, by politicians, and by public servants (Heeks, 1999; Pratchett, 1999). For Perritt and Rustad (2000), Freedom of Information can be seen as a tool for the society to control government and thus serving democratic values by giving citizens a feeling of being closer to policy decisions. They argue that accountability and quality of government decisions improve when members of the public have information allowing them to express meaningful views before decisions are made; hence, the legitimacy of public institutions strengthens when the public knows what the institutions are doing. Adding to this, Drake (2003) comments that open access to information provides citizens the opportunity to learn about what government is and is not doing; therefore, government information is vital for business, education, research, health, and well-being of people and democratic governments. She also argues that government information funded by taxpayers belongs to the taxpayers and should be readily available for taxpayers use.

Based upon different authors (Bellamy and Taylor, 1998; Ecclestone, 1998; Heeks, 2000; Perrith and Rustad, 2000; Sood, 2001), it is possible to deduce a number of political, social, and organisational factors that may drive governments to guarantee Freedom of Information rights, as shown in Table 1 below.

Table 1 – Freedom of information drivers

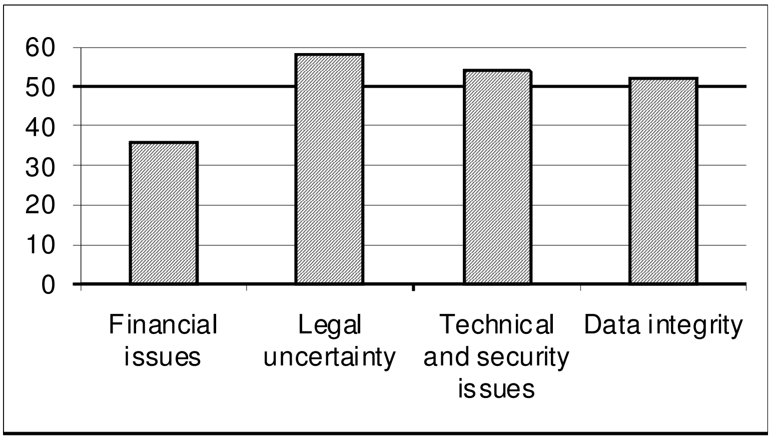
Political	Social	Organisational

Government transparency;
Government legitimacy;
Democracy support;
Responsiveness;
Representativeness.
	Public engagement;
	Public participation;
	Public awareness;
	Public empowerment.
		Effective joined-up services;
		Improved quality of services;
		Better decision-making;
		Better performance.

As a matter of fact, Freedom of Information is not a recent concern of democratic governments. What is new is the existing technological context that has significantly widened the possibilities of information access and sharing. Consequently, governments are seeking to adjust and/or improve their legal framework for supporting information sharing practices under this new scenario, where the means of communications are increasingly expanding to the Internet and mobile technologies. For example, in the United States (US) the Electronic Freedom of Information Act, which was enacted in 1996, establishes disclosure and dissemination obligations extended to electronic formats, compelling government agencies to publish often-requested information in electronic spaces such as the Internet. Similarly in the UK, in April 2000 the House of Commons presented the Freedom of Information Bill to the House of Lords, expanding the British Government's policy on disclosing government information to the public. This fact represents a more open policy towards public access to government records in Britain (Perrith and Rustad, 2000).

Despite governments' efforts to establish legal frameworks for supporting information sharing, in practice things do not seem to be working smoothly. Regarding regulation aspects, a government report (PIU, 2002), published by the Cabinet Office's Performance and Innovation Unit (PIU) in the UK, suggested that the complex nature of regulation prevents the realization of a number of benefits for consumers through better data use. This conclusion was based upon the findings of a survey conducted by central government departments in the UK, which revealed that legal uncertainty was a major barrier hindering better use of data held by public organisations (Figure 1). The PIU (2002) warned that the interaction between legislation and administrative powers has largely been left to individual public bodies to interpret. Hence, there needs to be greater understanding of what the law actually allows.

Figure 1 – Barriers hindering the use of data held by government.
(% identifying specific barriers)



Source: PIU (2002)

From a contextual perspective, two types of information sharing can be identified; these being the sharing of information between departments within the same organisation, and the sharing of information between distinctly separate organisations. In terms of the approach to be taken to the sharing of information, from a legal perspective, there is little difference between the two types of information sharing. Information should be used only for the purpose for which it was collected; this includes sharing information between parts of the same organisation for another unrelated purpose.

Subject to the provisions discussed above, regarding the Data Protection Act 1998 and the Freedom of Information Act 2000, there is no overriding restriction on the sharing of information. Unfortunately, there is also no single law that regulates the sharing of information. Therefore the sharing of information is governed by a number of different legal areas, the interrelationship of which can be quite complex.

However, some general principles with regard to what is legally allowed for information sharing can be put forward. In order to share information, the body that wants to share information with another body has to be certain that it has the power to do so. Does it own or control the information, and has the information be given to it with the right to be shared? Then it has to be determined whether there are any statutory restrictions on the information that it is wished to share. For example, there are specific statutory provisions with regard to information about an individual's medical records. If there are no specific statutory provisions then it is necessary to determine if the sharing of the information would interfere with an individual's rights under the Human Rights Act 1998, particularly the respect to privacy. Also, it needs to be determined whether the sharing of information is in accordance with the principles of the Data Protection Act 1998. Finally, it is necessary to consider whether there is a duty to maintain the confidence of the information under a common law obligation.

Subject to these general principles there is no bar in the sharing of information where there is a recognised need for the information to be shared. Thus, there has to be a definable purpose in the sharing of the information, and a specific set of information that it is necessary to share to meet this purpose.

In addition, where an individual has given explicit consent for their information to be shared; or, the information is not confidential in nature; or, the sharing of information is a requirement of a legal obligation, either under the terms of a statutory provision or a court order; or there is an overriding public interest in disclosure, it is also permitted to share information.

Addressing other problems concerning information sharing, Drake (2003) draws our attention to the problem of suppression of information in the short run, which she claims will likely have unknown, long-run consequences. She argues that our freedom to access unclassified government information is being compromised by ideology and national security, which is one of the many reasons government information is being withheld from public access. This way, a number of government agencies have removed unclassified information that might be considered sensitive from their Web sites. The key problem, she emphasizes, is that it is not clear who decides what information is sensitive or what criteria are used to determine sensitivity.

Concerns regarding suppression of information issues are also addressed by 'The Campaign for Freedom of Information' (CFOI) in the UK. For the CFOI (Ecclestone, 1998), the privatisation of public organisations may lead to significant amounts of information that were previously disclosed being withheld from the public on the grounds of commercial confidentiality. Furthermore, the CFOI claims that government information publicly available on the Internet may be obscure or difficult to obtain. The disparities between government departments depict two extreme opposite situations: on the one hand some departments have lagged far behind the best practices, while others have overloaded their sites with superfluous information.

Other aspects such as the legacy of old mainframe computer systems, professional sensibilities about information sharing, and the political significance attached to operational autonomies are cited by Bellamy and Taylor (1998) as potential factors to inhibit the creation of new forms of information sharing or exchange.

3.2 Data Protection concerns

Besides the difficulties faced by governments to guarantee Freedom of Information rights, there is another underlying challenge for all public sector organisations: securing the integrity of sensitive information. In this respect, governments are addressing issues such as information security, information privacy, preservation of government information, etc. The key problem is how to enable information sharing without threatening privacy aspects. Conversely, another key problem is how to preserve security and privacy without threatening Freedom of Information rights.

Some authors see initiatives towards information sharing as a potential risk to privacy. For Tillman (2003), it remains to be seen how much of government efforts to implement information sharing will impact privacy and whether privacy will be sacrificed in the name of improved access to information. Commenting on the US e-Government law, he points out that one provision of the bill encourages the creation of a single software protocol that would enable different government computer systems to communicate, allowing the compilation of dossiers and databases not previously practical and making sensitive information easier to find. Holmes (2001) argues that people do not care if the information they require are held in different computer systems and by different departments, or even by a private company. But when they talk about privacy, they feel uneasy about the potential misuse of personal information. Analysing the impact of information technologies on the quality of democracy, Kakabadse and Kakabadse (1999) claim that the current democratic context is becoming more and more an electronic tyranny and citizens in Sweden and Germany are fretting about what they see as the impeding age of no privacy.

Indeed, the online activity of Internet users can be stored by businesses with the purpose of defining profiles of personally identifiable data that can be used and sold. According to Regoli (2002), this constant surveillance shifts power over one's identity from the user to the commercial organisation, absorbing individuality and independence, destroying the feeling of freedom brought by anonymity and the ability to be free from unsanctioned intrusion. Regoli also argues that the existing legislation is not well positioned to establish a framework that safeguards Internet users from the commercial amassing of individual dossiers from online information.

The UK Cabinet Office's Performance and Innovation Unit (PIU) affirms that with the rise of e-commerce and e-government, the scope for unauthorised data access and misuse is increasing (PIU, 2002). While technology is enabling better and more innovative uses of data, it also gives rise to new risks. For instance, government institutions around the world are significant targets for hackers breaking into systems from the outside and several hacker groups specialize in targeting government websites. Hence, public bodies need to provide firm assurances that information held in the pubic sector will be secure, and accessed only for specific reasons. For the PIU (2002), information needs to be protected from two potential threats: protection from unauthorised access and protection from data misuse.

4. Considerations on information ownership and access

While information held by government needs to be protected from unauthorised access and misuse, it also needs to be shared with the public so that democratic participation and public empowerment are endorsed by the government. Through this, it is important to realise that information held by government does not necessarily mean that the government is the owner of the information it holds. To better understand this aspect, it is necessary to consider the fundamental concepts concerning 'information possession', which is well addressed by Parker (1995), who comments that:

> "*Possession refers to information being in hand or under the control of the possessor but not necessarily known or available for use by the possessor. A possessor is always a living organism, e.g. a person or an animal, and a computer is not strictly a possessor of information. Only the person or persons in possession of the computer possess the information contained therein. In this case, the possessor could be the owner, service provider, custodian, or user of the computer. A corporate or partnership group of people can possess information; but while a government may possess information, it cannot legally own the information since the owners are the people governed and the information is in the public domain. That is why government-copyrighted information is assigned to the public domain, and the Freedom of Information Act in the United States makes all unclassified and nonsensitive information available to any inquirer.*" (Parker, 1995, p.19).

Parker's main argument is that information possessed might not be known by the possessor; rather, the information may be only held or controlled by the possessor. Thus, information can be possessed but its confidentiality may not be violated if the possessor cannot or does not desire to know it. Taking these considerations into account, it is possible to conclude that there is a clear distinction between information possessor and information owner. One party may possess information while another may own it, i.e. except when legally stated, possession does not necessarily entail ownership. Furthermore, as access to information can be given to those who do not possess the information, we can say that access to information leads to information possession. In spite of this, it is important to bear in mind that possession does not automatically result in ownership. Finally, Parker argues that in a democratic government information is jointly owned by the people – it is public information. Therefore, except for classified or sensitive information, governments should share and allow information access to the public.

Parker's arguments lead us to an important conclusion: the possessor of information is the party who controls access to it, i.e. the possessor of information is the entity that has the power to withhold or share it. While the possessor has the possibility to know the information it holds, there might be situations where the owners do not have access to the information they own. Although information possessed by government is assigned to the public domain, governments only share and disclose information if it is considered as unclassified and nonsensitive. This is the source of potential problems concerning access to government information, since the decision of which information should be considered as unclassified and nonsensitive is a process vulnerable to misjudgments and influenced by peoples' values and beliefs. On the other hand, information that should be really classified as sensitive is supposed to be protected from unauthorised access. This brings further challenges to governments.

Governments around the world have already started to discuss their legal frameworks covering issues ranging from preserving data privacy to encouraging sharing cultures. Some governments require that public bodies prepare, submit and adopt a '*publication scheme*' for the information that these bodies hold (PIU, 2002), while others are establishing e-government laws that require their bodies to conduct '*privacy impact assessment*' whenever they adopt new technology systems in order to verify whether the technology could lead to privacy risk (Tillman, 2003). In our view these initiatives are worthy; however, there are potential problems that might emerge from them. For instance, government managers may reduce the complexity of the problem to a mere elaboration a 'publication scheme', once such a 'scheme' is ready they feel they are complying with the rules and deem to have solved their issues regarding information sharing. Moreover, government bodies might opt for elaborating their 'publication scheme' making minimal adjustments based upon 'best practice' models, this way missing the opportunity to assess their own organisational reality and social context, not being aware that they are only postponing the cultural barriers that are likely to hinder proper information sharing. Regarding 'privacy impact assessment', the 'assessment' of privacy impact is made by people under the influence of their own beliefs and cultural values. In this sense, what is considered as a risk for one person does not necessarily represents a risk for another one. Hence, such assessment might be potentially harm Freedom of Information and/or Data Protection rights.

5. Government information: share or not to share?

The decision of what information can ethically and legally be disclosed and shared with other government bodies, private sector businesses, and the public in general, is a difficult task for government bodies. This sort of decision might be also affected by cultural values, institutional power, and both Freedom of Information and Data Protection interpretations, whose boundaries are difficult to delineate. As an illustration of the problem, we are going to briefly comment on some findings of a research developed in a public sector context in the UK.

The issue of information sharing was one of the aspects analysed in a case study that we have conducted in a Local Authority (LA) in the UK. The case study was conducted with the purpose of verifying the adoption of customer-focused strategies and processes by local government. One of the characteristics of customer-focused practices in the government context is the deployment of diversified channels or means for customer interactions in order to facilitate the communication flow and enhance access to government information. A fundamental premise taken into account was that the cognisance of public opinion is an essential requisite for improving government responsiveness, which entails initiatives such as creating input channels for listening to customers, providing public access to information, sharing information with different government departments or bodies, etc. Taking this aspect into account, we have investigated whether government managers share the same viewpoint on providing access to and sharing information with the public and/or other government bodies.

The case study was conducted in a LA whose main administrative structure consists of a Chief Executive Unit and five other head units or departments. The research methods involved the distribution of self-completed questionnaires to members of staff, semi-structured interviews with senior managers, and systemic observation of the departments' communication processes. We had 79 questionnaires returned from 150 distributed (53% of response rate) and a total of 11 senior officers who had strategic decision-making power were interviewed. The data collected was analysed through quantitative and qualitative methods.

According to our findings, most of the research participants think that the public should be informed about the internal procedures of their respective departments. In other words, the participants think that accessing information about internal government procedures is a public need. Nonetheless, this fact does not necessarily mean that government information is being effectively provided to the public or that the public actually have access to government information. Indeed, further results have shown that there are operational difficulties hindering customers' access to information about their own businesses, situations and personal details. In fact, the LA studied was still integrating its one-stop shops, call centres, and back-office systems in order to improve the flow of electronic communications. Certainly this aspect constituted an operational obstacle hampering access to information.

Although operational difficulties represent many of the problems concerning access to government information, we have conducted further investigation to check whether cultural aspects could also be impacting information sharing. We then turned to investigate whether the respondents share the same viewpoint on issues concerning government information sharing. For this, we obtained and analysed data related to issues such as data usage by government, data ownership, data value and charging, data storage and data sharing. Analysing these aspects in a wider context, Heeks (2000) affirms that different governments may have different viewpoints about public access to information, and some of these viewpoints may create access barriers to the public. For instance, the view that information held by the government should be used for supporting staff activities only may constitute a barrier for public access.

The research outcomes have provided relevant insights for the understanding of the predominant tendency of government manager's mindset regarding information sharing. One important finding was that operational difficulties are not the only barriers to information sharing. Cultural values and beliefs are potential barriers that might also hinder access to government information.

To reach the conclusion above we have conducted a qualitative analysis of the data obtained from the interviews with senior managers. The opinions of the managers were ordered according to the 'conservativeness' they imply when expressing their views on issues related to government information sharing. More specifically, the managers' opinions were ordered from a 'more conservative' to a 'less conservative' point of view. Under the perspective of our analysis, a 'more conservative' viewpoint means that a person is not prone to information sharing, i.e. he or she is more favourable to information withholding. Contrarily, a person who is more favourable to information sharing is considered as having a "less conservative" orientation. The managers' opinions shown in Table 2 below provide an illustration of these aspects. Based upon the opinions, it seems that most of the managers are not very prone to share and disclose information. This sort of attitude might be hindering information sharing initiatives.

Table 2 – Government managers' opinions regarding information sharing

Opinion	Orientation
"Data sharing is not really an issue for us."	More conservative
"We don't share too much information. Some of them with the Education & Personal Development [Department]*."*	More conservative
"We don't hold any data that is particularly sensitive… But we don't tend to share it except to get people to respond to it."	More conservative
"We need to be careful when sharing information."	More conservative
"I think it is very complex to make data available. We should have proper technology for doing that."	More conservative
"It is difficult to share information due to data privacy and IT incompatibility."	More conservative

"We have some difficulty to share information. Some times not because the systems we have, but because the individuals."	More conservative
"If you have the resources and security it could be done. But we need to look at how important it would be."	More conservative
"If we give generic information and non personal information we can do [share] *it."*	Less conservative
"They [the customers] *can apply to access data about themselves."*	Less conservative
"Banks are doing it now, aren't they? If it works for them it could work for us. So why don't?"	Less conservative

Based upon the findings commented thus far, and limiting our generalizations to the scope of the LA studied, we can fairly infer that although government managers agree that the public should be informed about available programs and services, in practice public access to government information remains to be fully implemented. The results suggest that many of the LA's managers have a more conservative viewpoint regarding information sharing, and this fact may be hindering the implementation of systems that improve access to information such as e-government initiatives. The findings also suggest that there are differences between people's attitudes regarding data withhold and disclosure. The lack of consensus concerning this latter aspect might be reflecting existing conflicts of interpretation, understanding, and application of Freedom of Information and Data Protection requirements. It seems that government managers are still having difficulty to classify the information they hold according to two distinct, but not necessarily exclusive, Acts of Parliament: the Freedom of Information Act 2000 and the Data Protection Act 1998. Moreover, government managers are influenced by cultural values and beliefs when interpreting the law, especially in situations where the law is perceived as being ambiguous or not very clear.

In addition to the aspects above, other factors might also impact information sharing in e-government initiatives. Zuboff (1988) comments that systems designed to enhance transparency and knowledge sharing can potentially raise fears among users who prefer a centralised control. Not uncommonly, new technologies might appear to be incongruous and an obstacle to the existing workflow, which requires an extra effort of acceptance. Belamy and Taylor (1998) expand on this issue by affirming that the adoption of new information and communication technologies induce significant changes in the management of organisational processes. A common scenario is that new technologies provoke new forms of inter- and intra-organisational interactions, allowing information to flow across hitherto impenetrable boundaries between functional sectors, departments, tiers of government, external agencies, etc. This kind of information flow may threaten well-established information-handling processes and pose serious challenges to the actors who have the control, which excites defensive behaviours against the emergence of new information-mediated relationships (Belamy and Taylor, 1998). Adding to this latter aspect, Bond and Houston (2003) warn that inter-functional relationships can be inhibited by strong functional identities. They point out that cross-functional problems are likely to emerge when managers from different functional areas struggle to control a new technology.

According to Hoenig (2001), when public organisations refuse to give up their historical identity and power, political barriers will show up. He also claims that personal barriers will slow down processes of standardisation and integration of data and information. By their turn, Metcalfe and Richards (1990) recognise that the central role of information in the management process creates a recurrent dilemma of reconciling conflicting principles of access and security, confidentiality and freedom of information aspects. This dilemma can be formulated in terms of two opposite sets of beliefs and assumptions about the relationship between information and organisation. First, there is a belief that most organisational problems are due to communication failure; therefore, if implementations fail because political intentions were not properly communicated, the recipe for improvement is greater openness, greater clarity and fidelity in information transmission, which leads to joint problem solving and ultimately to consensus regarding what decision to make. Second, there is a belief that information is power; hence, the control of information and secrecy is regarded as a strategic weapon in the political battles over policy and resources, which leads to guarded attitudes towards the disclosure of information. Expanding on the subject, Challis et al (1994) raise further issues regarding organisational information-handling. They question that, if coordination is about information exchange, what actually is being exchanged and by whom? They argue that the flow of information up to official lines of hierarchy is a biased process because all types of managers tend to over-emphasise information that reflect favourably on themselves and to under-emphasise those that reveal their weaknesses.

6. Discussion

The potential problems raised in this article lead us to a key conclusion: attempts to implement e-government initiatives without proper consideration of the legal and cultural aspects concerning access to government information are likely to not produce the expected benefits. When deploying e-government initiatives it is extremely important that governments bear in mind that:

1. The misunderstanding and consequent misapplication of legal aspects concerning public access to government information may frustrate Freedom of Information and/or Data Protection initiatives; and

2. Cultural values and beliefs represent a potential bias towards information disclosure or withholding. Bias towards information disclosure might harm Data Protection rights, while bias towards information withholding might harm Freedom of Information rights.

In the UK, the government Performance and Innovation Unit (PIU) warns that there needs to be more awareness of how the current legal framework operates with respect to public bodies' existing powers to collect, use and share personal data (PIU, 2002). The findings of our study show that there is no consensus on government managers' viewpoints regarding government information withholding and sharing. A slight tendency for data withholding, suggests that it is not easy for government bodies to decide what information can be ethically and legally disclosed or shared with other government bodies, private sector partners, and the public in general. The boundaries of Freedom of Information and Data Protection are difficult to delineate and, on the top of this, cultural values and beliefs are likely to influence biased positions regarding information withholding and sharing.

In other words, the lack of consensus concerning public access to government information might be reflecting existing conflicts of interpretation, understanding, and application of Freedom of Information and Data Protection requirements. Although guidelines and frameworks such as the "publication scheme" and "privacy impact assessment" are very helpful, they are general models that might potentially lead government managers to oversimplify the approach to tackle the problem within their local realities. Issues concerning access to information are delicate and deserve wider and deeper investigation and discussion. Government bodies should see this as a valuable opportunity to assess their own organisational reality and social context. In addition, cultural values, beliefs and peoples attitudes towards information withholding or sharing should not be overlooked or underestimated.

Governments should consider the fulfillment of Freedom of Information and Data Protection requirements as a major concern, as it is related to people's legal rights. In the e-government context, besides the cultural aspects previously commented, technical aspects such as integration of multiple channels of interaction, and integration with legacy systems add further complexity to the problem. In other to address these issues in a holistic manner, government bodies should strongly consider the creation of multidisciplinary groups to analyse and discuss the technical, cultural and legal dimensions involved in e-government initiatives. Multidisciplinary groups comprising managers from different areas of expertise can elaborate the necessary clarifications and solutions required to produce an overall enhancement of e-government programs according to local reality. People's values, beliefs, and knowledge regarding information sharing and withholding aspects should be taken into account and the discussions should be conducted in the light of current Data Protection and Freedom of Information practices, guidelines, and Acts. Some key concerns these multidisciplinary groups could address or act on are:

- Clarification on legislation concerning Freedom of Information and Data Protection rights.
- Clarification and definition of the criteria for classifying information as sensitive or not.
- Implementation of more balanced e-government initiatives in terms of providing the public with as wider access to information as possible without harming data privacy requirements.
- Analysis of existing best practices, guidelines, and legislation concerning the use of technological resources in order to guarantee people's rights to information protection and access.

7. Conclusion

In this article we addressed issues concerning the implementation of Freedom of Information and Data Protection in the government context. Problems concerning Freedom of Information and Data Protection rights were highlighted and the potential influence of cultural aspects on information withholding and sharing was illustrated by the presentation of some findings of a case study conducted in a local government context in the UK.

Regarding the context of e-government initiatives, the issue of data disclosure and withholding is still lacking consensus. Hurriedly and wrongly adopted regulations may lead to distrust and loss of confidence amongst citizens. The prevention of such problems can be achieved by the development of more balanced e-government initiatives that fulfill both Freedom of Information and Data Protection requirements. Multidisciplinary groups comprising government managers with different areas of expertise can potentially contribute to minimize the existing problems by providing clarity to legislation, clear criteria for information classification, and description of technical requirements for information protection and access. The overall enhancement of e-government initiatives can only be achieved if different areas of expertise interact more intensively with each other, in a more synergetic manner rather than fragmented and isolated within different areas, units or departments.

Also, cultural values and beliefs concerning public access to government information should not be overlooked or underestimated. The analysis and discussion of government managers' viewpoints on issues related to information withholding and sharing is of crucial importance for successful e-government initiatives. Open discussions, debates and analyses of these matters in seminars, workshops, forums, etc. create a valuable opportunity for government leaders to learn, understand, and better interpret the existing legal system and practices, or even raise issues to improve future initiatives. Besides, they can also meditate, reassess, review, and adjust their own viewpoints towards more unbiased positions and attitudes.

In conclusion, regarding issues related to public access to government information, the technical aspects should be observed together with a careful and in-depth consideration of the legal and cultural aspects involved in e-government initiatives that go beyond publication schemes and privacy impact assessments. This would allow a better balance between Freedom of Information and Data Protection aspects where more efficient, effective, and ethically correct e-government implementations could be achieved.

8. References

Bellamy, C and Taylor, J (1998), Governing in the Information Age (Buckingham: Open University Press).

Bond, E and Houston, M (2003), ‘Barriers to Matching New Technologies and Market Opportunities in Established Firms’, The Journal of Product Innovation Management, March, Vol. 20, Issue 2, p.120.

Challis, L, Fuller, S, Henwood, M, Klein, R, Plowden, W, Webb, A, Whittingham, P and Wistow, G (1994), ‘Investigating Policy Coordination: issues and hypotheses’. In: Mckevitt, D and Lawton, A (eds.), Public Sector Management – Theory, Critique and Practice (London: Sage Publications).

Dean, J (2000), ‘e-Government Evolves’, Government Executive, November 2000, Vol. 32, Issue 13, p. S-3.

Drake, M (2003), ‘Government Doublethink’, Searcher, May 2003, Volume 11, Issue 5, p. 26.

Ecclestone, A (1998), ‘Freedom of Information & the Internet: an Electronic Window on to Government’, The Campaign for Freedom of Information, <http://www.cfoi.org.uk/cyberwindow.html>, accessed in January 2006.

Harman, C and Brelade, S (2001), ‘Knowledge, e-Government and the Citizen’, Knowledge Management Review, July/August 2001, Vol. 4, Issue 3, p. 18.

Heeks, R (1999), Reinventing Government in the Information Age: International Practice in IT-Enabled Public Sector (London: Routledge).

Heeks, R (2000), ‘Government Data: Understanding the Barriers to Citizens Access and Use’, Information Systems for Public Sector Management Working Paper Series, Paper No. 10, Manchester: Institute for Development Policy and Management.

Hoenig, C (2001), ‘Beyond e-Government’, Government Executive, November 2001, Vol. 33, Issue 14, p. 49.

Holmes, D (2001), eGov: eBusiness Strategies for Government (London: Nicholas Brealey Publishing).

Kakabadse, A and Kakabadse, N (1999), ‘Information Technology’s Impact on the Quality of Democracy’. In: Heeks, R (ed.), Reinventing Government in the Information Age: International Practice in IT-Enabled Public Sector (London: Routledge 1999).

Metcalfe, L and Richards, S (1990), Improving Public Management (London: Sage Publications).

Moulder, E (2001), ‘e-Government… If You Build It, Will They Come?’, Public Management (US), September 2001, Vol. 83, Issue 8, p. 10, 5p.

Murphy, K (2002), ‘Data Protection and Freedom of Information – Is there a Contradiction?’, Seminar from Institute of Management Consultants in Ireland, 5th March 2002, Irish Information Commissioner, Dublin, <http://www.imci.ie/pressreleases.html>, accessed in December 2005.

Parker, D (1995), ‘Possession as an Element of Information Security’, Information Systems Security, Summer 1995, Vol. 4, Issue 2, p. 19.

Perrith, H and Rustad, Z (2000), ‘Freedom of Information Spreads to Europe’, Government Information Quarterly, 2000 Index Issue, Vol. 17, Issue 4, p. 403, 15p.

Pratchett, L (1999), ‘New Technologies and the Modernization of Local Government: an Analysis of Biases and Constraints’, Public Administration, Vol. 77, No. 4, pp. 731-750.

PIU (2002), ‘Privacy and Data-Sharing: The Way Forward for Public Services’. April 2002 Report, London: Cabinet Office, Performance and Innovation Unit, <http://www.number-10.gov.uk/su/privacy/index.htm>, accessed in February 2006.

Regoli, N (2002), ‘Indecent Exposures in an Electronic Regime’, Federal Communications Law Journal, March 2002, Vol. 54, Issue 2, p. 365.

Sood, R (2001), ‘E-Gov Initiatives Aim to Empower Citizens – Savvy solution providers can play a critical role in government’s transition online’, VARbusiness, January 2001, No. 22, p. 91.

Starling, G (2007), Managing the Public Sector, 8th Edition (Belmont: Wadsworth Publishing).

Tillman, B (2003), ‘More Information Could Mean Less Privacy’, Information Management Journal, Prairie Village, Mar/Apr 2003, Vol. 37, Issue 2, p. 20.

Zuboff, S (1988), In the Age of the Smart Machine (New York: Basic Books).