Governance and Information Governance some Ethical considerations within an expanding Information Society

Dr Don White,[1]
Dr John McManus[2] and,
Professor Andrew Atherton[3]

University of Lincoln
Faculty of Business and Law
Brayford Pool
Lincoln
LN6 7TS
England

015222 886165

dwhite@lincoln.ac.uk

[1] Dr Don White University Of Lincoln
[2] Dr John McManus University Of Lincoln
[3] Professor Andrew Atherton University Of Lincoln

Abstract

Governance and information governance ought to be an integral part of any government or organisations information and business strategy. More than ever before information and knowledge can be produced, exchanged, shared and communicated through many different mediums. Whilst sharing information and knowledge provides many benefits it also provides many challenges and risks to governments, global organisations and the individual citizen. Information governance is one element of a governance and compliance programme, but an increasingly important one, because many regulations apply to how information is managed and protected from theft and abuse, much of which resides with external agencies usually outside the control of the individual citizen. This paper explores some of the compliance and quality issues within governance and information governance including those ethical concerns as related to individual citizens and multiple stakeholders engaged directly or indirectly in the governance process.

Key words: Governance, Information, Politics, Ethics, Citizen, Stakeholder

Introduction

In today's information society, information and knowledge can be produced, exchanged, shared and communicated through many different mediums. Whilst sharing information and knowledge provides many benefits it also provides many challenges and risks to the organisation and individual citizen. According to Calder and Watkins (2005) the threats to information systems from criminals and terrorists are increasing and many organisations identify information as an area of their operation that needs to be protected as part of their system of internal control. Research undertaken by Atherton and McManus (2004) point to an information culture which is oversubscribed and less regulated than many believe. Protecting personal information is increasingly becoming a problem for those involved in the creation and protection of information and data (McManus, 2004a). The aim of this paper is to highlight some of the major issues facing managers today who operate within complex governance environments including multiple stakeholders (Freeman, 1984 and Clarkson, 1995) engaged directly or indirectly in the governance process.

Research Methodology

In writing this paper the authors have reviewed the literature in three areas: governance, ethics and stakeholder relations. The authors have also undertaken to draw on their individual research experiences for example, the research undertaken by Atherton and McManus (2004) into attitudes of data protection and governance focuses primarily on the considerations of multiple stakeholders in the use and misuse of company information. The research programme (2003-2004) covered 250 firms in the United Kingdom and employed a variety of research instruments including face-to-face interviews, focus groups, telephone surveys and a questionnaire directed towards key managers with responsibility for the implementation and oversight of the Data Protection Act. The survey questionnaire asked respondents to supply details concerning information privacy and their organisations approach to information risk (take in Table 2).

Information Conflict

As information assumes a more central role in an organisation and becomes an essential component of its power, the decisions that its members make about information – how it is acquired, processed, stored, dissembled and used – play a much greater part in the way an organisation exercises power. In essence the decisions take on greater significance (Mason, 1995). For example, Rindova (1999) argues that information governance directors and other key decision makers possess valuable problem-solving expertise, which they can apply to a variety of contexts. These key decision makers make their cognitive contributions to decision making by performing a set of cognitive tasks: scanning, interpretation and choice. This viewpoint conflicts with the dominant research paradigms on governance which view the contribution of decision makers to strategy making as being limited by their lack of independence or firm-specific knowledge. To the degree that decision makers contribute to strategy, most previous research has viewed their role primarily as dealing with the conflict resulting from divergent preferences of stakeholders. It is argued that these perspectives fail to recognise the contribution that decision makers make to dealing with the complexity and uncertainty associated with information strategy and other strategic decisions.

Botten and McManus (1999) provide evidence to support the perception that many international organisations and corporate institutions have fragmented and defused information strategies in which ownership and control of information governance is weak. Weaknesses in governance practices expose organisations to political, economic, and legal threats. Many of the recent UK acts associated with information protection and democracy address issues of legality (that is what's permissible under the act). Many Government institutions and large multinational firms' state that democracy, and respect for human rights and fundamental freedoms as well as good governance at all levels are interdependent and mutually reinforcing – but not all. Public access to government information should be a cornerstone of our democracy but, to what extent do UK citizens own and control their government's information and what information should be controlled by government and its institutions? It could be argued that historically UK citizens have not had the transparency that other countries afford their citizens for example, USA and Sweden (McManus, 2004a). The USA tends to support a national based policy on information resources tied to a market-based economy – with federal oversight to protect the rights of its citizens. Legislators in the UK and Europe favour a more socially inclusive but optional approach, which raises a number of ethical issues in the direction of information governance and trust.

Governance and Information Governance

A wide variety of definitions of governance and information governance have been proposed in the literature (Bulmer, 1993, Jessop, 1998, Ambit, 2002 & McManus, 2004a) the majority include attributes of security, democracy and ethics which also consume knowledge and trust within the governance framework. Both Ambit and McManus argue in favour of governance from the perspective of information citizenship and stakeholder inclusion that supports an inclusive information society based on solidarity, partnership and cooperation among governments and other stakeholders, (including private sector, civil society and international organizations). Research by Atherton and McManus (2004)[4] demonstrate those organisations which take a progressive view promote governance as part of their information and business strategy. This tends to increase a firms image and profile within their business communities. Atherton and McManus found few firms that opposed citizen or social responsibility within information governance but there are issues. For example, new methods of gathering such information expose individuals to unprecedented levels of surveillance, control, and pre-screening. Several new and emerging technologies, threaten current boundaries of personal privacy. Such technologies include DNA profiling, satellite surveillance and smart image recognition systems. Clearly how to protect information (and data) from misuse is a key factor of information governance. It could be argued that the mark of any information society may be seen in the way we trust government agencies to protect our personal information and privacy. It is not surprising that improving governance structure has been one of the priority areas in the UK. Many of the recent acts[5] associated with information protection and democracy address some of the issues above but not all. For example the proliferation of the internet (e-commerce and cyber trading) raises concerns of trust, associated to reliability and dependability for many citizens.

Governance problems

Within the information systems community, studies of trust to date have focused on isolated topics such as data protection. Our research suggests that an effort to provide a theoretical grounding for trust in information governance is still underdeveloped (Atherton & McManus, 2004). Strengthening trust within the information governance framework, including information security and network

[4] Research based on 250 SME's firms in the UK

[5] These acts apply to all UK-based organisations: Data Protection Act (1998), Human Rights Act (1998), & Freedom of Information Act (2005)

security, authentication, privacy and citizen protection, are all prerequisites for the development of any future information society and for building confidence among governments, organisations, citizens and the wider stakeholder community. A critical question is whether such prerequisites are shared by those engaged in global business activities? Increased business activity for example, e-commerce provides for many challenges. Within information governance, it is important to enhance security and to ensure the protection of data and individual privacy, while enhancing access and trade. Firms engaged in global activities must take into account the level of social and economic development of different countries and respect the governance oriented aspects of their information society. With this in mind it is no accident that today's information systems transcend the physical and liberty enhancing limitations of the past (McManus, 2004a). Many of today's information systems transcend barriers – some of them are walls, some distance, and some shadows some even transcend time. All these in the past have given integrity to the self and the social system; they are now much more permeable. In essence we have become a society of record, such documentation of our past history; current identity, location, physiological and psychological states and behaviour are increasing at risk and open to scrutiny.

Governance and risk

The concept of risk, which encapsulates both uncertainty and vulnerability, features prominently in the literature on governance. Governance and information governance has been defined in terms of acceptance of risk and utility for risk (Jolly, 2003, McManus & Wood-Harper, 2003, and Calder & Watkins, 2005). The presence of risk creates both opportunities and threats and a need for trust (that is a citizens confidence in the information and governance process) especially when dealing with multiple stakeholders. Trust serves to reduce risk and to increase risk taking in a measured way. Several authors have emphasised the importance of uncertainty as a necessary condition of trust within the governance environment (Cadbury, 1992, Turnbull, 1999 & Kochan, 2003). When dealing with multiple stakeholders' uncertainty generally arises from a lack of information or to verify the integrity, competence or actions of another. Paragraph 20 of the Turnbull Report[6] (1999), stated that a company's internal control system encompasses the policies, processes, tasks, behaviours, that taken together facilitate its effective and efficient operation by enabling it to respond to information risk. In short, both

[6] The Turnbull Report has been retitled the Turnbull Guidance

Cadbury and Turnbull Reports made it clear to the directors of public companies that their internal control systems had to address all forms of information (take in Table 1). The main problems with corporate governance in the UK as seen by commentators at the beginning of the 1990s were: short-termism; creative accounting; business failures and scandals; and directors' pay. The Turnbull guidance does not specify what risks should be included within the scope of "information" governance. Given the absence of definitive guidance on what risks to include or exclude those responsible for overseeing governance practice are generally culpable for any omissions or errors in their practices.

Table 1 Cadbury and Turnbull Governance recommendations

Cadbury 1992 Recommendations	Turnbull 1999 Recommendations
• Separate audit and remuneration committees • Audit committee meet with auditors • Disclosure remuneration of director's accounts • Three-year term of office • Non-executives have funds to take external advice	• Accountability for disasters and crises • Risk to company must be disclosed • Directors must have effective system of internal controls • Consultation with board members • Provide the senior management and board with early warning mechanisms; and monitor the system of internal control.

The underlying implication in the governance proposition is that we share enough common values that society can agree on good governance. In practice, however, only dramatic failures provide the basis for change, and this basis is known to be poor. Research by Hawley and White (1996) and McManus (2005) identify a number of issues in relation to ethics, structures, processes and emerging best practice within information governance. For example, within many information technology companies information governance, risk, transparency, and accountability lie not only with the organization but also with multiple stakeholders and governance committees (or boards) that are initiated to manage policy and risk. Some governance structures by their nature and the strategic mission of the organization require a number of stakeholders to come from any number of external groups. When this is the case, it is advisable to select candidates carefully with their risk quotient in mind. It is fine to have cautious or risk taking people on your side, but it is equally important to have a balance. Only in this way can the board produce balanced decisions (McManus, 2005).

Governance and stakeholder participation

Hawley and White (1996), observe a number of significant barriers to multiple stakeholder participation in governance prominent amongst these is that of permissible behaviour and openness. Definitions of permissible behaviour can often depend upon the individual stakeholder or stakeholder group involved in the governance process. Schein (1987) suggests using the concept of vulnerability to help identify which of the stakeholders should be considered before taking a particular action or decision. If different stakeholders are vulnerable to different courses of action, and in such circumstances it is important to know whose interest's one must ultimately protect Henderson (1982), refers to the consistency priority and uses the acronym PWISP – the "*party whose interest is paramount*" as a means of addressing this dilemma. This would support the contention that the governance decision making process, in organisations, is contextually dependent and a reflection of the prevailing distribution of power and political skill - as opposed to being an objective rational process. Davenport (1997), observes attitudes toward information predispose organisations, nations and societies to particular political arrangements. Yet the reverse can also be true, especially in a business organisation. In fact, information governance can be used either to distribute power or to concentrate it.

Governance and Ethics

At a strategic level those involved in the information governance process should give thought to the morally relevant considerations regarding to what purpose information is put (McManus, 2004a). According to Mason (1995), this firstly involves scoping out of the relevant information to obtain an understanding of the information life cycle, and an identification of the key decision-making processes. Second, it requires identifying all the key agents - givers, takers, and orchestraters – and the relevant acts, results and stakeholders. It also includes an understanding of agents and stakeholder's values and motivations of all agents and stakeholders personal, social, moral and ethical history. When we talk about morality and ethics within government, public and private sector organisations we are generally referring to the behaviour and collective outcome of actions taken by the managers and their subordinates (McManus, 2004b). In many organisations collective behaviour is an aggregate, given this situation it is considerably more difficult to pinpoint moral and ethical responsibility within organisations than it is with individual behaviour. When a government, public or private sector organisation operates, as it should, it will accept and respect the moral and ethical challenges presented however, for many these represent a significant challenge. The list of government, corporate and public offences against its citizens even with major legal sanctions are never-ending. The Sarbanes-Oxley Act (SOX-A) of 2002, (Haworth Pietron, 2006) introduced in the United States in the aftermath of Enron[7] has done little to tend the tide of governance scandals. In fact the politics of information governance remain undiscussable in many organisations – yet the negative consequences of information politics have led awry many initiatives intended to improve information use.

Behaviour in governance

Such ethical and governance scandals like Enron are often triggered by financial problems. When financial problems occur, it is tempting to do business with people you might not normally choose to do business with or in ways that you might not normally use. For such companies it is difficult to consider ethical issues when their company is in trouble. Research by Atherton and McManus (2004) into the application of Data Protection within the UK highlights that addressing ethical issues associated with fraud and financial misrepresentation is where most of the current reforms in governance have focused, equally important however, is that an organisation has a culture of fact based dispute management. Without such a culture, the right questions do not get asked, and just importantly, research is not being undertaken to test uncertainties within the business and governance environment.

Governance, Data Protection and Security

A recent survey[8] by Barrett (2006), points to an information culture where legal barriers to information access and usage can work against the interests of both the individual and community. For example, the study undertaken by Barrett indicates that the British public support for medical research is being hampered by rules on data protection. In principal UK citizens support the use of personal medical data for public health research but the governance aspects within the Data Protection Act (DPA) makes use of such information difficult. This tends to dispel the belief that individual citizens are always concerned about their right to privacy than

[7] Often referred to as the first major failure of the "New Economy," the collapse of Enron Corporation stunned investors, accountants, and boardrooms and sent shockwaves across financial markets when the company filed for bankruptcy on December 2, 2001.

[8] Geraldine Barrett, Brunel University asked 2,872 people about the acceptability of their personal information being used by the National Cancer Registry

public health. The results of the Barrett survey show that absolute privacy is not a priority of ordinary citizens. The vast majority of people are happy for information about them to be used for the wider public good, provided the information is kept confidential and secure.

Identifying information security goals that meet DPA, organisation and governance requirements is one challenge which brings organisations and citizens into conflict. British Standard 7799[9] stipulates that management should actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities. Research for the Information Commissioners office by Atherton and McManus (2004) examined data protection and information handling and security issues in 250 businesses. The study focused on understanding current practice in data handling and security. The survey involved telephone and face-to-face interviews with 250 businesses in 9 English regions and in Scotland. Of those questioned 80 per cent said that the DPA was relevant to their business, 20 per cent were not that sure. Respondents felt that key terms such as confidentiality, security and privacy were critical in managing data security and risk. Terms such as confidentiality and security were defined in terms of how they assist the business in improving its profile (usually from an ethical perspective in how it operates and treats confidential information, take in Table 2).

Of the 250 organisations interviewed, 225 (90.5 %) believed that security of data and information was important to their business operations. From the results of the survey there appears to be a strong bias to protecting data and this is reinforced through the qualitative statements of respondents. Irrespective of type of business there is a strong awareness amongst organisations of personal information, although respondents' definitions did vary. Key issues around security were focused on accidental loss, abuse, disclosure and ethical use of personal information. Even with good governance and data security some of the respondents acknowledged that data does go missing and abuse is some times difficult to police: "…Databases can be misused if they fall into the wrong hands – people can appropriate information from their companies and use it illegally."

[9] Also noted as ISO/IEC 17799 Data Security Standard

Table 2 ICO 2004 Survey terms ranked as most significant

Key Word	Most Significant	%
Confidentiality	27	38.6%
Data/Information Security	21	30.0%
Information Handling	6	8.6%
Privacy	5	7.1%
Information Risk	5	7.1%
Data Protection	4	5.7%
Data Sensitivity	2	2.9%

Social forces in governance

Two important social forces serve to keep organisations ethical they are the law and the market (self regulation). Both are to some degree inadequate for example, many large organisations and corporate institutions do not welcome regulation and use their power bases to apply pressure to the offending body and to receive amends to legislation. Laws have loopholes, and lawyers are likely to find them. The costs of enforcement can be substantial in addition; laws sometimes conflict with each other and thereby prove counterproductive. Such limitations suggest that ethical behaviour must originate within the institution or organisation itself, and as such must become embedded within its governance framework (culture, policies and practices). In many ways SOX-A attempts to force internal and ethical control by ensuring requirements are achieved through integrating three main functional areas, these are financial reporting, information security and business process control.

Conclusion

Information governance should be about setting the rules and regulations that ensure all information within an organisation is being used ethically and is in compliance with the legal framework that is law. To some degree information professionals are sceptical, at best, of the organisations ability to embrace information governance and in the main see government legislation as a way to bring organisations under control, by committing them to policy mechanism and standards of operation, which take value from their bottom line. Whilst there is some truth in this statement the reciprocal also applies in that without governance there would be wide spread exploitation. With respect to ethics it’s a question of balance, information access and control have become particularly important in debates amongst information professionals and researchers.

References

Ambite, J. L. et al. (2002), Data integration and access: In William J. McIver & Ahmed K. Elmagarmid. Advances in digital government technology: human factors, and policy. Boston, MA: Kluwer Academic Publishers.

Atherton, A. & McManus, J, (2004), Encouraging SME's to adopt the values Data Protection Act: Report for the Information Commissioners Office, ERDU, University of Lincoln, UK

Barrett, G., (2006) Research hindered by data law, online British Medical Journal, April

Botten, N. & McManus, J., (1999), Competitive Strategies for Service Organisations, (Chapter 6), Macmillan Press, UK

Bulmer, S., (1993),The governance of the European Union: A new institutionalist approach. Journal of Public Policy 13 (4), pp 351-380.

Cadbury, A., (1992), Committee on the Financial Aspects of Corporate Governance London: GEE.

Calder, A., & Watkins, S., (2005), IT Governance, 3rd edition, Kogan Page, London

Clarkson, M.B.E. (1995), A stakeholder framework for analyzing and evaluating corporate social performance. Academy of Management Review, 20: 92-117.

Davenport, T., (1997), Information Ecology, p 68, Oxford University Press, New York

Freeman, R.E. (1984), Strategic management: A stakeholder approach. Boston,

Haworth, D.A., & Pietron, L.R., (2006), Sarbanes-Oxley Achieving Compliance by starting with ISO 17799, IMS, Winter, pp 73-87

Hawley, D., and White, D., (1996), 'Modelling the ethical environment: a systems analyst and designer perspective', p 82, in Smith, K., and Johnson, P., Business Ethics and Business Behaviour, International Thomson Publishing Company, London, UK

Henderson, N.L., (1982), The Ethical Side of Enterprise, Sloan Management Review, 23, pp 37-47

Jessop, B., (1998),The rise of governance and the risks of failure: The case of economic development. International Social Science Journal pp 155, 29-45

Jolly, A., (2003), Managing Business Risk: A practical guide to protecting your business, Kogan Page

Kochan, T. 2003. Restoring trust in American corporations: Addressing the root cause, Journal of Management and Governance 7, pp 223-231

Mason, R. (1995), Ethics of Information Management, Sage Publication, page 198.

McManus, J., (2005), Managing Stakeholders in Software Development Projects, Elsevier, Butterworth-Heinemann, UK

McManus, J., (2004a), Information Governance an Ethical Perspective, Journal Management Services, December, pp1617

McManus, J., (2004b), Working towards an Information Governance Strategy, Journal Management Services, August, pp 8-13

McManus, J. & Wood-Harper, T., (2003), Information Systems Project Management: Methods, Tools and Techniques, (Chapter 5), Pearson Education (Prentice Hall), UK

Rindova, V., (1999), What corporate boards have to do with strategy: a cognitive Perspective, Journal of management studies, 36, pp953- 976

Schein, E.H., (1987) The Clinical Perspective in Fieldwork, Sage Publications

Turnbull, N., (1999), Internal Control: Guidance for Directors, Report ICAE&W, London