Australian Law Reform Commission
GPO Box 3708
SYDNEY, NSW 2001
Australia

Serious Invasions of Privacy

Dear Commissioners,

Question 1: I have contributed to previous *Privacy* inquiries, and the thing I note is how little the questions have changed, but how much privacy itself has been circumscribed by government and the private sector alike.

I stand by all the recommendations I made to you during your 2006 investigation, here included as Appendix 1. A theme which should clearly come through in your eventual *Report* is that all levels of government and their agencies are the greatest offenders when it comes to people having their privacy invaded. As someone with a disability, one is keenly aware of just how much personal information public authorities can demand of you by law.

This concern stood behind my submission to Father Frank Brennan, where one railed against government written and legislated human rights. It seemed to be another opportunity for the State to collect data on and control individuals. And as much as I didn't want government defining my rights then (as explained in Appendix 2), I now definitely do not want government defining the extent of my privacy.

Legislation

If legislation is to achieve anything, it should be to reverse the onus of proof. That is, if someone believes their privacy has been invaded, then the duty to prove this is not the case falls on the respondent. With the weight of law against them, this would put due pressure on government agencies and private sector bodies to more astutely justify the collection of information from people, as well as the rationale for maintaining large databases.

Equally, even in taking formal legal action, it is the Crown or a company you pursue in litigation. Generally, the officer or official who took the information from you is shielded behind the veil of the employer-employee relationship. If the legislation readily allowed the lifting of the veil, this would impose greater accountability. While some would argue that is likely to have 'a chilling effect'

on both government and industry, I say, not before time! There are too many agencies (both public and private), collecting too much information, for too many dubious reasons. And, unless those actually collecting the data know liability could potentially reach them *personally*, they will not moderate their behaviour.[1]

Australian governments should not be forcing people and their private, personal details onto online environments. For example, despite all the alleged convenience and cost savings involved, I deplore *Centrelink's* growing insistence (alongside similar moves from other departments) that you use their on-line document management system for communication and compliance purposes. Given what I have learned from friends with knowledge of IT (information technology), as well as from media reports, the notion of a "secure site" is still something that has to be treated with a degree of caution.

A practical example

For many of the same reasons, I will not sign up to the Federal Government's electronic health care record, despite the fact that as someone with complex care needs, I could benefit from the consolidation of my medical records. Unless I control the record, which people have access to it and, any individual or organisation which holds it enters a trustee relationship with me as beneficiary, then this will not be a program for me. The legal relationship of trustee is vital to me having much confidence that the e-health system would be accountable and credible.[2]

---

[1] This principle should apply to officers of public security, intelligent, revenue protection and social welfare agencies. For too long, the refrain of "it's in the public interest" for much of these agencies' work to be carried on in private, has sufficed; apparently so these bodies can "protect" the public.

However, asking more precisely which members of the public are having which interests affected and why, would be a far more compelling and robust test. I am increasingly doubtful that there is a generic (much less universal) public interest. Even if, for argument's sake, you sought to sustain the concept of a general "public interest" in relation to the work of state institutions, this clearly does not apply in relation to private bodies. This is one of the reasons why I have been so concerned about the outsourcing of State social services to the non-government/charitable sector (see my submission to the NSW Public Accounts Committee *Efficiency and Effectiveness of the Audit Office of NSW (Inquiry)* and why one was so pleased to see the Committee recommend in its Final Report that "follow the dollar" legislation be enacted in NSW. This would bring NGOs in receipt of public money within the scope of the Auditor's jurisdiction; a reform which is long overdue in this State.

My concerns regarding government "protection" are outlined in Appendix 2.

[2] The same legal relationship should apply in the case of Internet Service Providers, social media sites, businesses and government agencies alike. If, in their dealings with an individual, what are generated are not records over which they hold copyright but *which are held in trust to the benefit of the individual/source,* then this fundamentally changes the transaction. Most importantly, it rebalances the relationship between government and citizen, as well as between business and customer.

The proposal ultimately coming from the Government was for the Chief Executive of *Medicare* to hold the e-health record, with anyone concerned about a privacy breach being sent through a long and convoluted administrative complaint process, at the end of which stood the Privacy Commissioner. The third document appended alongside this submission, is my submission to the Senate Inquiry into the e-Health Record, where I advise how little I think of the proposal.

Nothing I have heard or read since makes me revise my view of e-health.

E-health is symptomatic of the long-standing "problem" with privacy. Government writes the laws, sets the terms and marks out the parameters of privacy for its own administrative convenience. The public are told our information will be held *confidentially* on porous, data-matching computer systems surrounded by *firewalls* of encrypted code, which officials can only access with *appropriate authorisation.* As for the subject of all this information, it is interesting how we must make formal applications, pay the prescribed fees and produce a cache of certified identification documents, before many organisations will concede they even hold information on us, much less disclose the details.

Unintended consequences

In many respects, privacy has created a new class of secrets, epitomised by those three annoying words: "*sorry, that's confidential."* Alternatively, the phrase *"further identification particulars are required"* can make the simplest transaction a nightmare. Who is being served by this growing envelope of secrecy? Not the public, as emails, bank accounts and other records continue to be hacked across the globe.

Governments and business are the big winners, as they present citizens cum customers, with quick, easy online transactions; until something goes wrong and, our credit card is overdrawn in Bulgaria, our bank account is cashed in The Congo and we cannot prove to anyone that we are who we say we are.

The new secrets are not so secret,[3] which makes the establishment of the information trustee relationship so vitally important, along with "lift the veil" provisions.

[3] There is nothing about this submission I feel the need to shroud in confidentiality, so am happy to provide it to you online.

Recommendations:

1. That the Commission commence its analysis on the basis that that all levels of government and their agencies are the greatest offenders when it comes to people having their privacy invaded.
2. That legislation reverses the burden of proof, so that governments and private sector bodies are presumed to have breached privacy, requiring them to prove they have *not* done so.
3. That, when a breach is established, the officer or official who accessed, recorded, took and/or used the information improperly be held personally liable and, not enjoy any shield from their employer, be this the Crown or a private company.
4. That all records, be they on paper, online or in any other form, be held in trust for the benefit of those to whom they relate and, that organisations holding records for third parties hold no copyright in the records.
5. That the Commission urge the Commonwealth Government to abandon the personal electronic health record, as an ill-considered, poorly designed and poorly executed policy, with an unacceptably high probability of being the sources of innumerable privacy breaches concerning the most sensitive records pertaining to every individual in Australia. I cannot comprehend how this would *ever* be an acceptable risk.

Yours sincerely,

Adam Johnston

10 November 2013