What Privacy?
I want to be left alone.

Dr. Anthony G. Place

25 February 2005

This is a personal submission without affiliation to any organisation or company.

I have worked as a computer system engineer in a research capacity for over 10 years. In this time my work has included the developing of technology for mobile phone location and high speed data scanning, both of which can be used to invade privacy. I have witnessed the continual erosion of privacy though electronic means and the increasing ease at which privacy can be invaded. Because I have worked in these environments I am acutely aware of the engineering interest and effort put toward the collecting of information.

I am concerned about the continuing quiet erosion of individual's electronic privacy, in the light of the recent strong conflicting reaction to physical privacy. It seem ridiculous to me that a person lying on a public beach has a much higher right to privacy, or "to be left alone", while the digital equivalent is being covertly perpetrated daily for much more then a simple prank. The digital collection and use of information is continuing, mainly due to peoples' ignorance and inability to comprehend its consequences in the digital domain.

Mobile phone self location was mandated in the US by the FCC for 911 calls, but marketing companies seem to have other ideas. If marketers will be allowed to use this valuable private information then who else should have access. Would anyone like there whereabouts tracked "in the name of advertising". There is also a big difference to using an instantaneous location to send out an ad and storing a years worth of location measurements and collating it with other third parties information. If marketing people can use this information, what about individuals' commercial or political rivals, private investigators or even law enforcement?

A real concern is that people are not informed of, nor capable of comprehending the full consequences, of this use of private information. So what if people know I buy, but what if this is used incorrectly to determine your diet. Storing data and using it incorrectly is a significant issue in protecting the integrity of the information stored. A person may allow data to be recorded, but it would be assuming it would only be used at face value.

Individuals should have a complete a right to privacy and any relaxation of this privacy should be strictly controlled and balanced by any beneficiary's protection of the data access and integrity. As data is getting ever cheaper to store, examine and use it is increasing important to control its use. Both government and commercial control of personal data should be more strictly controlled.

There has been a continuing trend in legislation to support the commercial interests over private interests in the Copyright arena. Access has been substantially restricted in the current Copyright Act 1968 and under the Australia US Free Trade Agreement. Is privacy the next thing to completely bow to commercial interests? Due to cheap and easy access data in the digital domain is fundamentally difficult maintain balanced control. However this lack of ability to control should not allow the balance to be tipped in favor of commercial interests, as it is the individuals right to be left alone.

This review is focuses on the phrase "to be left alone", which is meant to be a fundamental focus of The Privacy Act 1988. The "right to be left alone" is in no way protected in the digital domain under the Privacy Act. This is highlighted by the definition of personal information, where it extends only to require that the individual be identifiable, not contactable. The technological equivalent of identifiable should include such information that allows the person to be contacted, such as fixed and mobile phone numbers and email address. Biometric information and unique or quasi-unique numbers need also be protected. This is particularly associated with issues raised by smart cards in their ability to store more information, transfer data and individualise users. However it is the personal information and it access that needs protecting and not the smart card technology itself. The following recommendation is technology independent and is relevant for any media.

Recommendation:

"personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity ***or any contact information* is apparent, or can reasonably be ascertained ***or verified***, from the information or opinion.**

"contact information" includes address, phone numbers, email addresses, personal web pages or any details by which an individual can be contacted.

"verified" means being able to uniquely associate a record with the a person whose identity is unknown, which includes biometric information/techniques, credit card numbers or any method of individualising information.

The privacy principles are sound as a principle but, in the digital domain where everything is based on communication and advertising, many companies state that data collection is a component of their business and that they will share this information. However the problem lies in what entities are collecting and how these entities collecting it. The issue of 'cookies' and 'spyware' are ever increasing issue that should be targeted under the Privacy Act in a technologically independent means. It should not be enough to have a broad privacy statement on the site that effectively says a company can do as it likes.

As a concession to an individual giving up some level of personal privacy, a company should have a reason to record and use any information, and the company should maintain the databases accuracy and never disclose it to others. A company should only store information that it can directly use in its normal operation.

If inflammation is needed for statistics reasons, or is to be given to other companies, then all data should be anonymised. The cost of managing and maintaining accurate record needs to be met by the company as consumers are allowing a reduction in their right to privacy by providing this information on the assumption that it will make the business more cost effective and consequently benefit them. If companies say it is too cost effective to maintain the database then they are simply storing too much irrelevant information.

A company should be required to contact people for whom they have contact information at regular intervals in order to inform people and provide an opportunity to correct or delete information. Again, if companies say it is not cost effective to maintain the contact information, why are they storing this contact information?

Recommendation:

If a business makes an indirect contact such as mail or email a reference to where the personal details (including contact details) were obtained must be supplied. If a business makes a direct contact such as telephone, whether though a call center or in-house, then the details of where the personal details (including contact details) were obtained must be available. Direct marketing companies should provide a mandatory combined national register for people who do not want to be contacted by phone, mail or email.

The above requirements make sense and are mostly in the privacy principles. However, in the digital domain where sharing data is cheap and easy and often difficult to trace, how is it possible to find out who has this data, and who they are getting the information from? Like

with the email 'spam' problem, once the email address is shared and integrated with other databases, particularly offshore, the data is effectively out of anyone's control. Therefore the entities under The Privacy Act should be held to a high standard, more akin the EU Privacy Directive 95/46/EC, and the penalties for breaching The Act should be increased significantly.

Recommendation:

Adopt much of the EU Privacy Directive 95/46/EC as opposed to any self regulation.
Create tougher inter-entity sharing requirements whether international or domestic.
Reduce or abolish the small company exemption.
Make stronger penalties for privacy offences so they become a deterrent.

A further concern is about the Australian Government's persistence at getting a national database of residents. It is meant to be for security and proof of identity but I guarantee it will eventually be used for other purposes such as law enforcement. However data stored for one reason, should not be used for another, because it may not be suitable. Any identification system based on individual biometrics that can also form latent evident or are externally visible should be carefully considered. This goes to my previous comment on individualization. Retinal scans are useful for identification and could not be used for law enforcement as retinal images are not persistent or useful under casual observation. However, there is a lot of talk about DNA, and biometrics such as fingerprint and facial recondition.

Recommendation:

The term "imaging" should not be used in "biometric imaging data". Biometric data can include non-graphical techniques such as voice and mathematical model based techniques that may only use graphical images as an input to a model.

Individuals have given up some of their right to privacy to companies and these companies need to better protect the access and integrity of this data. These issues should not be though of as, they collected it and should use it the way they want, but rather that individuals are granting them access to use the data for the betterment of the individuals. Without privacy you can not have freedom.