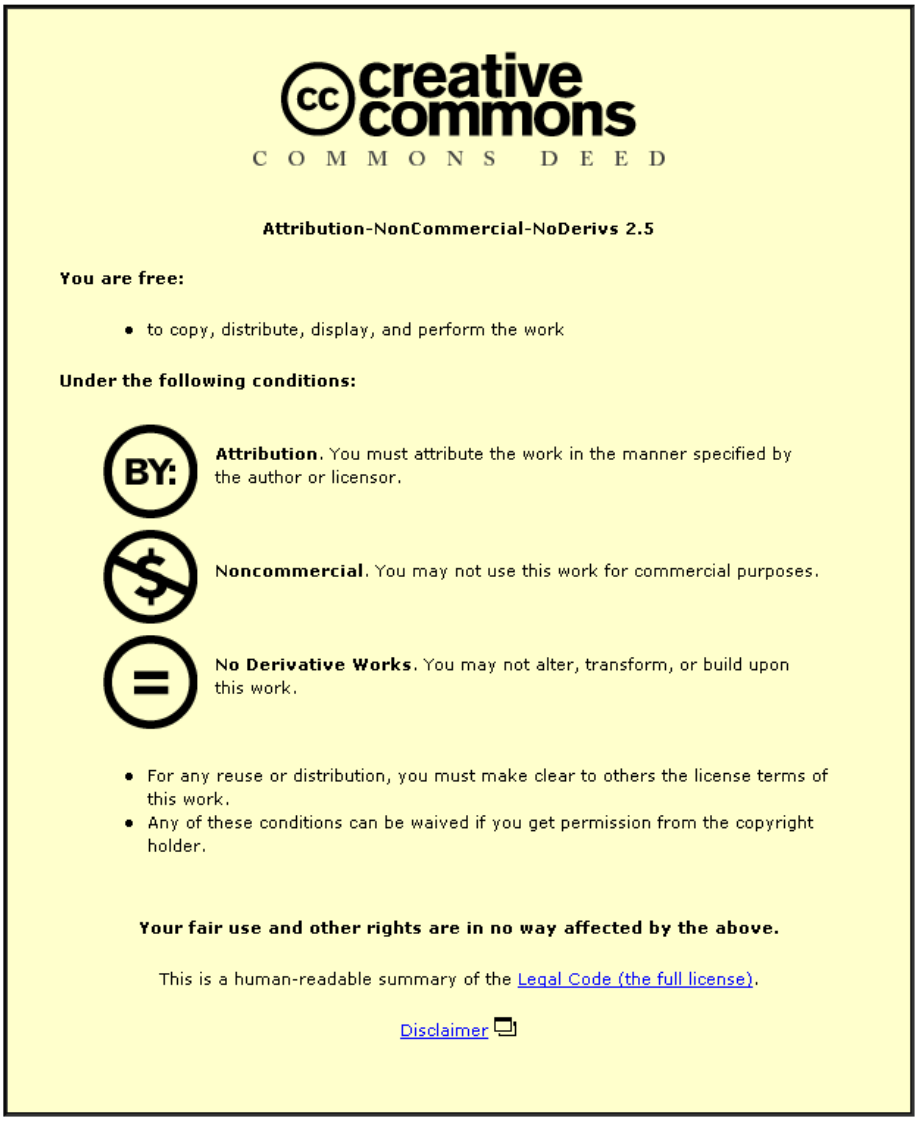


creative commons

COMMONS DEED

Attribution-NonCommercial-NoDerivs 2.5

You are free:

- to copy, distribute, display, and perform the work

Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor.

Noncommercial. You may not use this work for commercial purposes.

No Derivative Works. You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full license).

Disclaimer

The Factors involved in Sharing Information between Public Agencies

Ashley Cairns, Thomas W. Jackson, Louise Cooke
Department of Information Science, Loughborough University
Leicestershire, UK, LE11 3TU
a.s.cairns@lboro.ac.uk; t.w.jackson@lboro.ac.uk, l.cooke@lboro.ac.uk

Abstract

With the increasing move to partnership working in the public sector this paper looks at the main barriers in place which reduce the chances of Public Agencies working together. Agencies such as the Police, Local Councils, Youth Services and Health Services would like to work closer to improve their ability to serve the public whilst reducing the costs associated with this. A review of the literature along with personal experience from talking to and working with these agencies has identified the key elements affecting data and information sharing. The paper has found that whilst the agencies themselves are able to work on many of the barriers to data and information sharing the Data Protection Act 1998 continues to act as a deterrent.

1.0 Introduction

The technological world of 1998 was very different from that existing now in 2011. The growth of the Internet and Smart phones has moved information to a point where it is now expected to be instantaneously available anytime, anywhere. Information has now become a resource in its own right. 'New information needs to be disseminated continually to key individuals within organizations and as a result is treated as an economic resource' [1]. This has ramifications for organisations that need to ensure that their systems are able to provide this. Not only do their systems need to be able to provide this but they need to ensure they are legally allowed to do this.

A major problem that Public Agencies in particular are facing is to make informed and timely decisions they need to ensure they have all relevant information available. For example, a local housing authority is rehousing a single man in his 30's who has recently been released from prison. The housing authority would like access to the criminal history of this man so they can make an informed decision as to where to place him. If he had been in prison for drug related crime, they may want to avoid areas of high drug crime, if it was for a child abuse crime they would want to avoid areas near schools or community centres. In any circumstance the housing authority are likely to want to avoid housing the man near his victims. This is information that the housing authority will not have access to. Other Public Agencies such as Probation or the local Police will have this information but under the Data Protection Act [13] conditions 2, 3 or 5 neither the Police nor the Probation Service could lawfully pass on the information.

'If the market has imperfect information then the market fails to act efficiently.' [2]

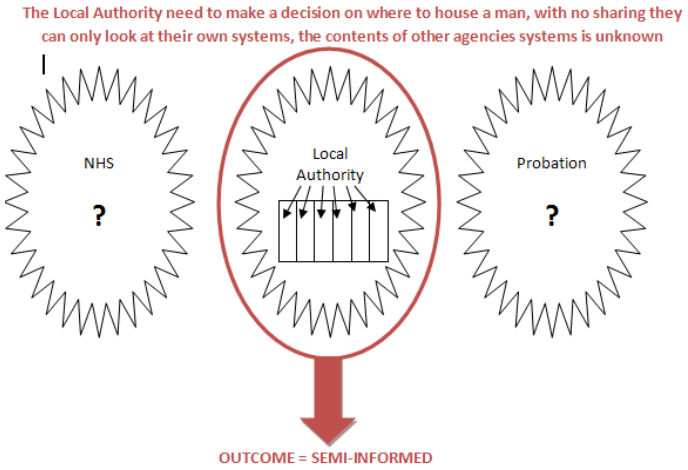


Figure 1 Semi-informed decision

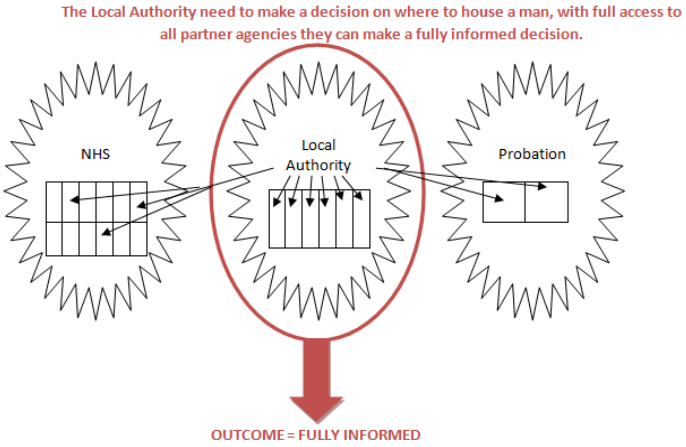


Figure 2 Fully Informed decision

A fully informed process requires information sharing between agencies. From an information perspective the ideal situation is real time access to all partners' systems. This would ensure timely and accurate decision making.

This paper begins by identifying three case studies where information sharing between Public Agencies was suboptimal and why there is now 'strong pressures from central government to increase inter-organizational information exchange.' [3]. The paper then discusses the role of the Data Protection Act in Public Agency interagency information sharing and the success story of the Childrens' Act 2004[14]. Factors affecting the success of information sharing are then identified and discussed. Finally the paper concludes with a short discussion on who needs to deal with each of the influencing factors.

2.0. Case Studies: The Need to Share Information between Agencies

Without access to other agencies' systems you may never know what you do not know. Whilst access to the other agencies' system is not required the relevant data from that system must be provided in a timely manner. People can then be confident they have access to all data/information that could be relevant to make a fully informed decision. This is particularly pertinent with the likes of the Soham case [15] in 2002. Huntley had come to the attention of Humberside Police and Humberside County Council Social Services on multiple occasions but was never convicted. Huntley applied for a caretaker job at a school in Cambridgeshire under a different name where the CRB (Criminal Records Bureau) check would have gone through Cambridgeshire Police. The Bichard inquiry [16] carried out following the Soham case showed that actions and decisions taken prior to the murders were made on the basis that those acting had all available information and people were working to the best of their knowledge. Without access to other sources they simply did not know that there was other information they should be considering before acting. From the Major Case Review carried out post trial it became evident that although not the fault of the Police Forces, if other systems and process been in place they

may have been able to reduce the chances of this happening. This was highlighted in Thomas and Walports' Data Sharing Review [4] 'The results of the Bichard inquiry show that better use of information might have prevented the Soham murders'. Another key message of the Bichard Inquiry was the finding that 'an IT system capable of allowing police intelligence to be shared nationally is a priority.'

The Pilkington case [17] in October 2007 involved the suicide of a mother and daughter as a result of repeated antisocial behaviour towards the family in Leicestershire. This is another example of where information sharing has been raised as a priority. The family had come into contact with the Police and local services on multiple occasions. Each individual contact with the Public Agencies was not enough to raise concern, but had the systems been in place to allow agencies to share information they may have been able to identify the family as vulnerable and been able to work with the family to make changes and improve their quality of life. As a direct result of this case nationwide the Police and other Public Agencies such as local councils are working hard to try to find a solution to enable them to identify vulnerable callers at point of contact. Most the Agencies internally now have flags, where if a person has called x number of times within a set period of time they are flagged as vulnerable and more attention is given to what can be done to solve the problem.

The Bichard Inquiry highlighted the need for information sharing between forces, but other cases (such as Climbie in 2000 [18]) involving a more multi-agency approach, in particular child abuse cases, have highlighted the need for greater interagency information sharing.

The Climbie case was a child abuse case which ultimately lead to the death of Victoria Climbie. Prior to her death the Police, four different local authority Social Services departments, the NHS and the NSPCC (National Society for Prevention of Cruelty to Children), had all come into contact with the family and noted the abuse. All agencies involved were found to have acted inadequately and as a direct result of this case changes were made to the legal system with the introduction of the Childrens' Act 2004 [14] and the formation of the Every Child Matters initiative [19].

It is clear that in the Public Sector information sharing and Partnership working (in particular) has moved high up on the agenda. Even to the extent that the government is currently carrying out a consultation with local governments with regards to community budgets, where they are asking local governments what they would like from the government to be able to carry out their work better.

3.0 Big Barrier to Sharing Information?

The Data Protection Act 1998 [13] was introduced in 1998 to replace and consolidate earlier legal Acts such as the Data Protection Act 1984 [20] and the Access to Personal Files Act 1987 [21], as a response to concerns about individual's right to privacy in an increasingly digital age. It was introduced to bring UK law in line with the European Directive of 1995 [22].

Since the introduction of the Data Protection Act there has been little practical guidance in its implementation with regards to information sharing. The ICO did issue a Data Protection Good Practice Note for Data Sharing Between Local Authority Departments [23]; the note clarifies that even if the Local Authority is passing information to another department within the Authority it must comply with the second Data Protection Principle as this passing of data would be a secondary use for the data. Although this helps to understand the need to satisfy the condition before passing the data between departments it reinforces an increased cost of sharing the data and hence reduces the likelihood of the data being shared. It again emphasises not sharing over sharing data.

The ICO recently produced a Data Sharing Code Of Practice [24]; this does provide some case studies as examples of what to do in particular situations and some templates for data sharing protocols. However the document is lengthy and seems in many places to simply reiterate the Legal Acts without further clarity.

In terms of legislation again there has been little to help bolster the defence of agencies who do carry out information sharing. The legitimacy of information sharing is often based on consent as rarely would sharing information fall under the 2nd condition of the Data Protection Act, often although data is collected for one purpose it can be very useful in others. For example, when data is collected at a crime scene it is collected for the purpose of solving a crime, however the charity Victim Support find it useful to be able to have access to the details of the victim so they can contact them to help offer support and practical assistance whilst the victim comes to terms with the crime. The passing on of this data would not come under condition two of the Data Protection Act, this is not what the data was intended for, but it is likely at least some of the victims of crime

would like the support Victim Support can offer them. A workaround has been put in place where by Police Officers attending the crime will now explain what Victim Support do and instead of victims opting in for the services as they once did it is now an opt out. This is based on the assumption that, in the immediate reality of a crime, the victim has many concerns other than someone phoning them later or the next day to offer support.

There is a degree of legitimacy to data sharing with regards to crime prevention and national security (Data Protection Act Section 29 [25] Crime and Taxation). In many situations it is unclear what data may be relevant to prevent crime. Most organisations require that those requesting data under section 29 do so in a formal written manner with justification as to why they need the data. Two examples at random from a Google search found 'The Police must inform the University in writing' [26] and 'Always ask for a request formally, in writing and on the organisation's headed stationery' [27]. This leads to increased bureaucracy, but more importantly could delay vital data being received. The decision to disclose is ultimately up to the individual ('it is up to you to decide to release personal information under this exemption' [23]). This can make people over cautious, it would be interesting to see how the recent ICO fines have affected disclosure under section 29 as people may be even more cautious now about sharing data, with the fear of incurring penalties for the organisation and perhaps in turn themselves.

4.0 Lessons of Success

There are a couple of Laws which explicitly allow agencies to share data/information in particular cases such as The Crime and Disorder Act 1998 [28](Police for crime prevention) and The Children's Act 2004 [14](multiagency for child well being).

'Improvements to the way information is exchanged within and between agencies are imperative if children are to be adequately safeguarded . . . [E]ach agency must accept responsibility for making sure that information passed to another agency is clear and the recipients should query any points of uncertainty' Lord Laming Review 2003 [18].

As a result of the Lord Laming Review in 2003 which identified information sharing as a weakness both within agencies and between agencies The Childrens' Act 2004 was introduced. This Act requires each local authority to set up a Local Safeguarding Children Board (LSCB) where key partners involved in Safeguarding children must all be represented. 'The overall aim is to encourage integrated planning, commissioning and delivery of services as well as improve multi-disciplinary working, remove duplication, increase accountability and improve the coordination of individual and joint inspections in local authorities.'[29]. Many families receiving attention from agencies can feel that their lives become a 'revolving door' for meetings with multiple Public Agencies, all with similar agendas and often similar courses of actions. One practitioner commenting on the situation said 'it's amazing these families are able to keep track of the meetings they are required to attend'.

The Children's Act has helped partnership agencies legitimately share information on a legal basis. The LSCBs have helped clarify what each agency is doing and made collaborating easier as it has put a basis of information sharing in place. LSCBs also allow agencies to co-ordinate their work and actions to reduce the burden on the family of the work they are carrying out.

5.0 - The Role of Cost, Trust, Privacy and Infrastructure

5.1 Cost of Sharing

There are many costs associated with information sharing: 'loss of exclusivity to information'; 'investment of time and effort'; loss of autonomy; costs of technology; and 'perceived risk' [5, 6]. Whether these costs are real or perceived as in risk and loss of autonomy makes little difference as 'the link between perceptions and behaviour has been well substantiated.'[7]

It is important for Public Agencies to be provided with motivation 'beyond the barrier reduction to participate in information sharing.' [6] The provision by government of clearer guidelines around information sharing or statutes which allow Public Agencies to share information with each other would remove a significant barrier, which the Agencies themselves cannot. As mentioned earlier the Children's Act 2004 has significantly improved the way Public Agencies work together to improve the lives of children. The agencies themselves are already beginning to work on other barriers such as interoperability of systems; producing technical standards of data and creating processes which can enable information sharing. National standards for the Police (MOPI [30]) and NHS (Information Standard [31]) have been created which represent the overriding authority with

regards to these Agencies' information standards. This lack of a joined up approach for all Public Agencies means that whatever work these agencies do at a lower (local) level is undermined by Government/ National directives. There is a need for a more unified approach to Public Agencies from the top down. Whatever Public Agencies do at a local level they will always need to work with the national directive: if each of these agencies have differing directives they will each be working toward their individual goal and simply forming weak linkages to share data/information. This is increasing the cost of sharing to the Public Agency and thus reducing the chances of it happening.

Perhaps the most significant cost factor in the Public Sector at the moment is the economic outlay required for information sharing. 'A relative funding decline has increased the pressure to 'do more with less'' [8]. As each of the Public Agencies face a reduced budget they can afford less time to try to understand the legalities of information sharing and to work out how they can carry out information sharing. They are less able to provide resources in terms of both money and employees time to attend partnership meetings spending hours working out what they can and can't do and how they could/should do this. In the current economic climate of doing more with less it is more important than ever for the government to provide simplified/clear guidelines for the Public Agencies to work with. This will reduce the cost of sharing and increase the chances of sharing occurring.

There are two approaches to sharing information [12]. The first is single copy, there is only one copy of the information and it is this copy which is passed on and altered as appropriate e.g. a handwritten witness statement. The second is replicated copy approach; rather than the original information being passed around and altered, a copy of the information is passed on and changed, meaning each holder of a copy can change that copy without affecting the others e.g. Organisation A creates a proposal for funding a copy of this is emailed to Organisation B and C, where B and C are able to alter the proposal without affecting the original. This means the value of the information to the original owner is unchanged, with the exception that they have lost exclusivity to the information. However in a public sector setting where organisations are not exploiting information to produce products or profit, loss of exclusivity is much less likely to increase the cost of sharing, while 'Not losing one's own possession of information seems likely to lower the barrier to information sharing' [1]. Where the option is available replicated copy approach should be taken as this will reduce the cost of sharing.

5.2 Trust

'Trust is the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or confront that other party' [5].

Part of the Data Protection Act requires agencies to report when a breach has occurred: between November 2007 to May 2010 there were 1000 such breaches [32]. The press release states that these were due to human and technical error. This includes both breaches with regards to people disclosing information to the wrong people (data/information sharing breaches) and issues such as people losing laptops containing data (data security breaches). The press release points to guides such as that produced by the ICO [33] to help explain the Data Protection Act in simpler language, however the ICO has failed to produce such a plain language guide for data/information sharing. Whilst organisations now understand and implement data protection they are now at a point where, to an extent, they are scared to share information. The recent fines of agencies are likely to make agencies more wary about reporting breaches and reduce the transparency of mistakes. It gives the impression that the ICO do not trust organisations to do the right thing (rightly so in some cases) but this top down attitude of distrust does not help build an open flow of information between trusting agencies. For Public Agencies to share data they must trust the other Agency with whom they are sharing. The recent ICO fines [34] came from mistakes made within an organisation, the ease with which mistakes are made within their own organisation can make others extremely cautious of sharing even with those they believe to be trustworthy. The fines act as yet another deterrent to sharing data/information between Public Agencies.

What the statistics fail to show is the number of instances where the sharing of data between Public Agencies has had a positive outcome. Organisations, particularly Public Agencies, are never rewarded for any proactive approach to data and information sharing but are instead brow beaten by the Data Protection Act whenever the smallest mishap occurs. This has helped to create a culture in the public sector of fear of information sharing. There is a perception that they constantly need to find work arounds or a tedious link to an exemption clause to justify the need to share data/information, which ultimately could be lifesaving

5.3 Privacy

The biggest risk identified from Thomas and Walport 2008 Data Sharing Review [4] was '[the] main concern is the effect of a real or perceived loss of privacy. This may lead to a loss of trust'. The need to pay a fee to discover what data/information an agency holds on you acts as an 'effective deterrent and a barrier to transparency', this also reduces the level of trust people can have in Public Agencies storing data on them.

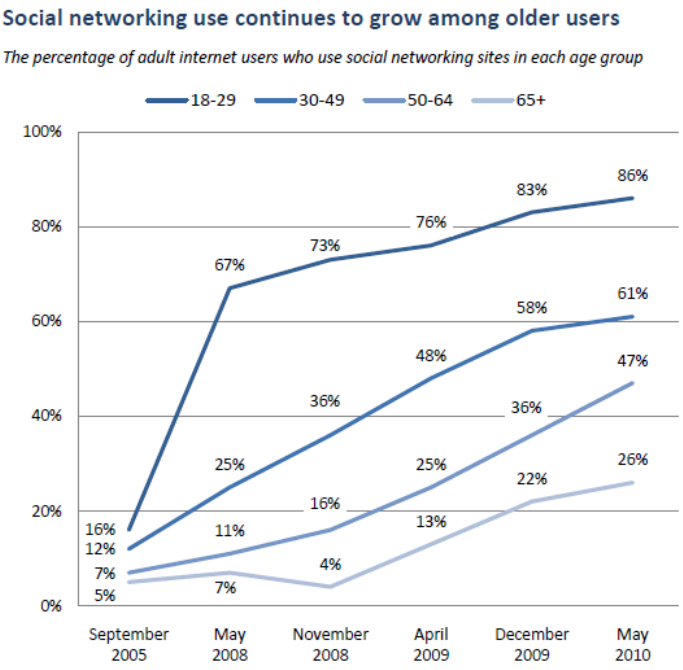
5.3.1 Media Reporting

Most people have read media stories where personal information has been lost. One case in 2007 of the data discs containing records on 7.25 million families claiming child benefit that were lost in the post [35]. The discs were password protected but the person who had sent the discs had breached all the security regulations in place at HM Revenue & Customs and the discs were never found. 2008 saw yet more media reports 'A record 37 million items of personal data went missing last year, new research reveals'[36] and again in 2009 **'**Thousands of NHS medical records lost**'** [37]. Every few months there appears to be a new media story about loss of data making the public worry about the security of their data.

These media stories highlight the need for a robust information governance framework, which can be used to minimise the risks of such data losses. The policies and procedures set out in an organisation's governance framework need to be regularly updated to reflect changing technologies and practices in the working environment. As was shown in the HMRC disc losses, even with policies in place people do not always follow them and it is important to try to automate data security as much as possible. For example, in Lloyds TSB they have a system in place where employees have different access rights to being able to copy data to removable media. You can only have the ability to copy data with business justification and even with the ability to copy data to these removable devices the data is automatically encrypted when written to the media. This has helped reduce the chances of data being copied, lost, stolen or used for fraudulent purposes.

5.3.2 Effect of Social Networking Sites

Loss of trust and privacy? One step closer to a big brother state? Whenever sharing of personal data is mentioned these are automatic responses from the media. In a world where millions of people update everyone on the minute details of their lives on social networking sites such as facebook and twitter, is this a view which is diminishing, particularly with Generation Z? (*The generation born between 1991 and 2010 also known as Generation I or Generation @ due to being the first generation to have been brought up with the internet[38]).* Attitude to data privacy does vary hugely between generations; many of Generation Z appear to see little problem with flaunting their lives all over the world, whereas older generations (in general) are more cautious when it comes to putting their personal lives online. This appears to be changing and the percentage of over 30's on social networking sites is growing quickly. In an online study carried out by Pingdom using Google Ad Planner data on US internet users [39] the most dominant age range in social networking turned out to be 35-44 (25%), but if you add in the 45-54 (19%) age range you have 44% of all social network users. Other research carried out by the Pew Research Center [40] in the United States found 'Between April 2009 and May 2010, social networking use among internet users ages 50-64 grew by 88% from 25% to 47%'. 'During the same period, use among those ages 65 and older grew 100%--from 13% to 26%'. Neither of these studies researched how the different age ranges used social networking sites and there appears to be no research in this area. The assumption is that people utilise the same social networking site in the same way for example LinkedIn is aimed at business connections where the likes of Twitter is for microblogging where users update the world on thoughts and actions.



Source: Pew Research Center's Internet & American Life Project Surveys, September 2005 - May, 2010. All surveys are of adults 18 and older.

Figure 3 Social Networking Use Continues to Grow

Social networking appears to have altered peoples' perception of privacy of data. A study found that 'many Facebook profiles they contain, or appear to contain, almost every category of data deemed especially "sensitive" by EU law' [9]. Another study found 'that users are generally unaware and/or unconcerned with protecting their privacy on social networking sites' [10]. Perhaps in 20/30 years when most of the population have grown up with this approach to online life the idea of privacy of data will have completely disappeared.

Can we truly still stand by the need for Public Agencies to respect a right to privacy many people themselves are not respecting? Or is it simply a case that the Data Protection Act was written in a different time, when few understood the true implications of not having the ability to share information between agencies? Does the danger of not sharing data between public bodies simply outweigh the dangers of sharing? Cases such as the Pilkington murder-suicide [17] in Leicestershire in relation to Anti-Social Behaviour or the recent Baby P case [41] in relation to Child Protection have highlighted the increasing need to utilise the information all these different agencies have, perhaps in ways that the agency itself has not thought of.

Drake et al 2004 [11] relates information sharing to a value chain within organizational subcultures. This could also be related to the different cultures present in different agencies that need to share information. Each of the cultures tend to 'require different data, information, and knowledge to do its work', have 'different abilities and propensities to collect and acquire its own information', 'gather data in different categories' and 'have different requirements for and uses of the outputs of its information, leading to challenges in coordinated and productive information sharing'. But it is these differences which in a Public Agency setting improve the agencies' ability to carry out work. For example Anti-Social Behaviour could be reported to a number of different agencies. Lady A reports 2 noise complaints to her local council due to late night noise, she then reports people throwing stones at her window to the police and reports 2 incidents of misbehaving children to a local youth group. These 5 incidents taken in isolation are likely to result in little action. However if each agency has access to the others information they could discover this is a pattern; all these incidents are occurring on a particular day and at roughly the same time. Further analysis shows this to be a group of 2 or 3 youths carrying out these incidents after getting off at the bus stop next to A's house following a youth club. The partnership Agencies can then take action and put a strategic plan together about how these agencies will tackle these youths and improve the situation for A. Individually none of these agencies would be able to put this pattern together and resolve the issue, together they provide different perspectives and can work in unison to put a solution in place. For example the police may caution the youths about what could happen if they continue their actions, the youth services may work with the youths to alter their behaviour and the local council could notice lighting at this bus stop is poor and install more street lighting. It is unlikely without access to the other agencies information that

any of these actions would take place and it is likely that the behaviour would continue, perhaps escalating into a more serious issue.

One possible move to improve information sharing could be to alter Schedule 2 condition 1 of the Data Protection Act, from the 'The data subject has given his consent to the processing' to 'The data subject has not objected to the processing'. It would be useful to carry out a case study to see what effect this has on Public Agencies' perceptions to information sharing.

5.4 Infrastructure

'A major obstacle to information sharing is the lack of a framework and an infrastructure that allows government organizations to share information selectively with different user groups. Lack of such a framework creates unwillingness among government organizations to share their digital content.'[12]

Although most organisations do have some network enabled systems in place the idea of giving another organisation access to their system is not a favourable one. Within organisations usually different employees have different access levels to the systems which are relevant to the work they carry out, restricting access to only relevant data. A similar access level system would be required for external users of the system also. A system would be required to, in real time, enforce the access policies of the external users. This in itself is not too hard a task to accomplish but when you take into account the number of different external users from multiple different partners which could be requiring access to the system perhaps on a one- off basis, this adds a large administrative burden for the organisation to manage users and their privileges.

6.0 Conclusions

The current trend towards partnership working in Public Agencies is likely to continue under the direction of the current UK government. This leads to a need to improve Public Agencies' ability to work together; working together requires the sharing of data and information. There are a multitude of issues affecting how an organisation shares information. The technology and processes must be in place and there must be a desire from the organisations to work together on a common goal. Technology and processes are areas the organisations working together are able to work through themselves and problem solve as relevant.

The main barrier to sharing data and information that the agencies cannot work on is the legalities of sharing this data and information. There are certain well defined areas such as Safeguarding Children where there is clear legal guidance for a need to share information. In most areas there is a lack of legal basis for legitimate information sharing. The Agencies are often forced to rely on Statutory duties placed on public bodies as a reason to share data and information. The problem they face is that they are not always sure to what information they need access to complete their work. For example, the police have the ability to access data under section 29 Crime and Taxation of the Data Protection Act, however they may not know exactly what data from another organisation would lead to the prevention of crime.

Sharing between public agencies will continue to be suboptimal whilst the costs of sharing are so high. To be able to implement a sharing programme takes time and resources which are scarce in the public sector. There is a need to reduce the overheads and change the culture of fear surrounding sharing. A major factor in this is to consolidate and clarify guidance related to data and information sharing making it clearer for all. The publishing of the ICO's Data Sharing Code of Practice Consultation in October 2010 [42] has at least shown that the government understands that it is unclear for organisations who share data what they can and cannot do. The results of the consultation have not yet been published but discussion with people in Public Agencies who carry out data sharing suggests that unfortunately this paper has not made the situation any clearer. By the time the finalised consultation is published this may have changed and be more usable for day to day practitioners. It does show that there is a desire from the government to help clarify information sharing for practitioners.

In conclusion whilst the agencies themselves are able to work on many of the barriers of data and information sharing including reducing the cost of sharing and putting the infrastructure in place, other factors such as the Data Protection Act 1998 continues to act as a deterrent to information sharing. This is something the agencies will be unable to change themselves and needs to be looked at from a higher authority such as the government.

7.0 References

Journals

[1] Hatala JP, Lutta J (2009), Managing information sharing within an organizational setting: A social network perspective, Performance Improvement Quarterly vol 21 (4), pp5-33

[2]Coleman D.W, Hughes A.A, Perry,W.D (2009), The Role of Data Governance to Relieve Information Sharing Impairments in the Federal Government, 2009 WRI World Congress Computer Science and Information Engineering, vol 4 pp 267-271

[3]Richardson, S; Asthana S (2006), Inter-agency Information Sharing in Health and Social Care Services: The Role of Professional Culture, British Journal of Social Work vol 36 (4), pp657-669

[4]Thomas R, Walport M (2008) Data Sharing Review, Royal Academy of Engineering

[5] Yan Z, Sun B, Wang T (2009) A study on information sharing of e-government, proceedings of IEEE International Conference on Grey Systems and Intelligent Services, 2009 pp1331-1335

[6]Barua, A., Ravindran, S., & Whinston, A. B. (2007). Enabling information sharing within organizations. Information Technology and Management, vol 8(1), pp31–45.

[7] Brown M.M, Brudney J.L (2003), Learning Organizations in the Public Sector? A Study of Police Agencies Employing Information and Technology to Advance Knowledge, Public Admistrative Review, vol 63(1), pp30-43

[8] Hughes V, Jackson P (2004), The Influence of Technical, Social and Structural Factors on the Effective use of Information in a Policing, Electronic Journal of Knowledge Management, vol 2, pp75-86

[9] Edwards L, Brown I (2009), Data Control and Social Networking: Irreconcilable Ideas?. HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION, A. Matwyshyn, ed., Stanford University Press, 2009. Available at SSRN: http://ssrn.com/abstract=1148732

[10] Goettke R, Christiana J (2007) Privacy and Online Social Networking Websites, Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, May 14, 2007

[11] Drake DB, Steckler Nam Kock MJ (2004),Information Sharing in and Across Government Agencies: The Role and Influence of Scientist, Politician, and Bureaucrat Subcultures, Social Science Computer Review, vol 22(1), pp67-84

[12] Bhoopalam K Maly K, Mukkamala R, Zubair M (2007) Framework for Information Sharing Across Multiple Government Agencies under Dynamic Access Policies

[13] Data Protection Act 1998 **http://www.legislation.gov.uk/ukpga/1998/29/contents** **Retrieved 05/01/2011**

[14] Childrens Act 2004 http://www.legislation.gov.uk/ukpga/2004/31/contents **Retrieved 11/01/2011**

[15] BBC News, Huntley guilty of Soham murders, Posted 17/12/2003 http://news.bbc.co.uk/1/hi/uk/3312551.stm **Retrieved 11/01/2011**

[16] Bichard Inquiry, Published 22/6/2004 http://www.bichardinquiry.org.uk/10663/report.pdf **Retrieved 6/01/2011**

[17] Telegraph, Mother and daughter who burned to death: 'no excuses' says Alan Johnson Posted 29th Sept 2009 http://www.telegraph.co.uk/news/uknews/6241791/Mother-and-daughter-who-burned-to-death-no-excuses-says-Alan-Johnson.html **Retrieved 11/02/2011**

[18] Victoria Climbie Inquiry Report Published 3/06/2003 http://www.publications.parliament.uk/pa/cm200203/cmselect/cmhealth/570/570.pdf **Retrieved 10/01/2011**

[19**]** Every Child Matters Published January 2006 http://education.gov.uk/publications/standard/publicationDetail/Page1/DFES-0012-2006 **Retrieved 10/01/2011**

[20] Data Protection Act 1984 http://www.legislation.gov.uk/ukpga/1984/35/contents **Retrieved 5/01/2011**

[21] Access to Personal Files Act 1987 http://www.legislation.gov.uk/ukpga/1987/37/contents **Retrieved 5/01/2011**

[22] European Directive of 1995 http://en.wikipedia.org/wiki/Data_Protection_Directive **Retrieved 5/01/2011**

[23]Data Protection Good Practice Note Releasing information to prevent or detect crime http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/section_29_gpn_v1.pdf **Retrieved 10/01/2011**

[24] ICO Data Sharing Code of Practice Published October 2010 http://www.ico.gov.uk/about_us/consultations/our_consultations.aspx **Retrieved 28/10/2010**

[25] Data Protection Act 1998 Section 29 http://www.legislation.gov.uk/ukpga/1998/29/contents **Retrieved 5/01/2011**

[26] Loughborough University, Section 10: Disclosures to the Police and Legal Proceedings http://www.lboro.ac.uk/admin/ar/policy/dpact/disclosure/index.htm#sec10 **Retrieved 11/02/2011**

[27] Kirklees NHS, Data Protection – Prevention & Detection of Crime, Posted 05/2007 http://www.kirklees.nhs.uk/uploads/tx_galileodocuments/Disclosing_Information_to_Police_and_Others_Investigating_a_Crime.pdf **Retrieved 11/02/2011**

[28] Crime and Disorder Act 1998 http://www.legislation.gov.uk/ukpga/1998/37/contents **Retrieved 07/01/2011**

[29]The Childrens Act Report http://www.dcsf.gov.uk/childrenactreport/ **Retrieved 14/01/2011**

[30] MOPI (Management of Police Information) http://www.npia.police.uk/en/15088.htm **Retrieved 14/01/2011**

[31] NHS Information Standard http://www.isb.nhs.uk/ **Retrieved 14/01/2011**

[32] ICO (Information Commissioners Office) 1000 data breaches reported to the ICO Posted 28/05/2010 http://www.ico.gov.uk/~/media/documents/pressreleases/2010/1000_DATA_BREACHES280510.ashx **Retrieved 05/01/2011**

[33]Information Commissioner's Office demystifies data protection Published 26/11/2009 http://www.ico.gov.uk/~/media/documents/pressreleases/2009/GUIDE_TO_DP_261109FINAL.ashx **Retrieved 12/01/2011**

[34] ICO First monetary penalties served for serious data protection breaches Published 24 November 2010 http://www.ico.gov.uk/~/media/documents/pressreleases/2010/first_monetary_penalties_press_release_24112010.ashx **Retrieved 06/01/2011**

[35] Guardian, Lost in the post - 25 million at risk after data discs go missing Posted Wednesday 21 November 2007 http://www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.economy3 **Retrieved 11/02/2011**

[36] Telegraph Government's record year of data loss Posted 6th January 2008 http://www.telegraph.co.uk/news/newstopics/politics/1574687/Governments-record-year-of-data-loss.html **Retrieved 11/02/2011**

[37] Telegraph Thousands of NHS medical records lost Posted 25 May 2009 **http://www.telegraph.co.uk/health/healthnews/5381605/Thousands-of-NHS-medical-records-lost.html** **Retrieved 11/02/2011**

[38]Wikipedia Generation Z http://en.wikipedia.org/wiki/Generation_Z#Beyond_Z **Retrieved 11/01/2011**

[39] Pingdom Study: Ages of Social Network Users Posted 16/02/2010 http://royal.pingdom.com/2010/02/16/study-ages-of-social-network-users/

Retrieved 11/02/2011

[40]Pew Internet, Older Adults and Social Media Posted 27/09/2010
http://www.pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx **Retrieved 19/01/2011**

[41]The Times, After 17 months of unimaginable cruelty, Baby P finally succumbed, Posted 12 November 2008
http://www.timesonline.co.uk/tol/news/uk/crime/article5140511.ece **Retrieved 11/02/2011**

[42] ICO Consultation on the first ever UK code of practice on data sharing launched Published 8th October 2010
http://www.ico.gov.uk/~/media/documents/pressreleases/2010/Data_sharing_consultation_press_release_07102010.ashx **Retrieved 16/10/2010**

Appendix A: Royal Pingdom Social Networking Statistics

http://royal.pingdom.com/2010/02/16/study-ages-of-social-network-users/
Posted February 16th 2010

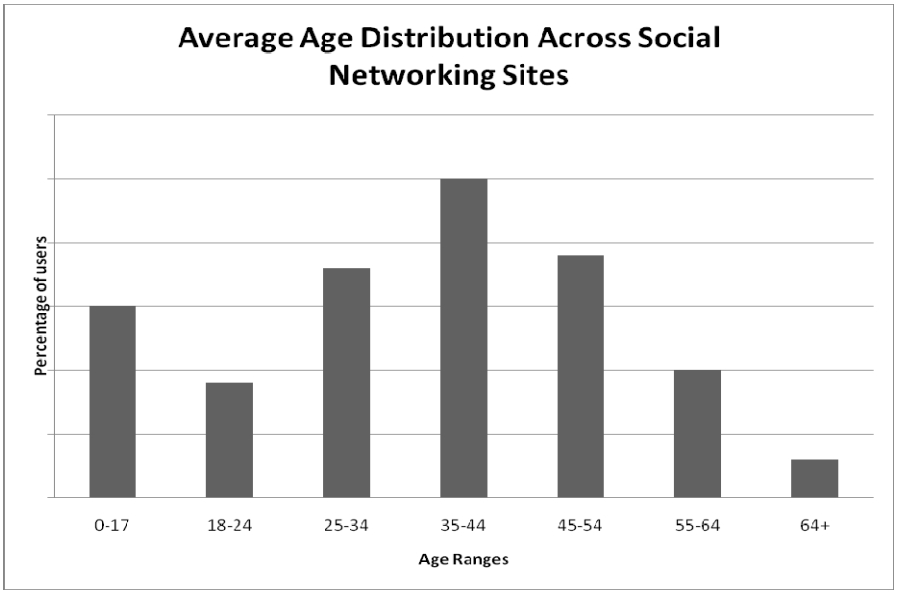


Figure 4 adapted from royal pingdom website

Some facts on age distribution on social network sites:

- **The average social network user** is 37 years old.
- **LinkedIn**, with its business focus, has a predictably high average user age; 44.
- **The average Twitter user** is 39 years old.
- **The average Facebook user** is 38 years old.
- **The average MySpace user** is 31 years old.
- **Bebo** has by far the youngest users, as witnessed earlier, with an average age of 28.