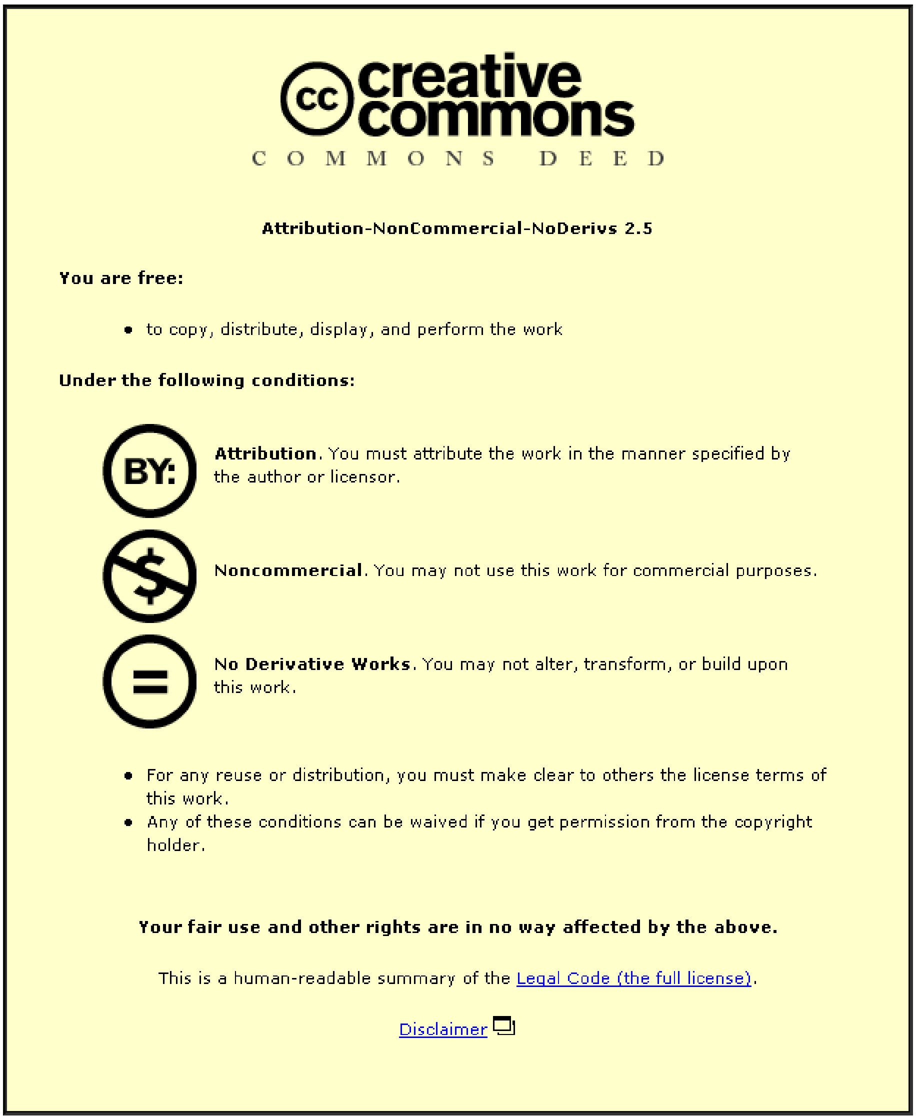

Data sharing and personal privacy in contemporary public services: the social dynamics of ethical decision making

Christine Bellamy (Nottingham Trent University), Perri 6 (Nottingham Trent University), Charles Raab (University of Edinburgh) Adam Warren (Lougborough University) and Cate Heeney (University of Edinburgh)

Paper presented to Working Group 6
Annual Conference of the European Group of Public Administration, September 1st - 4th 2005,
Berne, Switzerland.

Corresponding author:

Christine Bellamy,
Professor of Public Administration,
Graduate School, College of Business, Law and Social Sciences,
Nottingham Trent University,
Nottingham NG1 4BU,
UK

Email: Chris.Bellamy@ntu.ac.uk
Telephone: +44 115 848 5551/5537

Abstract

Amongst some of the most important and interesting ethical dilemmas facing street level bureaucrats in contemporary public services are those arising from conflicting imperatives in the use of personal data. On the one hand, public services are coming under pressure to retain and share more data about identifiable individuals, in order better to deal with their problems or to protect communities against the risks they pose. This pressure appears to conflict – at least to some degree - with confidentiality norms embedded in the codes of practice of public service professions as well as with privacy laws stemming from the European Data Protection Directive and the European Convention of Human Rights.

Furthermore, the ethical dilemmas associated with these conflicting imperatives may be growing more acute, as a result of changes in the political and social environment in which public servants work. Firstly, there is a widespread perception that information and communication technologies can support the extensive networking of public service data systems: this perception is giving rise to pressures to achieve service improvements and cost savings associated with the pooling, re-use and exchange of personal data. Secondly, there is a growing view that many of problems experienced by individuals, families and very small neighbourhoods can best be addressed by multi-agency interventions: this view implies that agencies will share data about these individuals, families and neighbourhoods to a greater degree than hitherto. Thirdly, growing pressures on public services associated the influence of communitarian ideas about the management of risks may be leading to tendencies to favour the public good over individual rights, especially in such fields as policing, child protection, mental health and public health. If so, we would expect these pressures to lower thresholds for sharing personal data between agencies.

This paper presents some provisional findings from a major research project funded by the UK's Economic and Social Research Council. The project has collected qualitative data from over 200 interviews with street level professional workers, managers and information systems managers in 12 cases of local multi-agency arrangements (MAAs) in England and Scotland. The data presented in the present paper is from the 8 English cases, comprising 138 interviews. These cases were chosen from four policy fields, namely:

- *health and social care for the elderly*
- *health and social care for the mentally ill*
- *public protection arrangements managing risks associated with violent criminals and sex offenders; and,*
- *crime and disorder reduction partnerships, which include organisations concerned with planning interventions against prolific offenders, domestic violence and drug-related crime.*

These fields have been chosen, for two main reasons. First, in all of these fields, decisions about what data to share, when to share them, who to share them with and how to interpret them and use them involve serious risks: the decisions made by individual workers may result in the abuse or death of a child, the loss of parole for a prisoner, the stigmatisation of a family or the refusal of employment for a job applicant. Decision-making in these fields therefore poses ethical problems with potentially serious outcomes for individual clients. Second, in the UK, all these fields are currently subject to central government initiatives designed to encourage greater sharing of personal data to support more effective multi-agency working. They are all fields, then, in which tensions with privacy are coming to the fore.

The data collected for this project will eventually provide the most comprehensive, detailed evidence yet available about the ways in which street level professional workers cope on a day to day basis with the tensions between imperatives to share data about needy and risky people, and imperatives to respect their confidentiality and personal privacy. The data will also provide evidence about the ways in which the coping strategies of such workers may be changing under the influence of changes in the political environment outlined above. A particular facet of the analysis will be concerned with the intended and unintended behavioural consequences of the growing use of data sharing protocols and other ethical instruments. These instruments are designed to govern the practices of street level professionals, and in so doing to protect the privacy of clients, patients, offenders, victims, witnesses and other individuals who come into contact with public services in these fields.

The overarching hypothesis framing this research is that individual decision-making will be shaped by the organisational, cultural dynamics in which it takes place. We are using neo-Durkheimian institutional theory as the analytical framework for a series of systematic comparisons: between MAAs in the four *different policy fields: between types of organisation (for example, police, health and social work agencies), between organisations that comprise these MAAs and between actors from different professions. These comparisons will enable us to assess the nature and influence of organisational dynamics in these fields, and to understand the ways that different mixes of institutional forms impinge on data sharing practices in different organisations and among different kinds of professional workers. We will also compare the ways in which risks to privacy are perceived and managed, and the ways organisational dynamics shape coping mechanisms adopted by individuals to manage the fear of blame.*

In turn, this analysis will help us understand the social influences on complex decision making by street level workers in policy fields that that are riven with important ethical issues.

Introduction

In previous papers (6 et al, 2002; 6 et al, 2005a; Bellamy et al, 2005a; Bellamy et al, 2005c), we have discussed the reasons for the increasing emphasis in British public services on 'holistic' or 'joined-up government' (JUG). We have argued that, as understood by the Labour Government that came to power in the UK in 1997, JUG differs significantly from previous attempts to increase co-ordination across government, because of its emphasis on multi-agency interventions at the *micro-level* of public services. The present Government's approach also advocates the targeting of resources in areas of greatest need and risk (Kemshall, 2002). Thus, a core aim of JUG is to increase capacity for multi-agency interventions in the lives of those individuals, families or very small neighbourhoods who are in particular need, or who thought to be at risk of coming to greatest harm, or who present the highest risks of harming other people. The three imperatives of JUG for social policy are, therefore:

- to increase efficiency in the use of scarce public resources by concentrating interventions on those individuals, families or neighbourhoods who are most in need or at risk;
- to increase the effectiveness of public services in dealing with them, by increasing capacity for co-ordinated, multi-agency action;
- to develop better information resources – including information systems for sharing data, and analytical tools - for identifying individuals, groups, areas at greatest risk, for assessing their needs, and for assessing the impact of multi-agency interventions in their lives.

As the last bullet point highlights, one important implication of JUG in the social policy field, is that street-level agencies are coming under increased pressure to share data about the people they deal with in the course of their work, whether they be pupils, clients, patients or offenders. Caseworkers also come under pressure to share data about third parties, including the families and associates of their clients, or the victims or witnesses of their behaviour. In particular, imperatives to share personal data more freely are coming from three sources. First, the present Labour Government that came to power in 1997 has launched initiatives in a wide range of policy fields, to mandate inter-agency collaboration by means of increased data sharing. Prominent examples are to be found in the policy fields we discuss later in this paper. Second, the Government investing large sums of money in national, strategic IT systems to support the sharing of data between local organisations involved in multi agency arrangements. At the time of conducting the research reported in this paper, only one of these systems, ViSOR, the national Violent and Sex Offenders Register, was actually in use. But over the next few years, the Government intends to introduce several big new systems, including: electronic patient records under NHS Programme for IT (NPfIT, now called *Connecting for Health)*; a database for holding basic details of all children in England and Wales to promote data sharing between statutory services such as health and education; databases of children and other vulnerable people who are considered to be at particular risk in the fields of health and child protection, and a new national police intelligence system (the IMPACT project) to promote the sharing of 'soft' intelligence data between local police forces. A more detailed list of planned new systems is given in Bellamy et al (2005b).

Thirdly, imperatives to share personal data are being reinforced by a stronger climate of blame when agencies fail to share personal data (Raab et al, 2005). In recent years in the UK, there has been a series of tragic events which, inquiries subsequently showed, could have been prevented if agencies had shared more data with each other about risky or vulnerable people that were known to them. Among these cases are those of the schizophrenic, Christopher Clunis who murdered a passing stranger while being treated in the community rather than in a hospital; a number of cases of children, notably Victoria Climbié (Laming, 2003), who were murdered by their parents or guardians, despite being known to social care agencies; and, most recently, the murder in 2002 of two ten year old schoolgirls in the Cambridgeshire village of Soham by a school caretaker, Ian Huntley, who was known to a police force in another part of England – the county of Humberside - as a probable serial sex offender. The Soham case led to a six month public inquiry chaired by Sir Michael Bichard who reported in 2004. The Bichard Report heaped considerable opprobrium upon senior police officers and social services chiefs for chronic failures in their information management processes, and it named junior officers, too (Bichard, 2004).

Ethical dilemmas associated with data sharing and privacy

The problem for street level workers and their managers is that pressures on their data management arrangements are not coming from a single direction, and that they are therefore being forced to make choices between competing and, we would argue, qualitatively different values in their data sharing and data protection practices.

The duty of confidentiality is well established in English common law, and is strongly reinforced in the training of professional workers such as medical doctors, nurses, social workers and probation officers. There are good operational, as well as sound ethical, reasons for its existence. One danger is that, especially in a climate of over-zealous data sharing, front line workers seek to avoid blame by passing on large amounts of data without sufficient concern for their quality, with the result that they overload colleagues with indigestible quantities of information or promote over-hasty interventions based on a misreading of the case (Reder *et al.*, 1993: 90). Defensive practice can extend to clients, too. If individuals suspect that their confidences will not be safeguarded, they may refuse to disclose information, or they may misrepresent essential facts about themselves, their relationships, their behaviour and their circumstances when professionals compile case records. Trust in professionals may be eroded, damaging the effective functioning of public services. Discourse within the caring professions therefore recognises the erosion of privacy as itself a source of risk.

The duty of confidentiality has, moreover, been strengthened in several important ways since the Labour Government came to power in 1997. Partly to encourage medics and patients to trust new IT systems, the British National Health Service (NHS) has put new, more rigorous arrangements in place to safeguard patient confidentiality, and these arrangements are being extended to the social care sector, too. The British Parliament has passed a new Data Protection Act (1998) to transpose the European Data Protection Directive (1995) into British Law, and in 2000 a new Human Rights Act (1998), based on the European Convention of Human Rights, came into force. These measures strengthened the British subject's legal right to privacy, including the privacy of their data. One consequence of these changes is that the ethical dilemmas created for the management of personal data in British public services have become much more salient in political circles (Performance and Innovation Unit, 2002; Department for Constitutional Affairs, 2003), and interviews conducted for our present study show that the issue is now firmly lodged in the minds of many senior policy makers in British central government. While they deliberate, however, street level workers in British public services are obliged to try to find ethically defensible passages between the Scylla of data sharing and the Charybdis of confidentiality in their day to day work.

This metaphor is apt, because agencies are trying to steer between what are, at bottom, irresolvable tensions. One source of difficulty is that data protection legislation, along with much of the guidance issued by various authorities, is couched in terms of high level principles. While these principles are probably not hard to decipher in abstract terms, there is nevertheless a considerable gap between the articulation of such principles and their operationalization in day to day, street-level routines. This problem is compounded by the huge cognitive gap between the proximal actions and distal consequences: between the short comings of day to day administrative routines and the potentially dire consequences that may sometimes follow from them a long way down the road. It takes no great leap of imagination, for example, to understand why neither the police chief in Humberside nor the relatively junior civilian workers who input intelligence data into his IT systems, were able to foresee the catastrophic outcomes that laxity in the filling up of forms and in the recording of data would have for the two Soham schoolgirls.

Even when workers are alert to the ethical components of day to day administrative or professional tasks, by definition, decisions about whether to share personal case data with other agencies, must be taken in the absence of all the information that is potentially available about that case. For example, a teacher might notice a man hanging round the school gates and wonder if he should inform the local police. A policewoman faced with an allegation about a potential sex offender might wonder if she should file the incident for recording on the police force's local computer. Her superiors might wonder how long the record should be retained. If the man in question has never been charged with, or convicted of, a criminal offence, there would be no hard data on the National Police Computer to inform such a decision. Should the force nevertheless request other local forces to search their files for softer, 'intelligence' data about him? Should these forces keep a record of this request, in case other allegations or checks are subsequently made about the same man? And how should any of these forces respond if they were subsequently asked for a police check about him because he applies for a job, or to join a sports club, where he would come into contact with children?

These examples illustrate an unavoidable dilemma faced by decision-making in this field, namely that it is *inherently* prone to error judgments about the degree of risk presented by a case, and that these errors are inevitably compounded by the lack of information at the point where the decision has to be made. This being so, agencies are, in effect, forced to choose between the risks associated with two kinds of decision errors. *False negative* errors (under-reacting) take place when persons are deemed not to be a danger, or to be in danger, when it subsequently transpires that they were. *False positive* judgment errors (over-reacting' take place when the converse occurs. In many areas of social policy, the risks attaching to *both* kinds of decision errors are both palpable and serious. As recent child protection scandals in the UK and elsewhere have demonstrated, a decision not to share data may lead to physical harm to, or even the murder of, a child. On the other hand, a decision to share on the basis of inadequate or inaccurate information may lead to child wrongly being taken into care, with devastating effects upon the child or its family. Or, as in the example above, a man may, perhaps wrongly, be refused a job, with equally devastating effects on his career. In either case, the problem for agencies is compounded by the knowledge that a perceived miscarriage of justice may generate a heated public reaction, with the consequence that blame is heaped on public service workers for making the wrong call.

Faced with these problems, many public service agencies now pay considerable attention to formulating detailed guidance and agreeing multi-agency protocols to control the use and sharing of personal data in case files. A major reason for investing in new IT systems is that they appear to offer the means of embedding controlled data sharing more routinely into everyday organisational life. However, as a growing body of research makes clear (Lewis, 1993; Plant, 1994; Fisher, 2001; Pater and Gils, 2003) - and as our own empirical evidence (discussed below) shows too - guidelines, protocols and codes of all kinds are as much honoured in the breach as in the observance. Furthermore, even if agencies try to enforce *detailed* rules of procedure, protocols and codes they cannot *resolve* the fundamental dilemma we discussed above: that there is an inescapable choice, in conditions of imperfect information, between the risk of false negative and the risk of false positive judgment errors. Indeed, codes simply introduce systematic biases towards one or other type of error. Ultimately, then, social policy agencies are obliged to choose between different kinds of risk. Some choices may be systematically embedded in policies, protocols and IT systems: others are made through the ad hoc, case decisions of individual, frontline workers. And in choosing between different kinds of risk, agencies are sometimes forced to choose between different values, which could only be validated by appeals to rival ethical systems.

In making this point, we are running counter to much of the official literature issued by central government in this field which speaks optimistically of striking a 'balance' between data sharing and privacy. In other words, there is an implicit assumption that these two imperatives can be brought into a relationship with each other, such that both can be sufficiently accommodated and neither is unacceptably damaged. We have argued elsewhere that, as articulated in current British government policy, the twin aims of privacy and integration cannot always be successfully accommodated (6 et al, 2005a; Bellamy et al, 2005a): indeed, they may often be much better understood as a constituting a dilemma than a trade-off. One reason is that protagonists often argue from rival value systems. The language of data protection and human rights is generally couched in individualist terms that place high value on human rights, especially the right to privacy. The presumption is that the privacy of data subjects should always be respected, unless they have given informed consent for their data to be shared, or unless there are clear and proportionate reasons for sharing without consent. In practice, data protection regulators and privacy experts interpret the notion of 'proportionality' to imply that the risk must be proximal and specific: that is, the presumption of privacy and confidentiality can only be overruled if there is a real and present risk of determinate harm. The empirical evidence gathered for the project described below suggests that frontline workers do indeed find it relatively easy to 'balance' risk in such cases: those where the risk to an individual's privacy is countered by a tangible and proximal risk to the same individual or, indeed, to other known individuals. For example, it is possible to argue from the same individualist value frame about whether social care agency should inform the public utility companies that a vulnerable and demented elderly person is in financial difficulties, in order to avoid the risks associated with the withdrawal of the power supply to that person's house. Likewise, it is possible to use such a frame to decide whether a Public Protection Panel should inform a prospective landlord about a named sex offender who is about to be offered a tenancy in a house close to the residence of a child he once groomed.

Less tractable tensions arise, however, in relation to risks arise that are by no means fanciful,, but which are unspecific, collectivised and distal. This is particularly the case in fields such as mental health, crime prevention, child protection and fraud control. In these fields, public agencies are claiming wide powers to retain and, sometimes, to share personal data, on the grounds that individuals known to them represent a danger of, as yet, unknown severity, (but which could well prove severe) to unspecified members of the public an indeterminate future. In such cases, there is often much less consensus about how to weigh the merits of rival claims, because the human rights of known individuals (usually the risky person, but sometimes their victims or associates, too) are being thrown into competition with the perceived long term interests of an impersonal public. Furthermore, this approach is being validated by reference to a crude but powerful Utilitarian ethics that, at bottom, values 'the greatest good' over individual rights, outcome over process, ends over means. Conflicts around these kinds of issues have emerged most explicitly in the UK in the aftermath of the Bichard Report on the Soham murders. This Report has, for example, encouraged the National Association of Chief Police Officers to adopt a more aggressive policy on retaining and sharing 'soft' data, on the grounds that scraps of information about a suspected person might eventually add up to a pattern indicating severe public risk. This policy has been challenged by the British Information Commissioner on grounds of disproportionate threat to individual privacy, and the matter has ended up in the High Court. And our research evidence shows, too, that some of our respondents, especially those in law enforcement agencies, are in no doubt that many decisions they are forced to take involve a straight choice between proximal, specific risks to individual privacy and distal, generalised risks to the public.

Data sharing and privacy in multi-agency working: a theoretical framework

It follows from this discussion that we should not underestimate the difficulties facing frontline services in managing the tensions apparent in this field, or the challenges these difficulties present to effective inter-agency working. We therefore need much more knowledge about the ways in which workers involved in multi-agency working experience and manage these tensions in their day to day work, especially in agencies dealing with particularly needy, risky or vulnerable people. This paper presents some early and provisional findings from the authors' current research project[1]. The theoretical framing of this project is set out in 6 et al (2004). It is based on neo-Durkheimian institutional theory, from which we developed a set of hypotheses about the impact of institutional forms on styles of data sharing and privacy protection in multi-agency working in England and Scotland.. Developed from the work of anthropological theorist, Mary Douglas and resting on Durkheim's characterisation of the elementary forms of social organisation, this theory emphasises the significance of two key dimensions of organisation – the degrees of social regulation and of social integration. Cross-tabulating these two dimensions yields four distinct institutional forms, which can be discerned in social life at every scale and in every human society (Douglas, 1982a [1978]; 1982b, 1992, 1996; Mars, 1982; Thompson *et al*, 1999; Rayner, 1992). These forms are:

- hierarchy (strong regulation and integration);
- individualism (weak regulation and integration);
- enclave (weak regulation, strong integration); and
- isolate (strong regulation, weak integration)

The overarching hypothesis for the current project is that distinct styles of personal data sharing and of absence of sharing (refusal to share, failure to share, inability to share, and so on) will emerge in each of these forms. Because many organisations exhibit hybrid institutional characteristics, the styles by which they share or do not share data are expected similarly to represent combinations of two, three or even all four of the sets of features associated with the elementary forms.

Figure 1 summarises the basic argument framing the project. In each cell, there first appears a characterization of the values taken by the institutional variables (the independent variables in our project), followed by a summary of the values expected in the 'style of data sharing' (the dependent variables in our project). Throughout the analysis conducted for the project, the term 'style of data sharing' is used to capture the specific pattern of sharing or not sharing in the social entity in question, including the means, extent and ease to which it occurs, or not.

[1] [1] *Joined up government; data sharing and privacy in multi agency working. ESRC* Award no RES/000/23/0158, 2003-5. Project team: Professor Chris Bellamy (Nottingham Trent University), Professor Perri 6 (Nottingham Trent University), Professor Charles Raab (University of Edinburgh), Dr Adam Warren (Loughborough University) and Dr Cate Heeney (University of Edinburgh).

Figure 1: Institutional forms and expected styles of information sharing or absence of it

Negative diagonal (isolate-enclave) Information sharing or lack of it defensively driven by avoidance of risk	*Weak social integration ←*	*→ Strong social integration*
Strong social regulation ↑	**Isolate**: coordination by individual coping with constrained circumstance and brute luck; Heavily constrained individuals acting opportunistically, unable to sustain trust **Information sharing** Embraced as opportunistic coping Rejection as inconvenient or bothersome	**Hierarchy**: coordination by rule, role and given fact; Centrally ordered community **Information sharing** Undertaken as regulated practice Rejection justified by lack of formal governance for it or because of opposing rules
Weak social regulation ↓	**Individualism**: coordination by voluntary agreement; instrumental, entrepreneurial individuals **Information sharing** Commitment to it as managerial strategy Rejection as inconvenience or threat to managerial or professional control of resource	**Enclave**: coordination by shared mutual commitment within bounded group; internally egalitarian, but sharply marked boundaries with others; held together by shared commitment to moral principle **Information sharing** Embraced as crusade for saving lives Embedded in clientelism Rejection as in principle wrong
Positive diagonal (hierarchy-individualism) Information sharing or lack of it positively driven by commitment or pursuit of opportunity		

Proximate source; 6 *et al*, 2004 : 11 and 15
Ultimate sources: Douglas, 1982a [1978], 1982b, 1992, 1996; Durkheim, 1951 [1897]

In broad terms, the theory proposes that there will be consistency between the general institutional character of the organization – including for this purpose, inter-organisational arrangements - and the specific ways in which local agencies attempt to achieve some kind of settlement between the potentially competing imperatives of information sharing and privacy.

How, then, does the theoretical framing of the project help us to understand the ethical dimension of settlements between these imperatives? In a recent article (2004) Maesschalck proposes that ethical dilemmas arise in public service organizations when their members find themselves in situations where they find it difficult to judge with accuracy what would constitute ethical behaviour. It is our contention, on the basis of the discussion presented above, that this situation holds in relation to tensions between data sharing and integration in multi agency working in the UK. Maesschalck further proposes that neo-Durkheimian institutional theory would predict that what shapes outcomes in such situations is the particular mix of instiutional forms characterizing the social entity in which such tensions arise (Maesschalck, 2004). Moreover, organizations characterized by the strong dominance of a particular institutional form are likely to over-emphasise the values on which their social solidarity is based to the exclusion of other values. The result is that their ability to manage and moderate the behaviours typically associated with those forms is actually reduced. Maesschalck argues, therefore, that strong institutional forms are likely to encourage unethical behaviour defined as 'a too radical (and therefore misunderstood)' application of dominant ethical standards (Maesschalck, 2004: 474). Paradoxically, then, the excessive assertion of particular kinds of regulation or integration can undermine the possibility of an acceptable and stable settlement between competing ethical imperatives. And, relating this theory to our own work, we would expect that those organizations displaying a mix of institutional forms are most likely to achieve the most sustainable and comfortable settlement between data sharing and privacy.

The case studies

To explore the power of this theory, we conducted a programme of qualitative research using semi-structured interviews. In line with the clear theoretical framing of the project, we developed a stronger theory-driven structure for the interview schedule and a more elaborate, pre-defined coding structure than is common in many studies that use such methods.

Between November 2003 and January 2005, we conducted 209 individual interviews, using three different interview schedules, with managers, frontline professional staff and information systems managers in twelve multi-agency arrangements (MAAs) in England and Scotland. The MAAs were drawn from the fields of (i) health and social care for older people, (ii) health and social care for people with mental health problems, (iii) crime and disorder reduction, and (iv) public protection from violent and sex offenders. Eight cases were in England and four were in Scotland. The sample includes MAAs in urban, rural and mixed localities. It was carefully selected, too, to contain MAAs that were identified by desk research and a preliminary set of interviews with senior policy makers, to reflect various levels of experience and success in multi agency working. In this paper, we present findings from the eight local English case studies, which comprise about 55 organisations. The data is taken from 138 interviews, each lasting about an hour..

Figure 2 below presents some basic information about each MAA in our sample. The sample is divided equally between the different fields listed above: two from each field. Within health and social care, MAAs were composed of local implementation teams for the National Service Frameworks for care for older people and for mental health care. In all these fields, multi-agency working between various health agencies and various social care agencies is specifically mandated by central government, either in legislation or else by formal policy guidance, and embraces agencies in both the statutory and voluntary sectors. Data sharing is explicitly permitted by legislation that supplements data protection law, and by a range of formal policy instruments, rules and protocols. As we have seen, it is also being embedded in new IT systems. By these means, agencies are required to make joint assessments and to provide integrated care to their clients. This involves the sharing of client information on a 'need to know' basis between medical and social work professionals who are trained in different ways and subject to different professional codes. In both cases, a rich body of related information about relatives, neighbours and, in some rare mental health cases, third parties who may be affected by the case, needs to be handled with great care.

Multi-Agency Public Protection Arrangements (MAPPAs) promote inter-agency cooperation to identify and manage risks presented by violent and sexual offenders living in the community (e.g. on parole or after release from prison). They typically source data about risky people and their victims from the police, probation service and prisons. Data is also sourced from, and shared with, health authorities, housing authorities and social care agencies. Crime and Disorder Reduction Partnerships (CDRPs) are local collaborative partnerships set up to analyse local crime statistics, plan crime reduction programmes and work with those at risk of offending or victimisation. CDRPs source data from a range of agencies, including police and probation services, courts, health authorities, social care agencies and education authorities. Much of these data are aggregated or otherwise anonymised, but some of them relate to very small neighbourhoods, or very small groups of offenders or victims. So true anonymisation is not always possible.

These fields were therefore selected for our sample because the work of agencies in them involves inescapable ethical dilemmas to do with:

- handling very sensitive information;
- making decisions about whether, when, why and exactly what to share about an individual with other agencies;
- making such decisions in the absence of full information; and
- deciding where decisions must be made urgently about risk.

Thus, multi agency working in these fields presents challenges both to the sufficiency of sharing for the purpose of integrated service delivery and risk management, and, at the same time, to the protection of appropriate confidentiality for all the categories of individuals about whom records are held

Figure 2: Summary characteristics of the case studies: MAA level

Case study (former labels in brackets)	*Country*	*Health and social care or crime and disorder (HSC / CD)*	*Geographical character*	*Clientele*	*MAA mandatory or voluntary (M/V)*	*Organisations in MAA (number, types)*
1	England	HSC	rural	mental health	M	24 (includingMH Trust, NHS Care Trust, social services, voluntary sector, private sector)
2	England	HSC	inner urban	mental health	M	14 (including social services, MH Trust, PCT, other voluntary groups). Additionally, an unspecified number of sheltered housing providers and GPs.
3	England	HSC	inner urban and suburban	Older people	M – partnership working mandatory, some discretion over form and members	5 partners interviewed (PCT, social services, housing, 2 voluntary bodies). Key NSF work done by a Strategy Group for Older People
4	England	HSC	urban	Older people	M – partnership working mandatory, some discretion over form and members	5 organisations interviewed. Approximately 25 organisations in total, including housing; PCT,social services and voluntary bodies
5	England	CD	urban	offenders (CDRP)	M	8 statutory orgs plus c40-50 voluntary orgs, including LA community safety; police; fire brigade; national charity
6	England	CD	rural	offenders (CDRP)	M	8 'responsible authorities', including police, LA community safety, PCT, Fire and Rescue. Approx 21 partners in total.
7	England	CD	mixed: small city and rural	violent and sexual offenders (MAPPA)	M	Approximately 20, although number is expanding, including probation, police, housing, voluntary sector, health sector, education, private security firm)
8	England	CD	large conurbation	violent and sexual offenders (MAPPA)	M	3 organisations as 'responsible authorities' (police, probation and prison service). Numerous 'duty to cooperate' partners including all NHS Trusts (27); local authority social services (10); local authority housing (10); local authorities (10). Plus victim support. Perhaps 65 partners in total, although this figure will fluctuate. This case study comprises a large urban area.

.

Data analysis

The data gathered from our interviews are being analysed at three levels. The first level is that of the MAA, the second level is that of the organisation and the third level is that of the individual interviewee. Thus far, we have conducted a variable-oriented analysis that has enabled us to map relationships between our independent and dependent variables across and between all three levels. This will be followed, over the next few weeks, by a theoretically-informed, case-based, configurational analysis of the social dynamics of each of our twelve cases. By means of this strategy, we hope to combine systematic, causal analysis of the social dynamics of data sharing, and also to situate cases in their specific historical, policy and local contexts.

In developing interpreting data, we have been very conscious of the strengths and limits of the methods we used to collect them. A rich, independent, understanding of the social dynamics of data sharing is probably best developed by means either of systematic observations of over a long period of time, using an ethnographic frame, and/or systematic analysis of case records. Both approaches are precluded in fields such as these, because of the impossibility of securing informed consent from all individuals whose data researchers might encounter in the field. Ethical approval would not have been granted for such a project, and these methods were, therefore, not seriously considered. Instead, we have relied on semi-structured interviews, supported by a limited amount of documentary evidence and the field researchers' observations and contextual awareness. These methods have allowed us to collect valuable data about workers' own experiences of multi-agency working, and to develop some contextual understanding of these data. The obvious limitation of the data is that we are obliged to rely primarily on interviewees' reported perceptions of institutional forms, on the one hand, and styles of data sharing, on the other.

In the present paper, we propose to focus on a sub set of the analyses performed thus far on our data; those that have shed particular light on the relationship between institutional forms and the ways in which frontline workers navigate ethical dilemmas[2]. As became clear in the discussion above, multi-agency working in our case study fields is mandated by central government by means of such policy instruments as new legislation and policy guidance. Indeed, many of the MAAs studied in this project owe their very existence to such instruments. We therefore wanted to know if our sample MAAs and their member organizations displayed strong hierarchical tendencies, and how, and how strongly, these tendencies impact on data sharing styles. However, as we also discussed above, neo-Durkheimian theory predicts that the sustainable and ethical institutionalization of formal policy instruments, such as these, requires the development of a much wider variety of institutional forms than those that are characterized by strong regulation. We were interested to find out if they were present, too, and with what effects. Conversely, we wanted to investigate whether strong institutional forms, particularly those involving strong assertions of hierarchy, are associated with excessive and counter-productive behaviours predicted by neo-Durkheimian theory, and whether these behaviours are less evident in MAAs and organizations displaying a mix of institutional forms.

Some empirical findings

Institutional forms

We begin by reporting some findings relating to these questions, in tabular form. First, we display a summary of our findings about the institutional forms characterizing each organisation in our sample. In Figure 3, three measures are reported. The first is an aggregated measure, using all the data from the subsidiary codes used to operationalise the concepts of social regulation and social integration. The second - 'Org by MAA' - shows the relative weight of the four basic institutional forms resulting from the degree of regulation coming from the MAA or national

[2] Readers who are interested in a more complete presentation of our findings will find the first tranche of results in 6 et al (2005b), and a more extensive analysis will be presented in 6 et al (2005c).

sources (governmental or professional), and the extent to which the organisation is integrated with the rest of the MAA. The final column – 'org by org' - shows the institutional forms that result from internal regulation, and the degree to which the organization is integrated within itself. Where a code is repeated (e.g. HH), this denotes a comparatively pure form; hybrid forms are shown by a sequence of codes in the order of greatest eminence.

The most marked differences between these scores are, as one would expect, on the regulation dimension. With only a few exceptions, MAAs add regulation, and do not reduce it. However, although we might expect that organisations would typically be more internally integrated than with the rest of their MAA, some organisations actually appear *less* integrated internally than they with the rest of the MAA: these are typically ones that have been specifically created as a result of the formation of the MAA.

Figure 3: Institutional forms of organisations in the 8 English MAAs

Org. case no	*Org function*	*Team employment structure*	*Aggregated instl form code*	*Org by MAA code*	*Org by org code*
1A	Merged NHS Trust		HH	HH	H/E
1B	Mental health Trust		HH	HH	H/E
1EIT	Early Intervention in Psychosis Team	Employed by 1A	EE	EE	EE
1CMHT	Community Mental Health Team	Employed by 1A & 1C	H/E	E/H	E/H
1CRT	Crisis Resolution Team	Employed by 1A	HH	HH	HH
1AOT	Assertive Outreach team	Employed by 1A	EE	E/In	EE
1C	Social Services (interviewee based in CMHT)		H/Is/E/In	H/Is	Is/H/In/E
2A	Mental Health Trust		IsIs	Is/Is	Is/Is
2CRT	Crisis Resolution Team	Employed by 2A	HH	H/E	HH
2CMHT	Community Mental Health Team	Employed by 2A and 2B	InIn	Is/In	In/Is
2EPS	Emergency psychiatric service	Employed by 2A	E/Is	Is/E	EE
2B	Social Services		Is/H/In/E	In/E	Is/In
2MH Day Centre	Mental Health Daycare Centre	Employed by 2B	H/E	E/H	E/H
2AOT	Assertive Outreach Team	Employed by 2B & 2C	E/In	E/In	EE
2C	Natinional charity for mental health		EE	EE	EE
3A	Social Services		HH	HH	HH
3B	Primary Care Trust		HH	HH	HH
3C	Local Older Person's Charity		EE	In/E	EE
3D	National charity for the elderly		H/E/Is/In	In	E/H
3E	Housing		H/E	H/E	H/Is
4A	PCT		H/Is	H/Is	HH
4B	Social Services		HH	Is/H	H/Is
4C	National charity for the elderly		HH	IsIs	HH
4D	NHS Acute Trust		[H/Is]		
4E	LA Housing, (Arms Length Mgt Org)		Is/H	Is/H	In/E
5A	Community Safety		H/Is	H/Is	H/Is
5DAT	Drug Action Team	Employed by 5A	H/Is	H/E/In/Is	EE
5B	Police		H/In	HH	In/H
5C	Information Services Partnership		HH	HH	HH
5D	Fire		H/Is	Is/H	H/In
5E	Sex abuse charity		H/E	H/E	E/H
5G	Drugs misuse clinic		Is/E	InIn	HH
5H	Children's services		H/Is	In/Is/E/H	E/In
6A	Community Safety		HH	HH	HH

6YOS	Youth Offending Service	Employed by 6A	HH	Is/H	H/Is
6B	Community Safety		IsIs	IsIs	Is/H
6C	Fire		InIn	Is/H	InIn
6D	Police		IsIs	IsIs	Is/In/E/H
6E	Addaction		HH	E/H	HH
6F	Primary care trust		Is/H	Is/In/H/E	IsIs
6G	Social Services; employed members of the DAT		H/Is	H/Is	H/Is
6H	IS Partnership		HH	HH	HH
7A	Probation		HH	HH	HH
7B	Housing		H/E	IsIs	H/E
7C	Social Services		H/Is	H/Is	H/Is
7D	Housing		HH	HH	HH
7E	Police		H/In	H/In	In/H
7F	Prison service		HH	HH	EE
7G	Mental health trust		H/Is	H/Is	H/Is
8A	Probation		H/Is	H/Is	H/Is
8B	Police		H/In	In/H	In/H
8C	Prison service		Is/H	Is/In/E/H	In/E
8D	Victim support		H/Is	H/Is	HH
8E	Housing		HH	HH	HH
8F	Primary Care Trust		H/Is	HH	IsIs
8G	Mental Health Trust		HH	HH	H/Is
8H	Housing		H/Is	HH	H/Is

Data sharing styles

Given the limitations of our methods, it is difficult to obtain robust measures of: the quantity of data that is actually being undertaken, how far, and in what circumstances it is being shared; whether data is being shared when it should be; and how far, and how well, personal privacy and confidentiality are being respected. The data relating to the dependent variable have therefore been gathered almost entirely from interviewees' reports, backed up, where available, by background documents. We encouraged interviewees to be candid, assuring them of the anonymity of their own identities and those of their organizations and MAAs, but the data relies heavily on their perceptions and experiences. Indeed, when we undertake our case-based analysis, we will be interested in exploring in some detail how and why their framing of the issues differ from each other.

Nearly all of the MAAs we examined had developed extensive formal documentation on the key aspects of their client information management. Most had local protocols on information sharing. Many had also adopted local confidentiality or privacy policies. In each case, of course, their work is governed by other codes that apply to their field. In the case of the crime and disorder field, the Association of Chief Police Officers' Data Protection Code of Practice (2002) was in force during the period in which most of the interviews were conducted. After the Bichard Report (2004) was published, ACPO and the Information Commissioner agreed to develop a new code to control police information management more broadly, subsuming data protection (National Centre for Policing Excellence, 2005). In the fields of health and social care, MAAs applied codes developed by professional institutes such as the British Medical Association and the General Medical Council, or codes published by government departments such as the NHS (2003) Code of Confidentiality. Moreover, many of the MAAs are constituted around certain types of document, such as a constitution or a written mandate from local or national authorities. Even those MAAs that have come into existence as a result of local choices rather than central direction, tend to produce written documents specifying their powers, roles and purposes. It is therefore unsurprising that Figure 3 shows that many of the MAAs display a bias for strong regulation in general and for hierarchical organisation in particular.

In none of the MAAs was the handling of client records conducted entirely electronically at the time of the interviews. By 2004, the NHS had achieved a lower level of digitisation of patient data than had the police and many other criminal justice organisations. In addition, the delayed introduction of the NHS National Programme for Information Technology (*Connecting* *for Health*), means that partnerships are either continuing to use local bespoke systems or else maintain paper records, and in most cases, both. The implementation of the Single Assessment Process for the care of older people has prompted investment in a number of specialist systems. By contrast, in policing, there are some well-established national system which are run on the Police National Computer (PNC), including the Violent Offender and Sex Offender Register (ViSOR),[3] the new, national record system used by the MAPPAs. But there is still very little technological infrastructure available for sharing data between agencies in the criminal justice system.

Access authorisation rules relating to client data on these systems varied considerably across our sample, even in the same policy sector. Some MAAs routinely allow accredited staff access to the whole database, while others permit access only to specific case records on the basis of a particular need to know. In general, mental health agencies permit accredited professionals more access than do the others. This may reflect the much greater integration of multi-professional teams and the practice of more intensive team casework in that field. Figure 4 summarises the key differences between MAAs in these respects.

Figure 4: Styles of information sharing in 8 English MAAs.

Case study	*Electronic records, paper or both*	*Whose data are shared*	*How data are organised*	*Scope of access to information held by other organisations (routine for whole database, case-by-case authorisation)*
1	chiefly paper	HSC patient	Depends on team and/or locality	At discretion of individual rather than via formal procedure.
2	paper, electronic	HSC patient	Some electronic DS schemes being piloted by social services	At team level, access at discretion of individual
3	paper	HSC patient	Electronic version of Single Assessment Process (SAP) being piloted.	Routine for whole database
4	paper, electronic	HSC patient	Some sharing between PCT and social services databases. Awaiting benefits of NPfIT (now Connecting for Health)	Generally routine, although exceptional cases referred to Caldicott Guardian
5	paper, electronic	Offender, victim	Sharing of electronic data at daily crime reduction meetings	Access formalised by protocol drafted by MAA level body, stating access controls
6	paper, electronic	Offender, victim	Some partners share information in a joint repository	Routine, with exception of anti-social behaviour data
7	paper, electronic	Offender; victim	New database being piloted.	Each case 'has an owner' in police and probation
8	paper, electronic	Offender; victim	Joint access to offender database for police and probation	By case by case authorisation in probation, prison service and Victim Support

Managing tensions between data sharing and privacy

For reasons discussed above, the assessment of how far, and how well, ethical dilemmas about data sharing and privacy are being resolved, depends heavily on interviewees' reports. One proxy for this measure is the confidence that interviewees expressed in the adequacy, first of data sharing and, second, of confidentiality. We have, therefore, constructed a simple ranking showing how confident the interviewees in each MAA and each organisation were, on average, that their MAA was sharing information of the right kind in the cases when they felt it ought to be shared,, and that it was respecting confidentiality appropriately. The results are presented in Figure 5. Clearly, averages are sometimes misleading, when they hide sharp divergences. Indeed, there were differences of view among the interviewees in almost every MAA, which means that,

[3] see http://pito.org.uk/what_we_do/intelligence_investigation/visor.htm

almost unavoidably, the resulting averages tend to converge just on either side of moderate confidence.

Figure 5: Interviewees' confidence in adequacy of sharing and confidentiality protection in MAA

Case study	*Interviewee confidence that information sharing in MAA is adequate and appropriate*	*Comments on interview confidence in information sharing*	*Interviewee confidence that client confidentiality is adequately and appropriately respected in MAA*	*Comments on interviewee confidence in confidentiality compliance*
1	M	General consensus of confidence that within-team sharing worked well; less confidence in sharing between teams across mental health system	M -> H	General consensus of confidence that within own team, confidentiality was respected, but less trust that others in MAA conformed to confidentiality norms
2	M	General consensus of confidence that within-team sharing worked well; less confidence in sharing between teams across mental health system; some distrust of other teams	M	General consensus of confidence that within teams, confidentiality protection worked well, but less confidence that other teams protect confidentiality as well as the interviewee's own
3	M -> H	Generally high confidence significant divisions: voluntary organisations felt excluded from sharing between statutory services	M -> H	Generally high confidence, apparently based n detailed prescription in protocols
4	M -> H	Generally high confidence, but conflict within the housing service over the relative priority of demands for sharing and confidentiality	M -> H	Generally high confidence, apparently based n detailed prescription in protocols
5	M	Some divergence of view: senior police officer frustrated that insufficient sharing was being done	M -> L	Senior police officer's demands for more sharing resisted by other officers and others in MAA on confidentiality grounds
6	M -> L	Marked low confidence among some organisations that had little trust and limited experience of other cooperation with other MAA members	M	Some internal divergence among police: Data Protection Officer concerned about confidentiality opposed various proposed extensions of sharing, demanded specific written authorisations etc
7	M -> H	General consensus score: Only one organisation concerned was district council housing body feeling that sex offender has been "dumped" on them without sufficient information having been shared with them	M	General consensus over confidentiality, although some disquiet within the Mental Health Trust. In particular, a manager feared litigation if personal data was shared inappropriately.
8	M -> L	Great diversity of views in very large and fragmented MAA	M	Some concern in prison service that more sharing was being done than was appropriate in some cases

In general, it seems clear that health and social care cases show higher levels of interviewee confidence in the appropriateness of sharing and of confidentiality practice in their MAAs than do the crime and public protection ones. The highest level of confidence, overall, appears to be shown by interviewees in the MAAs that bring together health and social care for older people, and weakest level of confidence by those in CDRPs, where conflict among the police, and between the police and other organizations, about the appropriateness of sharing is particularly marked.

There are few cases that exhibit significant divergence in the degree of average interviewee confidence in the extent of compliance with confidentiality and information sharing norms. In part, this reflects the fact that interviewees appeared to see these issues as correlative. If they had concerns about the nature and extent of sharing, they were usually on confidentiality grounds and conversely if they were concerned about the effects of confidentiality, it was usually on the ground that it blocked appropriate data sharing.

A richer picture emerges when data are analysed at the organizational, rather than the MAA, level although again the reader must bear in mind the probable skew in the distribution of institutional forms across the data set at this level. The theory predicts that:

- organisations that are markedly hierarchical will develop a sense of confidence that they are conforming to the rules appropriately, so long as regulation, in particular, does not become excessive
- organisations marked by isolates will show less confidence in the information sharing and the confidentiality practices of their own organizations, than workers in other organizational forms. For by definition, isolates tend to distance themselves from the organisations in which they are employed, and to show, at best, qualified loyalty to its practices. They also struggle to build trust with people in other organizations.
- enclaves will show more confidence in their own practices than in those of the rest of the organisation or MAA. By definition, an enclave will want to mark the boundary between its internal practices, in which its members will typically show great confidence, and those of others, in which its members will have significantly less trust. This ambivalence will probably show up in moderate confidence.
- Individualist organizations will display moderate confidence, because individualistic institutions cultivate a combination of wary vigilance and an effort to seize strategic opportunities.
- hybrid institutional forms are more likely to yield moderate confidence, because those tending to support strong and those tending to support weak confidence offset each other.

Figures 6 and 7 display simple frequencies on the data set of 55 organisations in England, and show the distribution of high, medium and low confidence in organisations' capacity for data sharing when appropriate (Figure 6) and in organisations' confidentiality arrangements (Figure 7), by institutional form. The results have been colour coded with the three traffic light colours to pick out associations with strong confidence (green), moderate confidence (yellow) and weak confidence (red). The colours on each line are given a letter code in the far right hand column for ease of viewing in monochrome printing. The colour coding has mainly been used where there is a continuous set of entries along part of a row. The tendencies are clear, although not absolute – as one would expect with associations found using this kind of coding at this level of aggregation and with the kinds of error bands to be expected of modest N qualitative research.

Figure 6: Confidence in organisations' appropriate information sharing, by institutional form

Institutional Form	H	H -> M	M -> H	M	M -> L	L -> M	L	Totals	Colour code
HH	3	1	7	4	0	2	1	**18**	**G**
IsIs	0	0	0	1	0	0	1	**2**	**R**
EE	1	0	0	1	0	1	1	**4**	**G (H) – R (M-L)**
InIn	0	0	0	1	0	1	0	**2**	
H/Is	1	1	3	5	1	1	0	**12**	**G**
H/Is/E/In	1	0	0	0	0	0	0	**1**	**G**
H/E	2	0	0	1	0	1	1	**5**	**G (H) – R (M-L)**
H/E/Is/In	0	0	0	0	0	1	0	**1**	
H/In	0	0	0	1	1	1	0	**3**	**Y**
Is/H	0	0	0	1	1	0	1	**3**	**R**
Is/H/In/E	0	0	0	0	0	1	0	**1**	
Is/E	0	0	0	0	0	1	0	**1**	**R/Y**
E/Is	0	0	0	1	0	0	0	**1**	**Y**
E/In	0	0	0	0	0	1	0	**1**	
Totals	**8**	**2**	**11**	**16**	**3**	**11**	**5**	**55**	

Figure 7***: Confidence in organisations' respecting confidentiality, by institutional form***

Institutional Form	H	H -> M	M -> H	M	M -> L	L -> M	L	Totals	Colour code
HH	4	3	5	5	0	1	0	**18**	**G**
IsIs	0	0	0	1	0	0	1	**2**	**R**
EE	1	0	1	1	1	0	0	**4**	**G (H) – Y (M)**
InIn	0	0	0	2	0	0	0	**2**	**Y**
H/Is	2	2	1	4	1	2	0	**12**	**G**
H/Is/E/In	1	0	0	0	0	0	0	**1**	
H/E	2	0	2	0	0	1	0	**5**	**G (H-M) – Y (M)**
H/E/Is/In	0	0	0	1	0	0	0	**1**	
H/In	0	0	1	0	1	1	0	**3**	**Y**
Is/H	0	1	0	1	0	1	0	**3**	**Y**
Is/H/In/E	0	0	0	1	0	0	0	**1**	
Is/E	0	0	0	0	0	0	1	**1**	**R**
E/Is	0	0	0	1	0	0	0	**1**	**Y**
E/In	0	0	1	0	0	0	0	**1**	**Y**
Totals	**10**	**6**	**11**	**17**	**3**	**6**	**2**	**55**	

Figures 8 and 9 display the same traffic light analysis of the data set by the function or sector. Given their greater articulation of individualism in their institutional mix, the police are slightly more likely to be associated with weak confidence on both dimensions. Interestingly and revealingly, confirming the theory, interviewees in voluntary bodies, which exhibit greater tendencies than other bodies toward enclaved institutional forms, tend to show greater confidence in their ability to respect confidentiality (marking boundaries) than in sharing information appropriately (blurring boundaries).

Figure 8: Confidence in organisations' appropriate sharing of information, by functional type

Org sector	H	H -> M	M -> H	M	M -> L	L -> M	L	Totals	Colour code
NHS – MH	5	0	2	3	0	2	1	**13**	**G**
NHS – PCT	0	0	2	2	0	0	0	**4**	**Y**
Local Auth – general	0	0	1	2	0	2	0	**4**	**Y**
Social Services	1	0	3	2	0	2	0	**8**	**G**
Housing	1	1	0	2	0	0	2	**6**	**G (H-M) – R (L)**
Community Safety	0	0	0	2	0	0	0	**2**	**Y**
Police	0	0	0	1	1	1	1	**4**	**R**
Probation	1	1	0	0	0	0	0	**2**	**G**
Prison	0	0	1	0	1	0	0	**2**	**Y**
Fire	0	0	1	1	0	0	0	**2**	
Voluntary	0	0	0	2	1	3	1	**7**	**R**
Private	0	0	0	0	0	1	0	**1**	
Total	8	2	10	14	3	11	5	**55**	

Figure 9: Confidence in organisations' respecting confidentiality, by functional type

Org sector	H	H -> M	M -> H	M	M -> L	L -> M	L	Totals	Colour code
NHS – MH	5	1	2	3	2	0	0	**13**	**G**
NHS – PCT	0	1	1	2	0	0	0	**4**	**Y**
Local Auth – general	0	0	1	1	0	2	0	**4**	**Y**
Social Services	1	1	3	2	0	1	0	**8**	**G (H-M) Y (M)**
Housing	0	1	1	2	0	2	0	**6**	**Y**
Community Safety	0	0	0	2	0	0	0	**2**	
Police	0	0	1	0	1	1	1	**4**	**R**
Probation	0	2	0	0	0	0	0	**2**	**Y**
Prison	0	0	1	1	0	0	0	**2**	**Y**
Fire	1	0	0	1	0	0	0	**2**	**G (H) – Y (M)**
Voluntary	3	0	1	3	0	0	0	**7**	**G**
Private	0	0	0	0	0	0	1	**1**	**R**
Total	**10**	**6**	**11**	**17**	**3**	**6**	**2**	**55**	

Finally, Figure 10 displays an analysis of the differences between interviewees' level of confidence in their organizations' capacity for data sharing and their level of confidence in confidentiality arrangements, by institutional form.

Table 10: Differences between confidence in sharing and confidentiality by institutional form

Institutional form	**Confidence in appropriate information sharing greater than confidence in respecting confidentiality** (total)
HH	2 (18)
EE	1 (4)
H/Is	2 (12)
H/E	1 (5)
Is/E	1 (1)
Total	**7 (55)**

Institutional form	**Confidence in respecting confidentiality greater than confidence in appropriate information sharing** (total)
HH	4 (18)
EE	3 (4)
InIn	1 (2)
H/Is	3 (12)
H/E	3 (5)
H/E/Is/In	1 (1)
H/In	1 (3)
Is/H	3 (3)
Is/H/In/E	1 (1)
E/In	1 (1)
Total	**21 (55)**

Institutional form	**No difference between confidence in approp-riate information sharing and confidence in respecting confidentiality** (total)
HH	12 (18)
IsIs	2 (2)
InIn	1 (2)
H/Is	7 (15)
H/Is/E/In	1 (1)
H/E	1 (5)
H/In	2 (3)
E/Is	1 (1)
Total	**27 (55)**

Discussion: the relationship between independent and dependent variables

In this section, we discuss the main findings that emerge from these analyses, in the light of our theoretical framing of ethical dilemmas created by tensions between data sharing and privacy. We will illustrate the discussion, too, by drawing on discursive evidence in our interview data. In particular, we ran a qualitative search of those codes that provide information about the kinds of worries interviewees have about data sharing and confidentiality. In particular, we systematically reviewed the evidence provided by professionals and managers about the sources of, and points of reference for, the ethical frames they bring to ethical dilemmas. We also searched these codes for their views about the effectiveness and utility of legal frameworks, organizational rules, professional codes and inter-organisational protocols relating to data sharing and confidentiality.

Hierarchy

We are, in general, somewhat cautious about our analysis of this institutional form, because formal aspects of institutions are notoriously easier to pick up in structured coding schemes than informal ones. This effect may be exaggerated, too, because of the primacy, and therefore the visibility, of formal policy instrumentation in the establishment of the MAAs – in particular, it may exaggerate the level of regulation. The discussion in this section must therefore be read with an awareness of a possible skew in the data set toward institutional forms on the right hand side of the matrix in Figure 1, that is, towards hierarchical institutions, in particular, and highly regulated institutions, in general.

In hierarchical settings, we would expect sharing and confidentiality practices to be matters of rule following, and to be undertaken in conformity with professional norms, organizational status and ascribed responsibiltiies. The two sets of MAAs conforming most closely to this institutional form are the local implementation teams for the National Service Frameworks for care for older people (cases 3 and 4)., and the MAPPas (cases 7 and 8). Both sets of MAAs have been established relatively recently, but in both cases their programmes are subject to considerable central government prescription and, in the case of the MAPPAs, their data sharing processes are also being embedded in nationally-imposed IT systems.

Our analysis confirms, overall, that that, as predicted by theory, an element of hierarchy (H) in the institutional mix tends to increase confidence that data are being shared appropriately, and that confidentiality is being properly respected. The presence of hierarchy tends, indeed, to be associated with increased confidence in *both* dimensions of data handling. So far as excessive regulation is concerned, there was, overall, in our data set, rather less grumbling by interviewees about the inhibiting effect of laws, rules and codes than we expected, and this generally holds, too, for organizations characterized by strong hierarchy (HH). This is surprising. In general, studies in the UK have tended to find that data protection laws and codes are widely perceived by frontline workers to inhibit effective multi-agency working. Our data, however, does not contain much evidence that workers experience data protection law as a strong inhibitor of their *own* data sharing practices, and this holds for codes and protocols, too. In contrast, our interviews contain far more complaints that workers in other agencies within the same MAA use data protection law and privacy codes as excuses for not sharing data that they are unwilling to share for other, less acceptable, reasons.

This is not to say organizations with strong H characteristics do not display evidence of excessive or inappropriate social regulation. Sometimes, the over-zealous but misdirected strengthening of formal regulation, in particular, leads to unethical behaviour in Maesschalck's terms. The problems are of several kinds. Perhaps the most pervasive problem, especially in the strong H cases mentioned above (3, 4, 7 and 8), stems from the over-zealous or careless imposition of formal rules from on high - from the top of the MAA, from the professional body or from government – in situations where they do not appear to street level workers to have an obvious rationale or purpose. The problem is compounded if the action that is supposed to follow from them is far from clear. Especially when formal regulation is not underpinned by shared, implicit understandings of ethical practice, the attempt to reinforce formal regulation may highlight, rather than help to resolve, the ethical dilemmas that workers face. Here, for example, is a quotation from a probation service manager in case 8, a MAPPA:

> *… if there's a piece of legislation would come down such as the MAPPA legislation which is saying you have a duty to cooperate and you sort of have a duty to share information but it feels as if the legislative framework to allow that information sharing to happen it doesn't feel it is in place and it feels as if there's a tension um all the time between the duty to cooperate and if you like the ability to cooperate and I think it is a real tension and the act would be quoted would the Data Protection Act (*Manager, Org: 8A).

In such a context, too, the *proliferation* of codes and rules that are intended to provide more clarity, simply adds to the problem, as an interview with a manager of a day centre in Case 2 illustrates well:

> *Well I mean, the thing is, I'll refer to psychological guidelines by the association, I would refer to social work guidelines. I'll refer to nursing guidelines …. We have got guidelines but we haven't got a policy (*Manager, Org 2B).

A second problem in strongly regulated settings, is that the existence of codes and rules may become a fig-leaf for practices that might otherwise be considered unacceptable. Here is a Superintendent of Police speaking about the liberating impact of the Crime and Disorder Act 1998, which established a legal mandate for data sharing to prevent or detect crime:

> *... the Crime and Disorder Act, and I can't quote the section, but there is a particular section around, really runs a train right through data protection because it says, well you know if it's in the interests of preventing crime and disorder and it's a responsible body that you're giving it to, then go ahead and give it and that's … the permission that we take to do it. In terms of best practice erm we're not there yet because we don't have a protocol which covers everything that we're actually, we actually share* (Manager, Org: 5B).

Yet another problem is that the existence of a strong regulatory framework can undermine workers' sensitivity to the ethical nature of decisions, by relieving them of a personal sense responsibility for them. In other words, strong formal regulation may push behaviour down-grid by encouraging isolate responses to ethical dilemmas. As a worker in a Drug Action Team in Case 5 told us, when asked if they were more worried about being blamed for sharing or not sharing data: '*From a personal side, as long as I could justify to myself that I'd followed due process …. I think from a personal side it really wouldn't matter to me'.*

As neo-Durkheimian theory would predict, then, the attempt to control behaviour by means of stronger formal regulation can, in practice, undermine the very capacity for ethical decision-making that it is supposed to reinforce. It does this by confounding or masking the ethical dilemmas that workers face, rather than providing help in navigating them ethically. In contrast, the mitigation of strong formal regulation by strong informal institutions may be more supportive of ethical decisions. As organizational sociologists know well (e.g. Misztal, 2000), effective, stable, hierarchical institutions rely as much on informal and unstated aspects of the social order as they do upon the formal, explicitly codified rules. In this context, the ability to navigate dilemmas with confidence rests mainly on experience, training, inter-personal trust and shared professional mores. Interviews given by professionals and their managers about their data sharing and confidentiality practices provide many reports of high satisfaction with data sharing practices, on these grounds. Here, for example, is a manager who works in an organization coded HH, and who is very confident about his team's data sharing practices. What is abundantly clear, too, is that their confidence, relies much more on a deeply ingrained, sense professionalism – and one, too, that is shared with other workers - rather than on the organisation's rules:

> *I think there are Trust guidelines, but I can't remember or even flicked through them, but I would have a very good idea of what was confidential, and it would be from my own professional organization and professional training (*Team leader, Mental Health Trust. Org 1B)

We have written in some length in another paper (6 et al, 2005b) about the dysfunctions associated with excessive reliance on formal regulation. As we have begun to see above, informal institutions can provide the means of providing organizational members with subjective understanding of the meaning and purposes of rules. They may also provide an institutionallysanctioned means of bypassing obstructive ones or dealing with gaps or contradictions in them. At the same time, strong reliance on informal practices can creates problems, especially if it becomes difficult for workers, and especially for their managers, to read informal institutions accurately. At best, there is a danger that, in the absence of obvious evidence to the contrary, managers simply assume that patterns of behaviour that have become routines and normal are necessarily ethical and acceptable. At worst, the workrounds and stratagems that come to be employed import inconsistencies and particularities into organisation's handling of ethical dilemmas and can thereby legitimate unethical behaviour. What is certain, is that the absence of transparency undermines an organisation's ability to assure its ethical standards.

Isolate

As predicted, strong articulation of isolate institutional forms tends to decrease confidence on *both* dimensions. In settings where isolate ordering plays a significant part in the mix, we would expect information sharing to be opportunistic, a matter of day to day coping, rather than based on principled decision. Isolates find various ways of distancing themselves from the form of social regulation under which they operate; that is, they conform to it both without enthusiasm and without strategy Indeed, in ethical terms, we would expect isolate institutional forms to be associated with an indifference to ethical issues, rather than with the positive challenging of them or the conscious overriding of them. But this indifference is the very source of the ethical problems that are predicted to be associated with isolate forms. In particular, isolate institutions may foster indifference to, or fatalistic acceptance of, the consequences of actions for which individuals feel able or willing to take no responsibility.

Isolate elements are most strongly apparent in Case Study 6, a CDRP in a rural area. The predicted problems are, indeed, evident in this case. For example, in the interview quoted below, a manager of a community safety team describes how data sharing fulfills the organisation's objectives, even though they recognise that it risks overriding professional principles. But – so distant is the manager even from professional codes, let alone from organisational ones – that they describe 'riding roughshod' over clients' rights as a 'technical' matter:

> *Erm, within the organisation I accept it, erm, I signed up objectives of the organisation and the guidance issued by Government. I actually think it, I think it's, it runs the risk of being excessive, the amount of information we're sharing and, and erm, in a sense you're technically in danger of riding roughshod over individuals' rights. (Manager, Community Safety Team. Org: 6B).)*

Conversely, interviewees from organizations displaying significant isolate elements were more likely than any other set of interviewees to be critical of their own data sharing or confidentiality practices, or of those of their organisations. This willingness to be critical is partly a function of their moral and psychological dissociation from the organization in which they work. But it sometimes allows the exercise of independent moral reasoning, albeit moral reasoning which never quite connects with decision processes in the wider MAA. The lack of confidence in the practices of their organizations is manifest in several ways. Some workers simply do the best they can on a case by case basis, knowing that matters are far from right, but with no great confidence that they will improve. Here, for example, is a professional worker in a Drug Action Team in the same CDRP, talking about the constraints imposed by confidentiality rules on their ability to work in a multi-agency setting, but apparently accepting them in a fatalistic manner

> *No, I think we, we all understand the constraints under which we've got to… I can't issue crime, I can't issue police officers with health data, I can't issue Health crime data, erm, and we just have to, to play in that way. (Org 6G).*

As we saw above, other workers cope by dissociating themselves from the ethical consequences of their actions, and others, still, resort to behaviour that is designed simply to defends themselves against blame for unfortunate consequences. One strong theme that emerges from interviews across our data set is the use made of data protection legislation or professional confidentiality norms to insulate professional workers from exercising professional responsibility for sharing data appropriately. For example, in case study 8, a MAPPA, overall a strongly hierarchical MAA, we found several agencies complaining about psychiatrists who are unable or unwilling to resolve dilemmas presented by patient confidentiality, on the one hand, and the risk associated with mentally ill people, on the other:

> *…there was certainly one occasion where it had been reported that an individual was extremely dangerous and er should not be seen, no-one should see the person on their own. That was reported as being a comment from the psychiatrist who had been looking after this guy, but we couldn't get a psychiatrist to actually say that. Couldn't actually get him to put that into a report or to provide any advice to us. And that is frustrating, and that was frustrating. And I think he sort of held, he hid behind the patient confidentiality (*Director of Public Health in a Primary Care Trust: Org 8F).

Another manifestation of the lack of confidence in data sharing or privacy arrangements is to call for reform. One of the more interesting hybrid forms in our sample is the H/IS form. Interviewees situated in this form tended, as would be predicted by theory, to exhibit high problems in forming trusting relationships across, or even within, organizational boundaries, and they also had a high awareness of the ethical problems. But interspersed in their accounts are specific calls for reform, and in some cases, some tentative optimism that matters might improve. In other words, the injection of some element of H seems to create some confidence in that direction.

Enclave

The articulation of enclaved elements within the institutional mix is predicted to be associated with patterns of information sharing that strongly differentiate the in-group, within which sharing will be regarded as vital, and out-groups, with whom information sharing will be regarded with suspicion. Consistently with the hypothesis, the mental health case studies, where enclaved elements are most clearly marked, show the greatest tendency to emphasise sharing of client information within the specialist team (assertive outreach, crisis resolution etc). There is also a distinct tendency not to trust other teams within the wider MAA with information. The excesses of enclaved organizations stem, then, from inappropriate concern with boundaries and inflexible attachment to principles which define their special purpose or character. The overall tendency is to inhibit data sharing across the MAA, even when it is appropriate, and to make a fetish of the principle of confidentiality as a way of policing those boundaries. Here, by way of example, is a very clear statement of such an approach, from the head of a resettlement service working in a prison:

…we take the view that confidentiality is within the organisation, so we need … more people need to know what's happening, but it's kept within the organisation and that's where the confidentiality stops when it goes out (Head of Resettlement Service, Org: 7F).

Enclaves also tend to develop strong clientalistic relationships with those they perceive as their particular supporters or stakeholders. That is to say, they tend to develop a strong sense of loyalty to what they regard as their own client base, and to protect their interests, as they perceive them, in competition with other client groups or from the incursions of other professional workers. This is an important source of the commitment to clients or patients often displayed by enclaves in the social policy world, but it is also a potential source of unethical behaviour. Here is a worker in an emergency psychiatric team, which has frequently to deal with mentally-ill people in a confused, distressed and, sometime, a dangerous state. They are complaining about the unwillingness of the local Drug Action Team to share data about their clients.

> *Well because of the nature of their work, they've got like a very, they've got very strict confidentiality rules between themselves and their clients. And unless the client has got a written statement with us here authorising us to get information from drug and alchohol teams they just wouldn't give us any information (*Psychiatric worker. Org 2E)

Enclaves can also be a source of concern within the hierarchy of MAAs, because of their over confidence about their own, internal data sharing practices and their unwillingness to integrate with the rest of the MAA:

> *I don't like the idea of teams having their own little confidentiality sort thing, you know. We need to be mindful of confidentiality, and we need to be sharing information with other people within a fair framework of risk and we need to be mindful of people's confidentiality because it can break down. People can get free and easy (*Team Manager, Org 1B).

Enclaved institutional forms are to be found most often in teams on the margins of MAAs in our sample, and since this is where many voluntary organizations are to be found. The result is that they inhibit data sharing between the statutory sector and the voluntary sector in multi-agency settings. In general, they tend both to result from and to reinforce distrust between organizations. While they can sometimes act as the voice of principle and a source of ethical awareness within an MAA, they can also undermine effective multi-agency working in significant ways.

Individualism

In settings which exhibit a greater degree of individualism (In), albeit in settlement with hierarchical and other elements, we expect sharing to be agreed on a case-by-case basis, and subject to individual discretion. Because weakly regulated institutions allow greater scope for disagreement between individuals, and for differing interpretations of the same practices or rules, we should also expect the emergence of conflict. This may erupt between formally sanctioned authorities and people in subaltern roles, or between people in different agencies. We would also expect the weak level of social integration to lead either to a more instrumental attitude to data sharing and confidentiality than in enclaved settings, or to the strong assertion of personal ethical standards.

These features are, indeed, to be found clearly in organizations in our sample with significant In elements, and especially in case study 5, a CDRP. This MAA included two managers (*B* and *D*) engaged in vigorous individualistic behaviour that ran counter to the information sharing culture of their organisations (B and D). Ethical considerations were clearly subordinated to their desired outcomes. When asked about their approach to information sharing, a police superintendent (who is also quoted above) talked freely of their role in influencing the employment of street wardens by the local authority to tackle anti-social behaviour. In this instance, the interviewee took a personal role in vetting their suitability, and justified blocking one individual in the following way:

> *And that individual had been arrested for murder, erm and er was not, I think was charged and acquitted, but there was very real concerns about the person's character and there're the sort of things that they needed to know but I really and truly I've influenced that person's employment and and and again you're back to, does the end justify the means, and I dare say a barrister could earn a few*

> *pounds out of [XXX] Police for that particular case, but what do you do, you know do you then that run by and you have somebody who has a fetish for martial arts erm become a street warden to go out and tackle anti social behaviour, I think (laughs) it would be madness.* (Police Superintendent: Org 5B*)*

This focus on instrumental action in relation to substance of the particular judgments about the use of information is supported by an instrumental approach to making decisions. The process typically involves cutting deals with colleagues and in playing the role of broker or kingpin between different groups, by securing personal control of expertise:

> *Now the information sharing there [with local authority housing and Sure Start] is fantastic, because if you want any information you just walk next door and ask and it's done, and it's done because they share the same canteen, they share the same changing facilities, you know what I mean, it is one, it is one body that actually work together, so if you ask them what the protocols are, I suppose you ask me cos I'm responsible for them, the answer is there aren't any, they just do it, they work together on a day to day basis because they're all dealing with the same problems, erm and assisting each other in tackling their problems… (*Police Superintendent: Org 5B)

Where elements of In are present in otherwise strongly integrated organizations, we have found some evidence of individualistic behaviour amongst people who believe that their personal effectiveness depends on stratagems at odds with a dominant culture. This is most marked in our sample amongst the police whose results-oriented training tends to grate against the greater preoccupation of caring and health professionals with the rights of their clients. It is in this context that we found some of the clearest expressions in our *local* cases, of the clash between the dominant individualist ethical system that privileges the immediate rights of known individuals and a Utilitarian framing of data sharing that wants to privilege the interests of the wider public, however distal the risk. Here, for example, is another senior policeman, who is joint chair of the MAPPA in case study 7. He is speaking in an interview in which he stands up for an ethical position which he knows not to be consistently shared. He does so on the grounds that, in a field devoted to protecting the public against particularly repugnant crimes, the free sharing of almost all personal data can be justified. For this person, there is a straight choice between data sharing and privacy, and they are confident they how to make it.

> *I would say that any snippet of information from whatever source could prove to be crucial in the management of a sex offender. Now at the end of the day, I appreciate there have got to be safeguards which are built into that and the safeguards of the human rights act etc. But you've got to look at the duty of care we have as a statutory agency in terms of the management of the whole issue around public protection* (Police: Org 7E).

As one would expect, then, the presence of conflict over data sharing in organisations with a significant element of IN is associated with generally low confidence that *both* data sharing and confidentiality practices are appropriate.

Conclusions

Public services in the UK are being asked to share information with other agencies in order to manage behavioural risks and, at the same time, are under increased pressure to maintain the appropriate confidentiality of their clients' personal information and of the personal information of other people too. As political concern with risk has risen, the government has decided to introduced multi-agency arrangements mandated to manage risk. In so doing, it has also introduced rules that are steadily more formal, explicit and detailed, in the hope of ensuring greater horizontal consistency in decision making, especially decision-making about data sharing..

The analysis presented here gives little room, however, for believing that these changes have eliminated the dilemmas facing frontline workers, nor have they limited scope for discretion and judgment. Indeed, what may well have happened is that the difficulties of resolving these dilemmas have been increased. The proliferation of laws, rules, codes and protocols compound the problems of ethical decision making. Nor has the introduction of such rules obviated the problems of interpreting them, resolving conflicts, and in some cases, finding ways round the rules.

It is clear, too, that the ways in which frontline workers choose to navigate these dilemmas is shaped by the institutional setting within which dilemmas are framed and choice exercised. We have demonstrated the usefulness of neo-Durkheimian institutional theory in analysing how judgments about personal information are made in some prominent policy fields. The study shows that distinct styles of handling personal information and that these styles can be explained by their consistency with the deeper institutional character of the organisational settings in which they are found. Ways of managing personal information and the settlements between confidentiality and privacy, are seen to be intelligible and understandable responses to these organizational settings. In particular, the interaction of formal and other types of regulation teaches us that there are limits to law makers' capacity for prescribing how agencies make choices between the risks associated with false negative and false positive judgments when dealing with needy, vulnerable or risky people. The upshot of all this is that we cannot expect public services to manage ethical dilemmas with the transparency, consistency and predictability that we might like.

REFERENCES

6 P, Bellamy C and Raab C, 2004, Data sharing and confidentiality: spurs, barriers and theories, paper given at the Political Studies Association conference, University of Lincoln, April 2004.

6 P, Raab C and Bellamy C, 2005a, Joined up government and privacy in the United Kingdom: managing tensions between data protection and social policy, Part I, *Public administration*, 83, 1, 111-133.

6, P. Warren A., Bellamy, C. Raab, C and Heeney, C. 2005b Social policy as judgment: risks of injustice and the injustice of risk in the use of personal information. Paper given to the Annual Conference of the Social Policy Association, June 2005.

6, P. Warren A., Bellamy, C. Raab, C and Heeney, C 2005c The governance of information sharing in networked public management. Paper to be given the 8th Public Management Research Conference, hosted by the School of Policy, Planning and Development, University of Southern California, at Los Angeles, 29 September to 1st October 2005

6 P, Seltzer K, Leat D and Stoker G, 2002, *Towards holistic governance: the new agenda in government reform*, Basingstoke: Palgrave MacMillan..

Association of Chief Police Officers, 2002, *Code of Practice on Data Protection.*

Bellamy C, 6 P and Raab C, 2005a, Joined up government and privacy in the United Kingdom: managing tensions between data protection and social policy, Part II, *Public administration*, 83, 2, 393-415.

Bellamy C, 6 P and Raab C, 2005b,Multi-agency working in British social policy. Risk, information sharing and privacy. *The Information Polity.* 10, 1-13.

Bellamy C, 6 P and Raab C, 2005c, Personal data in the public sector: reconciling necessary sharing with confidentiality?, in Lace S, ed, 2005, *The glass consumer: life in a surveillance society*, Bristol: Policy Press.

Bichard, Sir M. 2004. The Bichard Inquiry report, London: Home Office, available at http://www.homeoffice.gov.uk/docs4/bichardreport.pdf

Buss A, 1999, The concept of adequate causation and Max Weber's comparative sociology of religion, *British journal of sociology*, 50, 2, 317-329.

Department for Constitutional Affairs, 2003, *Public sector data sharing: guidance on the law*, London: Department of Constitutional Affairs.

Douglas M, 1982a [1978], Cultural bias, in Douglas M, 1982, *In the active voice*, London: Routledge and Kegan Paul, 183-254.

Douglas M, 1982b, *Essays in the sociology of perception*, London: Routledge and Kegan Paul.

Douglas M, 1992, *Risk and blame: essays in cultural theory*, London: Routledge.

Douglas M, 1996, *Thought styles: critical essays on good taste*, London: Sage.

Fisher, C. 2001. Managers' perceptions of ethical codes. Dialectics and dynamics. *Business Ethics. A European Review.* 10(2) 145-156.

Durkheim É, 1951, [1897], *Suicide: a study in sociology*, tr Spaulding JA and Simpson G, London: Routledge.

Kemshall H, 2002, *Risk, social policy and welfare*, Buckingham: Open University Press.

Laming, Lord H, 2003, *The Victoria Climbié inquiry*, London: Department of Health and Home Office, available at http://www.victoria-climbie-inquiry.org.uk/finreport/finreport.htm

Lewis, C, 1993, Ethics codes and ethics agencies. Current practices and emerging trends, in H G Frederickson (ed), *Ethics and Public Administration*. New York:M E Sharpe..

Maesschalck, J. 2004. The impact of new public management reforms on public servants' ethics. Towards a theory. *Public Administration* 82 (2) 2004: 465-489.
Mars G, 1982; *Cheats at work: an anthropology of workplace crime*, London: Allen and Unwin.
Misztal B, 2000, *Informality: social theory and contemporary practice*, London: Routledge.
National Health Service (NHS), 2003, *Code of confidentiality*, Leeds and London: National Health Service.
National Centre for Policing Excellence, 2005, *Code of Practice on the Management of Police Information. Available at* http://www.homeoffice.gov.uk/crimpol/police/bichard/index.html
Performance and Innovation Unit, 2002, *Privacy and data sharing: the way forward for public services*, London: Performance and Innovation Unit, Cabinet Office (now the Prime Minister's Strategy Unit).
Plant, J. 1994. Codes of Ethics, in T L Cooper (ed) *Handbook of Administrative Ethics.*New York: Marcel Dekker.
Raab CD, 6 P and Bellamy C, 2005, Sharing client information in public services: the management of blame, paper presented at the European Consortium for Political Research, Joint Sessions of Workshops, Granada, 14-19 April 2005.
Rayner S, 1992, The cultural theory of risk, in Krimsky S and Golding D, eds, *Social theories of risk* Westport, Connecticut: Praeger.
Reder, P., Duncan, S. and Gray, M., 2003, *Beyond blame: child abuse tragedies revisited*, Brunner-Routledge, London.
Thompson M, Selle P and Grendstad G, eds, 1999, *Cultural theory as political science*, London: Routledge.