PRAIS - PRivacy impact Analysis for Information Sharing

R Harbird[1], A Finkelstein[1], S Hailes[1], E McKinney[2], R Jeyarajah-Dent[3]

[1]Department of Computer Science
University College London
Gower Street
London WC1E 6BT

[2]LogicaCMG UK Ltd
81 George Street
Edinburgh EH2 3ES

[3]Coram
Coram Community Campus
49 Mecklenburgh Square
London WC1N 2QA

PRAIS - PRivacy impact Analysis for Information Sharing

Keywords: Privacy, multi-agency information sharing

Abstract

Recent government initiatives have actively promoted information sharing for staff working in social care in the delivery of services. Research has shown however that social workers are sometimes reticent to share or may share information inappropriately despite the availability of guidelines from both government and local authorities. There are no computer-based tools in general use to support practitioners in resolving the issues they are confronted with in deciding when to share, what to share and with whom to share information. To address this deficiency, we are undertaking research intended to clarify the requirements for a privacy mediation tool which will ensure that information sharing conforms to legal requirements, fair information processing principles and the conditions set out in local data sharing agreements. The rationale and high-level design of our privacy impact analysis software are presented in this paper.

Information Sharing in Social Care

UK governments are promoting multi-agency information sharing as a key component of new work practices for those providing services to children and families. In support of this activity governments have produced best practice guidelines[1] and most local authorities have developed their own data sharing agreements and manuals. Despite the amount of information available, staff do not always feel confident to share what they know. The need to communicate seems straightforward until you consider that at least seventeen different documents on information sharing have been produced by the UK Government since 2002[2]. Further problems are reported

around the effectiveness of the communications[3]. Where there are no child protection issues and sharing is not mandated, there have been several instances where sharing has been performed without due diligence or reference to codes of ethics or good practice[4]. It is clear that the process of information sharing in the domain of children's social care is far from clear-cut, and, at the very least, more training and education is needed.

Computer-based information sharing is still fairly limited. Data sets are, or soon will be, made available in large, regional repositories such as ContactPoint in England[5], or via a central hub like the eCare system in Scotland[6] and systems based on the FAME architecture in England[7]. Decisions relating to the privacy protection of individuals have effectively been made during the design phase of the computer software and there are no decision-support tools which aid the practitioner in making complex decisions about whether specific information should be submitted for sharing in a particular context.

Privacy and Personal Information

More generally, information sharing by organisations and government departments facilitated by new computer systems is increasing apace and the widespread use of computer systems to collect, analyse and share personal information has given cause for concern. Technologies offering opportunities for mass surveillance promise improvements and exciting opportunities in areas such as healthcare services and crime prevention but there may be unintended and undesirable consequences. There are risks associated with growing numbers of people having access to large databases particularly in a healthcare context[8] and the length of time that records persist might facilitate profiling or social sorting for undesirable purposes.

Privacy Impact Assessments

The key challenge for engineers is to "design for privacy" from the outset[9] and in recognition of this governments around the world are developing their own variation of the Privacy Impact Assessment (PIA). The main objective of performing a PIA is to gain an understanding of the impact which a new process, system or technology may have upon the personal privacy of individuals. Fundamentally the PIA should ensure that the risks to privacy are mitigated and that data is not inaccurate or out-of-date, excessive or used in unacceptable or unexpected ways beyond the control of data subjects, Table 1, below, contains a summary of key PIA principles [10,11,12,13].

Key PIA Principles	
Accountability	An organisation must appoint someone to ensure that privacy policies and practices are followed. Audit functions must be present to monitor all data accesses and modifications.
Purpose	There must be a clearly specified purpose for the collection and sharing of personal information. Data subjects should be told why their data is being collected and shared at or before the time of collection.
Scope	Only information that is required to fulfil the stated purpose should be collected or shared.
Limiting use, disclosure and retention	Data can only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorised to receive it. Personal data should be aggregated or anonymised wherever possible to limit the potential for computer matching of records.

	Personal information should only be kept as long as is necessary.
Personal information	Treatment of the information must conform to fair information processing practices. Information must be collected directly from the person unless there are very good reasons why this is not possible.
Accuracy	Every effort must be made to ensure that the personal information shared is accurate.
Safeguards	Personal information must be protected from loss or theft. Safeguards must prevent unauthorised access, disclosure, copying, use or modification.
Consent	Data subjects must give their consent to the collection, use and disclosure of their personal information.
Openness	Privacy policies must be made available to clients.
Individual access	Clients have the right to ask to see their personal information and to request the correction of perceived inaccuracies. Clients must be informed about parties with whom it has been shared.
Challenging compliance	Clients must be able to challenge an agency's privacy processes.

Table 1 - PIA Principles

All these elements are essential but the PIA process is not directly applicable to the situation where a practitioner needs to share information on an ad hoc basis and must consider at least some of these principles as they apply to the specific scenario before acting.

PRAIS

The PRAIS research project involves collaboration between: computer scientists from University College London, child protection experts from Coram and information technology professionals from Logica CMG. The aim of the project is to use PIA principles to guide the vision and development of` a dynamic decision support tool known as PRAIS, so called because it provides PRivacy impact Analysis for Information Sharing.

PRAIS will provide a policy-driven privacy framework which will assist practitioners in making information sharing decisions with an awareness of the privacy implications. In the short-term the goal of the project is to produce a prototype which can be used for further requirements analysis with partners in local authorities. In the longer term our vision is broader: PRAIS will also be used as a training tool to help professionals learn experientially about the issues in managing personal information. PRAIS will help both policy makers and decision makers to address, not only the legal, but the moral and ethical issues involved with information sharing. PRAIS will improve the timeliness and the quality of data sharing and help staff to manage the negative impacts of information sharing where these occur. The target user group is staff based in children's social services departments but the design has a wider application and could be used in other areas where professionals have to share personal information even where this takes place across legal jurisdictions. PRAIS encapsulates fair information processing principles and, as such, will help a wide spectrum of organisations to deal with managing users' consent and the needs and requests of information subjects.

User scenario

The information sharing process is illustrated in the user scenario diagram below; PRAIS sits between the practitioner and the social care data store and mediates all information sharing actions. PRAIS is based on the architecture developed for the Identity Governance Framework[14]

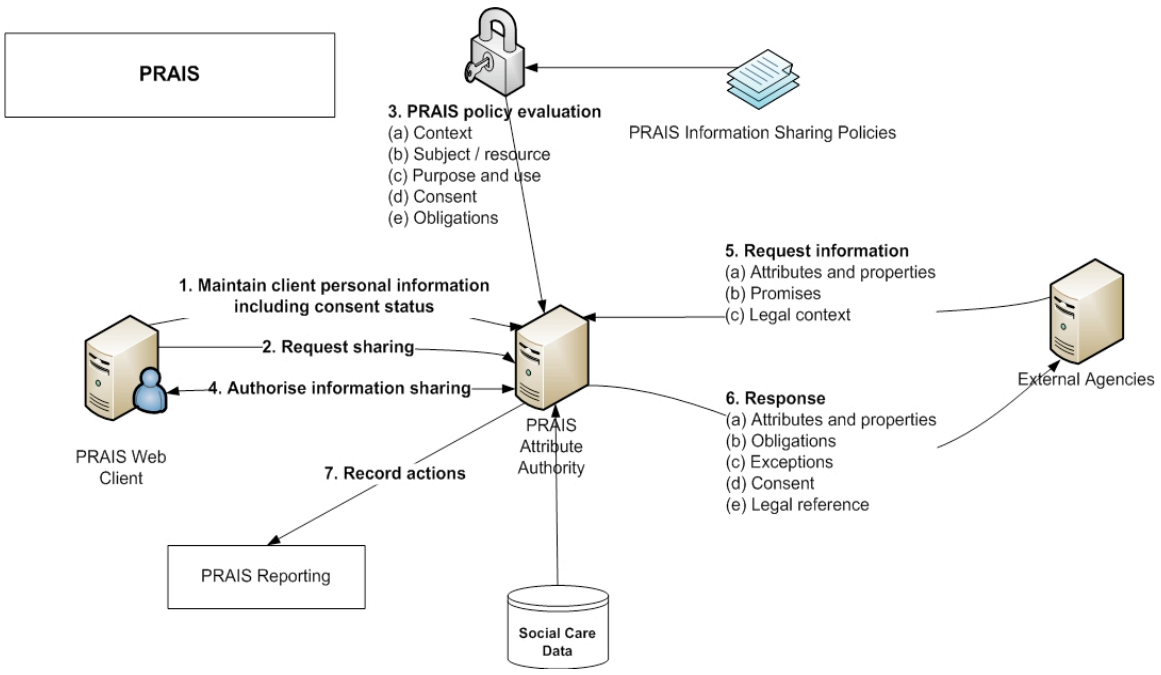

Figure 1 User scenario diagram

1. The practitioner uses the computer system to create and maintain all personal information about clients and their consent status.
2. Using PRAIS, a practitioner requests information sharing with an external agency for a specific purpose.
3. PRAIS evaluates the practitioner's request. First it retrieves the policy associated with the information sharing purpose and evaluates the rules associated with it. The rules may cover:

   a. Context - PRAIS will evaluate whether the intended recipients are permitted to receive information about the client for the purpose specified.
   b. Resources – what data may be shared? Is it accurate and up-to-date?
   c. Consent - has consent been obtained from the data subject for the purpose specified?
   d. Obligations – these are the rules which receiving parties must obey, e.g., data may not be propagated further by the receiver.
4. PRAIS presents the user with the information that may be shared and the practitioner accepts or rejects the sharing decision. If information sharing is authorised then the system sends the intended recipients a message indicating that they may retrieve data.
5. In due course the target agencies request the shared information, stating:
   a. The attributes to be retrieved,
   b. The promises made with respect to the data, e.g., recipients may undertake not to propagate the information further.
   c. The legal context within which the information is requested.
6. The PRAIS system responds with:
   a. A set of attributes and their properties.
   b. Exceptions: some of the attributes requested may be unavailable.
   c. Obligations.
   d. Consent status, the information may have been shared with or without the owners consent depending upon the reason for sharing information.
   e. Legal references to legislation relating to the data.
7. Every PRAIS transaction is logged. The system can be configured to notify staff with responsibility for monitoring information sharing with alarms and exceptions.

Information sharing is based on a “pull” model; this means that the recipients are alerted that information is being made available to them after which it is retrieved from the source. At first this

may seem counterintuitive but this design choice has been made because it allows the owner of the information to retain liability for the data and to audit each use.

Future Work

The next step for the PRAIS project is to refine and develop further specific information sharing scenarios with our partners in social care. This will enable us to experiment with expressing and interpreting policies using a policy language and policy evaluation engine. As a starting point we will investigate the applicability of recent work in policy-based security management in the healthcare domain [15,16] which bears certain similarities in terms of the strict security requirements with respect to personal data.

In the longer term, PRAIS must be supported by a set of subsidiary security-related capabilities, these are:

1. Identity management functions for authentication and authorisation of both practitioners and external agencies.
2. Privacy policy management functions to support policy authoring and policy compliance management.
3. A common data model for social care. A widely accepted Electronic Social Care Record (ESRC) is needed to support information sharing facilitating electronic data sharing agreements which are at least part-validated by machine.
4. Data matching and mapping functions. Information transfer between organisations with heterogeneous information sources may imply the need for data matching and mapping so that that records and fields can be linked without the need for common identifiers or a common schema.
5. Data anonymisation, obfuscation and aggregation. The user scenario in this paper depicts a situation where one record is or a small number of records are shared. Agencies

must also provide statistical information to government bodies and in the future data records may be used en masse for research purposes. Before this can happen, data must be "cleansed" to remove personal identifying attributes. We envisage that PRAIS will be supported by software which will de-personalise data on-the-fly, using techniques depending upon the query submitted and the number of data records returned.

6. Information life-cycle management. Organisations have responsibility for managing the data they collect securely and this includes disposing of data once it has served its intended purpose. Tools to assist with automatic information housekeeping are a necessary part of the privacy toolbox.

Conclusion

Much of the information sharing in social care can be described as ad hoc and workers are expected to interpret written guidance to ensure that proper care is taken with personal information. It is our belief that the privacy implications of sharing can be at least partially evaluated by computer. The aim of the PRAIS project is to develop a prototype for a policy-based tool which can analyse information sharing decisions on-demand. To date we have developed an innovative high-level architecture and our next step is to implement a set of representative scenarios using a policy engine to demonstrate the feasibility of the PRAIS vision. This initial work should be seen in context as part of a much broader picture in which PRAIS will form an integral part of the day-to-day business process of information sharing. Eventually, PRAIS will operate as part of a risk assessment framework evaluating the predictability of particular sharing outcomes using mechanisms which are generic yet flexible enough to be applied to a wide range of industry sectors such as finance, education and healthcare.

References

[1] Department for Education and Skills. Information Sharing: Practitioners' Guide. HM Government; 2006. Available from: http://www.ecm.gov.uk/_files/ACB1BA35C20D4C42A1FE6F9133A7C614.pdf.

[2] Richardson S, Asthana S. Inter-agency Information Sharing in Health and Social Care Services: The Role of Professional Culture. British Journal of Social Work. 2006 Jun;36:657–669. Available from: http://bjsw.oxfordjournals.org/cgi/citmgr?gca=bjsw;36/4/657.

[3] Munro E. What tools do we need to improve identification of child abuse? Child Abuse Review. 2005 Dec;14:374–388. Available from: http://www3.interscience.wiley.com/cgi-bin/abstract/112220785/ABSTRACT?CRETRY=1&SRETRY=0.

[4] Anderson R, Brown I, Clayton R, Dowty T, Korff D, Munro E. Children's Databases - Safety and Privacy. Wilmslow: Information Commissioner's Office; 2006. Available from: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fipr%20report.pdf.

[5] Department for Children Schools and Families. ContactPoint; 2007. Available from: http://www.everychildmatters.gov.uk/deliveringservices/contactpoint/.

[6] Scottish Executive Data Sharing and Standards Division. eCare; 2005. Available from: http://www.scotland.gov.uk/Resource/Doc/923/0019775.ppt.

[7] Morrison K. FAME - The Key to Multi-Agency Working. eGov monitor. 2004; Available from: http://www.egovmonitor.com/features/fame.html.

[8] Anderson R. Healthcare IT in Europe and North America; 2005. Available from: http://www.cl.cam.ac.uk/~rja14/Papers/nao-report-final.doc.

[9] Royal Academy of Engineering. Road User Charging, A Statement by the Royal Academy of Engineering; 2006. Available from: http://www.raeng.org.uk/policy/reports/pdf/road_user_charge/road_user_charging.pdf.

[10] 6 P, Birch A, Copping M, Raab C. Information Sharing for Children at Risk: Impacts on Privacy, E-Care Programme. Scottish Executive Health Department.

[11] Clarke R. Xamax Consultancy - PIA Guideines; 1999. Available from: http://www.xamax.com.au/DV/PIA.html.

[12] Office of the Privacy Commissioner of Canada. Fact Sheet: Privacy Impact Assessments; February 2007. Available from: http://www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp.

[13] Information Commissioner's Office. Framework Code of Practice for Sharing Personal Information; 2007. Available from: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf.

[14] Liberty Alliance Project. Identity Governance; 2007. Available from: http://www.projectliberty.org/liberty/strategic_initiatives/identity_governance.

[15] Agrawal R, Grandison T, Johnson C, Kiernan J. Enabling the 21st century health care information technology revolution. Communications of the ACM. 2007;50:34–42.

[16] Eyers DM, Bacon J, Moody K. OASIS role-based access control for electronic health records. Software, IEE Proceedings. 2006;153:16–23.