PRIVACY AND HUMAN RESEARCH – commonsense and common foundations

2011 ANNUAL GOLD COAST HUMAN RESEARCH ETHICS COMMITTEE FORUM
17 February 2011

LINDA MATTHEWS
QUEENSLAND PRIVACY COMMISSIONER

J. Robert Oppenheimer, the so-called 'father of the Atom Bomb', once described the process behind its creation as being little more than the practical application of theoretical physics; he said:

> *"When you see something that is technically sweet, you go ahead and do it and you argue about what to do about it only after you have had your technical success. That is the way it was with the atomic bomb."*

The morality of the Manhattan Project, the ethical implications of creating what Oppenheimer was later to describe as 'the destroyer of worlds' were, at the time, no more than an afterthought.

Today, consideration of ethical dimensions is built into the design, review and conduct of research on many levels. This is particularly so in the area of 'human research'. Everyone here would be familiar with the *Australian Code for the Responsible Conduct of Research* was jointly issued by the National Health and Medical Research Council, the Australian Research Council and Universities Australia and its companion publication, *the National Statement on Ethical Conduct in Human Research*.

So I am not going to talk to you about the content of these documents. I am going to talk about how Queensland's relatively new privacy legislation – the *Information Privacy Act 2009* or, as it is known, the IP Act, may impact on the conduct of human research.

I have two key messages:

- First – privacy need not be a hindrance to researchers – I will explain why.
- Second – we want to collaborate to find workable solutions if problems do arise. One example is the 2010 Review of TransLink's disclosure of go card information to the Queensland Police Service.

Some of you may be familiar with the Commonwealth Privacy Act and its privacy principles. Our Queensland legislation has similar principles but the application of them has some slight variance.

Privacy is mentioned – several times – in both the Code and the Statement. But, while these documents note that privacy is an important consideration in research, they are largely silent on how privacy protection can be achieved.

Privacy is defined in the Statement as 'the domain within which individuals and groups are entitled to be free from the scrutiny of others'. Its context is 'human research' which in itself *is* intimate scrutiny of individuals and groups.

Some may say that being free from scrutiny and being the subject of research are mutually opposed goals. I think that it is realistic to acknowledge that there is some tension between respecting the right of persons to keep their information 'private' and obtaining that information for the purposes of research. The task is to work out a balance which delivers on both, and the IP Act can assist. It provides for the *responsible* use of personal information. It is a pragmatic mixture of protection and licence.

Jurisdiction

Let's start at the beginning. Why should what the IP Act says impact on you as a human researcher?

It goes without saying that if you research in Queensland, there's a better than even chance you are subject to Queensland law. The IP Act covers all operations of Queensland Health – there are nine National Privacy Principles applying to that agency. The IP Act covers all Queensland Universities – except Bond University.

If you are with the private sector and your organisation has a turnover of more than $3 million per year, the Commonwealth's privacy act could apply. If you are a private sector organisation and your research is conducted on behalf of Queensland Health, any other State Government agency, or for a University, you may be covered by the IP Act. Even if you are normally covered by the Commonwealth's Act because you are a research organisation that has a multi-million dollar turnover you may still be subject to Queensland's Act.

The Commonwealth legislation has a provision that says if services are being provided to a Queensland State entity the Commonwealth defers to the State and their Act will not apply to that service. This means if you are one of those organisations and you're working with Queensland government you are not covered by any privacy legislation. Even if you fall into this category, you are likely to be caught in another way.

The impetus to bind you to compliance with the IP Act will come from the contracting agency. The IP Act requires the contracting agency to take all reasonable steps to bind their contracted service providers to the privacy obligations in the IP Act. If the contracting agency does not take these 'reasonable steps', it is not only itself in breach of its obligations under the IP Act but, if a privacy issue arises out of

the research, the liability for it falls back onto the contracting agency. They will bind you for the simple expedience of protecting themselves.

The application of privacy principles to human research

How are the privacy principles likely to impact on your research? Two core privacy principles are: obtain only the information necessary to fulfil a purpose and ensure that *all* the information sought is relevant to that purpose. If you don't need the person's family history for the research, don't delve there. Collecting information just in case it might be relevant is bad for privacy and potentially bad for research; extra information must be stored, managed, organised and protected and if you don't need it, don't waste the resources.

When you obtain information from an individual, tell them what your purpose is in obtaining it, tell them what will happen to it from here, tell them who else will access it and who they in turn may provide it to. People want to know what is going on with their information and they want to know where it ends up.

You need to safeguard their information. Personal information is an increasingly valuable commodity. Whole industries – legitimate and criminal – are making huge amounts of money from dealing with personal information. More money than is available to any humble researcher. An example of the former is Facebook. Nobody really knows how much Facebook is worth, but the most recent estimate puts it at $US50 billion. Facebook doesn't actually make anything. All Facebook does is collect and recycle people's information; Facebook is worth a lot of money because its data store can be used to make a lot of money.

An example of the latter is the fastest growing crime in the world – identity theft. On average, most victims of identity theft lose $1000. Which doesn't sound a huge amount–noticeable but not devastating—until you add it all up. Identity theft is a $3.5 billion industry in Australia.

Anywhere there is money to be made people will devise ever more ruthless and inventive ways to make it. No matter how prosaic the information might seem, it is valuable to someone. The participants expect, and the law demands, that their trust is not breached; that their information is not lost, stolen, misappropriated, inappropriately given away or misused. The research organisation is obligated under the privacy principles to protect data from these risks; it should be kept securely and accessed on a needs basis only.

Queensland's IP Act is kind to researchers, far kinder than the administrative standard in place before July 2009. While I was preparing this presentation one of

my staff told me about a task she was given when she worked for another agency: facilitating the movement of personal information to a researcher, which involved shepherding it through four different agencies. I obviously can't discuss specifics, but it was significant research into a large portion of the population, with the potential for extremely beneficial results. Because this information was about people, it couldn't just be given to the researcher. No, it had to be deidentified, passed through multiple hands, random numbers assigned and matched with other random numbers, reidentified, deidentified, and passed from agency to agency, vetted by multiple senior officers and privacy officers, until finally a dossier containing all the information needed by the researcher was compiled. She estimates it took eight months by the time the whole thing was finished and passed through close to a hundred hands. There was no kindness available for that researcher, and he could have been forgiven had he gotten sick of the whole thing and found something to work on which involved less red tape.

The IP Act's kindness manifests itself in two ways:

- permitting the use of personal information by the organisation to conduct research, and
- permitting its provision to persons outside the organisation so they can conduct research; notably, this includes the publication of the outcomes of the research.

It is a fundamental privacy tenet that an organisation can use personal information for the purpose for which it was obtained. This is called ‘primary use’ and it underpins modern commerce. But researchers have an additional dispensation. The privacy principles permit a research organisation to use information for a secondary purpose. That is, to use information that was obtained for one purpose for another purpose entirely.

However, the secondary use is not unrestricted. There is fine print. There are conditions. But they are not onerous. The secondary use must be necessary for research that is in the public interest. If the use involves publication, the information must be de-identified. Again, this is not difficult to do when dealing with groups of individuals. Lastly, it must not be practicable to go back to the individuals concerned and obtain their agreement. There are many reasons why going back to the individuals concerned is not practicable: the data may be old and the people involved now have different contacts; there are too many people involved and contacting them would be an onerous use of resources. The criterion will be easy to satisfy as long as the justification is appropriately reasoned.

There is similar latitude with disclosure. Disclosure is information passing outside of an organisation. Ostensibly, an individual’s personal information should not be given out to anyone other than the individual themselves. So where does this leave the researcher? In a very good position, because the IP Act allows information to be disclosed if the disclosure is necessary for research in the public interest. Subject to

the same simple and commonsense provisos as secondary use, the researcher could simply be given the information without jumping through multiple hoops.

It is important to remember that privacy has a relatively narrow application. Privacy is all about personal information. No personal information, no privacy issues. This category of information is both broad and narrow. It is broad because any information, true, false, fact, opinion, interesting or banal about a person is their personal information. It is narrow in that only individual persons have personal information; governments, organisations, corporations, businesses are not individuals and therefore do not have personal information. The deceased are regarded by the IP Act as in a different category from the living; they, too, have no personal information.

Now, that distinction is not much use in the area of human research. But another qualification is: in order for a person's information to qualify as personal information, the person must be identifiable. There must be some identifying characteristic associated with the information. That could be a name, a work or other title, a person's photograph, their recorded voice or any other means that the person could be identified.

In the absence of identifying characteristics, there are no privacy issues. There are, accordingly, no privacy issues with de-identified or aggregated data.

An example:

The press reported some concerns late last year when person(s) were writing down number plate details from cars at various train stations. I wrote to the agency seeking information and found out that they were surveying where people were living and comparing it to the train station usage in order to plan for future car park expansions. Useful, but a potential breach of privacy in that the agency (a private company contracted to government) was matching number plates with details from the Transport database. In this case, however, there wasn't a privacy breach because the Transport department only gave out postcode information, not names or addresses.

Agreement

There are further 'flexibilities' within the privacy principles in terms of secondary use and disclosure. You can always ask the participant if they agree to the secondary use or to the disclosure. Obtaining agreement is one of the more solid permissions available.

The agreement does not even need to be express. It can be implied. I would caution you to not rush to use implied agreement. It is a fragile permission. The test to be applied is 'if I were to ask this person whether or not they would agree to this, they would always say – yes, of course'.

Such a situation could arise where the technological restraints at the time of the initial research meant there were limits to the analysis of the data. Today the tools are more sophisticated, allowing a deeper, more valuable, level of analysis to occur. One can mount an argument that if these tools had existed at the time of the initial research, the participant would have agreed to their use. This may be an example of where the participant gives their implied agreement to the new analysis.

Waivers

The IP Act recognises that in some limited circumstances, there is a greater public interest in not complying with the obligations in the privacy principles. In common with some privacy regimes there is the capacity for an approval to be given that waives or modifies an agency's obligation to comply with the privacy principles. If I am satisfied that the public interest balance falls in favour of non-compliance I am empowered to issue an approval which has the force of law. The waiver or modification can be temporary or long term, have a blanket application or be tightly focussed.

I have yet to have an agency apply for a waiver or modification but one that has a strong public interest component is in its early stages of development. I do not anticipate that this authority will be called upon overly but it remains an option of practical resort.

Genetic Research

Now I'm going to briefly touch on addressing privacy issues in genetic research. I won't go into it in too much detail because I am starting to run out of time and this area is a whole series of discussions in itself.

What is particularly interesting about genetic research is that it not only reveals information about who a person is or even who that person's blood relatives are, it can also reveal who the person may be – will they have a predisposition for disease or other medical condition. For many persons this last information will be something that the person themselves does not know.

Perhaps of all of the areas of human research, genetic information is of interest to the widest range of persons and entities. The individual wants the information, family members, past and even future, want the information. Law enforcement agencies want the information, the insurance industry definitely wants it, as would healthcare providers and other marketers. Even those officers in the government formulating long term strategies for the health system would like the information.

And of course, for those who have seen the movie '*Gattaca*': soon enough, career advisers will want access to the information.

Given the value of the information and the number of entities with an interest in it, it becomes even more important that the individual has control over the use and disclosure of the information.

As mentioned, genetic information also can go beyond the *individual* and be applicable to other members of the individual's genetic family. In this respect, it is not information that is unique to an individual but rather, it falls into a category of information we call 'mutual personal information'. This is a tricky category to deal with because of the difficult questions of 'to whom does this information pertain' and who has a say about its disclosure.

The best way to deal with this category of information is to have the conditions setting out its potential disclosure to other family members clearly outlined at the beginning of the research project. In many cases this will not be a contentious issue. In the majority of cases, most individuals will want genetic information to be made available to their family members.

In cases where the individual may be working against their family's best interests, the privacy principles have again provided a measure of necessary flexibility. There is an exemption in the IP Act (Information Privacy Principles 10 and 11) that secondary use or disclosure can occur where it is necessary to lessen or prevent a serious threat to the life health safety or welfare of any individual or to the public generally.

This is a proportionate test. There has to be a necessity element and the threat has to be serious but unlike the previous definition in the Information Standards, the threat does not have to be imminent – it can apply to a potential threat. The information does not have to a complete response to the threat; it is sufficient that it merely modify its impact.

A recent NZ case illustrates this point. A doctor, Robert Henderson, saw a woman as a patient and he suspected that she was a current drug user. Dr Henderson, after sitting on his suspicions for three days, decided informed the woman's employer, a residential care facility, of his suspicions. The woman was understandably not happy about her employer having this information and complained that Dr Henderson had breached her privacy. The woman's privacy complaint was upheld in the first instance.

Dr Henderson appealed to the NZ Human Rights Review Tribunal who found that he had not breached the woman's privacy because they considered he had reasonable grounds to believe the woman posed a threat to the residents of the facility.

Summary

I'll end by summarising the main point of my presentation here today. During my time as Privacy Commissioner, I have found it to be a common perception that privacy is an administrative hurdle to a project's outcome – that is both overly restricts methodology and/or adds an unnecessary bureaucratic burden. That privacy is all red tape with no upsides. One Regional Council Mayor has recently described privacy as 'a noose around our necks'.

Perhaps not unsurprisingly, I would not agree with this perception. Moreover, I would argue that in the area of human research the view that privacy is a hurdle is a misconception for two reasons. Firstly, privacy and the ethics of human research share common foundations. Ethical conduct in human research demands respect and concern for the participants. The core ethos of privacy is agencies must treat individual's personal information and by implication, the person themselves with respect. People are not just featureless inputs in government programs – they are the reason for government. Privacy reminds us all not to leave people out of the pictures.

As with ethical conduct, we do not respect privacy because we obliged to do so, we respect it because it is the right thing to do.

Secondly, privacy likes research. There is a raft of permissions built into the privacy principles - some general and some specific to research – to permit flexibility of approach. There are limits; you cannot deliver privacy protection without having some checks and balances but there is enough 'wiggle room' in the principles to permit business to be done. When you look at them closely, what Information Privacy Principles 10 and 11 consist of are little more than lists of exemptions for secondary use and disclosure.

It is also true that privacy considerations need to be built into a research project from its onset and there is work involved in this but that is nothing more than another consideration in a plethora of factors that have to planned, designed and implemented in any research program.

I'll end it there. Thank you for inviting me to speak to you on this topic. If you need or want to follow up on anything I have touched on here in more detail please do not hesitate to call us at our work. My office is a resource for all Queenslanders and we are more than happy to talk anyone through privacy issues.