

Privacy with Tracking Devices used in Health related applications

A discussion paper by:

Dr Peter R Croll

Chair of HIPS, HISA Privacy in Health Forum

Director, Health Informatics Society of Australia (HISA Ltd.)

Owner, Better Life ICT (www.blict.com)

Technology now presents a range of electronic devices that allow for tracking the location of people or objects. Some devices are only receptive, i.e. they can inform a user as to their current location but not transmit that information to others. An example of a receptive only device would be a personal GPS, frequently now used for street navigation in vehicles. Some devices transmit information allowing their location or identity to be determined by others. This can be either when they are in close range of a particular location, as with RFID chips, or more remotely when they have longer range communication capability, e.g. a mobile phone connected to a GSM cellular network.

With receptive only devices there can be some privacy concerns. For example, consider a vehicle with GPS system that stores in its memory a history of the locations visited and that information was readily obtainable by the service station or the manufacturer without the user's knowledge. Although this may occur, concerns over privacy violations are more acute with devices that can transmit data.

Any device that has the capability to transmit information that can be used to track the whereabouts of an object or person needs special consideration. There is much greater potential for this information to be intercepted without the user knowing and by a wider range of people. This information may only contain an identity reference number but if it can be readily linked to an individual then the Australian Commonwealth Privacy Laws 1988 will apply. Furthermore, if the information is considered to be of a sensitive nature, such as a person's medical condition, then further more stringent Federal and State laws may also apply.

There are a number of new technology applications where privacy concerns may be raised. For example, a person with dementia can cause harm to themselves if allowed to travel freely without the knowledge of their carer. Providing them with a transmitting tracking device can alert a call centre when they roam too far from home. If necessary, an accurate and most recent location reference can be given to their carer to help assist in finding them. Others at risk, like children and lone workers can also benefit from such safety alerts. The key issue is whether they have given their consent to be tracked and if other people who they may not be aware of are also tracking them.

There are a growing number of applications that involve the tracking of objects that can be related back to an individual. These include using RFIDs to track everyday objects such as items purchased from shops. Normally, they are only required at point of sale for item identification or at the shop exits for security purposes yet after leaving the store they can remain active and can be tracked by receivers in other locations. Furthermore, it should be noted that a customer may have identified themselves to the shop through their bank card or their shop loyalty cards. This can provide for a

unique reference from an item to the person carrying it. This is an area of active concern for the government which is now considering the proposed review of the current Privacy laws.

More recently there has been a move towards tracking medical related objects. This might include blood, tissue/bone samples or an individual's medicines. RFID chips are now cheap enough to assign to these items. With the more expensive items it is now cost effective to use 'active' RFID devices that can be programmed to store a lot more information than a unique identity number. With such medical items it is a frequent requirement to ensure that, when necessary, an identifiable link to the correct individual concerned can be established.

In recognition of the need to incorporate the advances in technology the federal Privacy Laws are under currently under review. The proposals will be first tabled in parliament in 2008 but such complex legislation is unlikely to be passed in law until 2009/10 or later. The Health Privacy related legislation may take even longer. The proposal is that much of the health related issues would be handled by the introduction of "Privacy (Health Information) Regulations" to be established by the Privacy Commissioner. Hence, conformance to the current laws is needed for the foreseeable future.

To help organisation determine if they are sufficiently compliant with current privacy legislation, the Australian government provides guidelines for undertaking what is known as a Privacy Impact Assessment (PIA).

Privacy Impact Assessments (PIA):

A PIA is a tool that can help determine if an organisation or agents are following their vision and values, can reduce the risk of not meeting their contractual and legal obligations and improve their position when, for example, tendering for new contracts. The Australian guidelines describe the PIA process as story being told about a project that will identify privacy impacts and lead onto management recommendations. The guidelines state:

"A PIA is an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals – it 'tells the story' of the project from a privacy perspective. The purpose of doing a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts." [PIA 2006]

The emphasis is on identifying when an organisation or government agency is collecting information that is unnecessary for the given project or whether the project will lack appropriate accountability or oversight processes. The aim is to identify, analyse and manage privacy impacts and seek out solutions that drive good privacy practice and underpin good public policy while still achieving the project's goals.

The key stages of the Australian PIA and the complexity of Health related information:

The starting point of a PIA is to broadly describe the project and then map out the 'information flows' of any personal information across an organisation. It should be noted that this is not health information specific. A PIA can, and should, be applied to any project that involves any personal information. In health there are some further concerns resulting from the highly sensitive nature of clinical information. In fact just having your registration details located at a particular healthcare

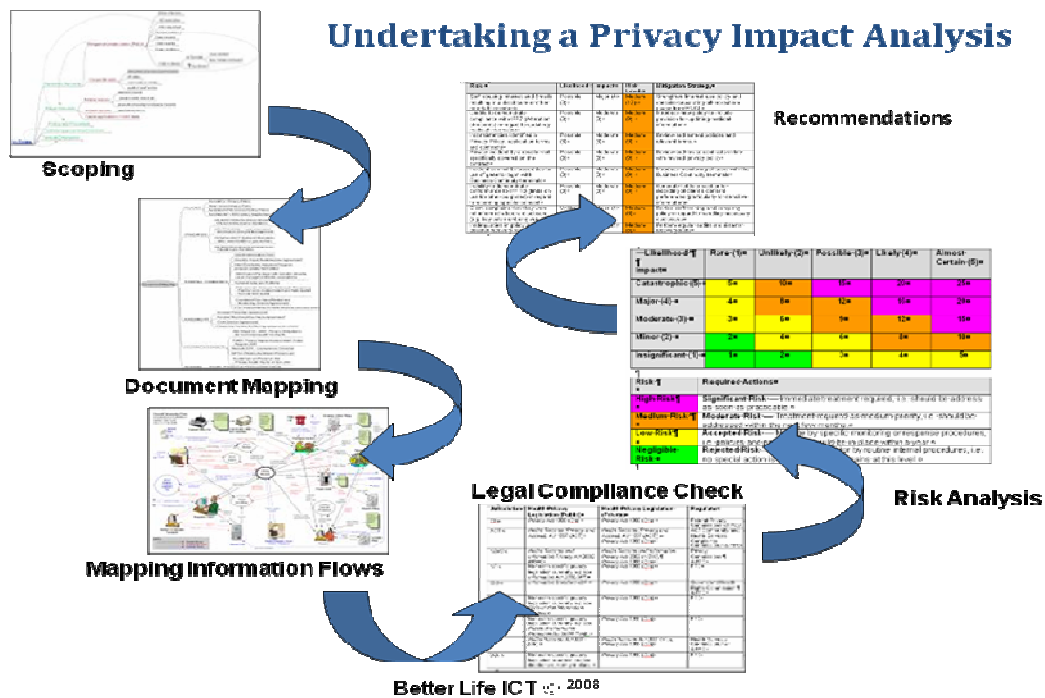
provider might constitute sensitive information, e.g. mental and sexual health practices. Therefore any mapping should consider all personal information before looking at the sensitivity risks.

The Australian PIA guidelines provide a check list to determine compliance with each of the Privacy Principals, i.e. either the 11 Information Privacy Principals (IPPs) and/or the 10 National Privacy Principals (NPPs). This is a bit more complex with Health data since the Australian Privacy laws can differ depending on whether we are considering private or public healthcare providers and then which State they reside in. Further complexities occur with the use of this data when it crosses borders and jurisdictions and if it will have a secondary use for medical and public health research. This topic is too complex to be adequately addressed in this discussion paper, for further details please refer to [Liu 2008, Magnusson 2004, ALRC 2007 and Croll 2006-8].

By using the checklist supplied in the PIA guidelines and mapping an information flow mapping it is possible to determine the main privacy risk impacts and draw up recommendations for management. In practice this can be a non-trivial task when dealing with complex organisations that have evolved their privacy principals over time and are driven by different motives to that of the community and the individuals they hold information on.

An independent analysis is the best way to determine the actual working practices within an organisation. It is also critical to get an external insight on the 'perceived risks' and a measure on how best to handle them as these can have a direct negative effect on the attitude and behaviour of your customers and clients.

The following diagram indicates the stages involved:



Outcome:

The Australian PIA guidelines state a number of key benefits can arise from undertaking a PIA. In brief these include: avoiding costly or embarrassing privacy mistakes; compliance with privacy laws; reflecting community values; avoiding function creep relating to privacy; future proof against known upcoming privacy law changes; ensuring stakeholders and the community are better informed; demonstrating that protecting personal information is important to the organisation concerned and that this has been critically evaluated.

Dr Croll's direct experience at undertaking PIA's with international organisations has led to the development of a set of software tools that streamline the process specifically for health related applications.

Contact his team at anytime for a free professional assessment of your needs:

Email: peter@blict.com

Phone: 0458 625 428 (045 TO BLICT)

References:

[ALRC 2007] "Review of the Australian Privacy Law", Discussion paper 72, Australian Law Reform Commission (www.alrc.gov.au), Sept 2007.

[Croll 2006a] PR Croll, Are undue Privacy concerns putting our Health Research at high risk? Privacy Law Bulletin, LexisNexis Butterworths, vol. 2, no.10, April 2006, pp139-140.

[Croll 2006b] PR Croll & J Croll, Privacy Compliance – Managing the Risks when Integrating Health Data, Health Informatics Conference Sydney, Aug. HIC 2006.

[Croll 2008a] PR Croll, Special Issue: Health Information Privacy and Security, electronic Journal of Health Informatics www.eJHI.net, Vol 3, No 1 (2008).

[Croll 2008b] PR Croll, Privacy Impact Assessments – the Organisation versus the Individual's viewpoints, Health Informatics Conference HIC'08, Melbourne 2008.

[Liu 2008] V. Liu, L. May, W. Caelli, PR. Croll, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis, electronic Journal of Health Informatics, 2008; 3(1): e3.

[Magnusson 2004] Roger Magnusson, 'The changing legal and conceptual shape of health care privacy' (2004) 32 Journal of Law, Medicine & Ethics 680-691.

[PIA 2006] Privacy Impact Assessment, Australian Gov., Office Privacy Commissioner (www.privacy.gov.au), Aug 2006.