



# Data Privacy

Julian Thomas

Technology, Communications and Policy Lab

Digital Ethnography Research Centre, RMIT

# Difficult, unresolved problems...

The screenshot displays the front page of The Guardian website. The main headline is "My Health Record" with the subtext "Keep track of your important health information all in one place." Below this, there are buttons for "For you and your family" and "For healthcare professionals". A notice states: "This year, you will get a My Health Record unless you tell us you don't want one. If you don't want a My Health Record, let us know by 15 November 2018. Find out [how to opt out](#)." Below the notice are three video thumbnails: "Melissa's My Health Record story", "Your health record in your hands", and "Liz's My Health Record story". On the right side, there is a large article titled "Private health sector most vulnerable to data breaches - report" under the "Data protection" category. The article mentions that the finance sector is second, with criminal attacks and human error playing significant roles. A Samsung advertisement for the Galaxy Note9 is visible on the far right.

**My Health Record**  
Keep track of your important health information all in one place.

For you and your family — OR — For healthcare professionals

This year, you will get a My Health Record unless you tell us you don't want one.  
If you don't want a My Health Record, let us know by **15 November 2018**. Find out [how to opt out](#).

**Melissa's My Health Record story**  
Over 20 years we've seen hundreds and hundreds of providers.

**Your health record in your hands**  
All you need to know about My Health Record in 2018

**Liz's My Health Record story**  
"We can just log on to My Health Record and everything is right there."

[More news and media](#)

**The Guardian**  
Australia edition

**News** Opinion Sport Culture Lifestyle More

Australia World AU politics Environment Football Indigenous Australia Immigration Media Business Science Tech

**Data protection**

**Private health sector most vulnerable to data breaches - report**

Finance sector is second, with criminal attacks and human error playing significant roles in both sectors

**Melissa Davey**  
@MelissaDavey  
Tue 31 Jul 2018 17:17 AEST  
97  
This article is over 1 month old

**SAMSUNG**  
The new super powerful Note  
Learn more  
Galaxy Note9

# 45 years ago...

VOLUME FIVE, NUMBER ONE, FEBRUARY, 1973

PRICE

THE

AUSTRALIAN

COMPUTER  
JOURNAL



## Data Banks and Privacy — The Attitude of The A.C.S.

A problem which has lately received much attention, especially in Australia, is that of the privacy of information concerning individuals held in data banks. The Australian Computer Society feels that this is a problem on which it has a responsibility not only to express an opinion, but also to take an active part in convincing the appropriate bodies that adequate legislative controls must be implemented to ensure protection of privacy. This document expresses the attitude of the Australian Computer Society on this most important problem. It should be realised that this document covers the issue in broad perspective and provides a framework for future documents aimed at elaborating specific aspects or addressed to a particular objective.

### Introduction

The advent of modern technology and especially the proliferation of the computer and associated devices, has brought many advantages to present-day society. Whilst the positive advantages man has gained, and can continue to gain, must be recognised as of tremendous benefit, these must not overshadow or blind us to the very real dangers which have accompanied technological development. The developments of computer technology are making it increasingly easy for systems to be developed which fail to take into account the rights of individuals to privacy. It is thus becoming more and more likely that individuals' rights to privacy will unnecessarily be ignored, and the Australian Computer Society is anxious to ensure that precautions are taken to protect these rights.

### The Inevitability of Data Banks

We recognise that in our complex modern society data banks are not only essential, they are inevitable. The collection of large amounts of information relating to individuals within society is nothing new. The taxation collector has had very private details of earnings and expenses for a hundred years. The first census was taken in this country about 150 years ago. We have, in credit bureaux, in police files, in medical histories, in the armed services, in banks, in insurance companies, in marriage bureaux, in hospital files, in social services records and so on, a never ending record of the minutiae of our daily lives. Modern society cannot exist without such information.

The individual's protection in the past has been the difficulty of access to such information. The means had not been devised which enabled such large masses of data, stored in a variety of ways, to be analysed, sorted, collated and interpreted as one integrated set of related facts on a routine basis for everybody. Data were collected and used for specific purposes and the lack of effective and economical means of processing these for other unrelated purposes reduced the likelihood of unauthorised use. The existence of data banks is not new, but the power of the computer to manipulate them is.

The goals of economy and efficiency draw us towards ever growing accumulations of data. The Australian Computer Society, as the body representing the com-

puter professionals in this country, is very much aware of, and very concerned about, the use to which such information can, and possibly will, be put.

### The Problem of Definition

A data bank may be defined simply as a collection of information capable of being accessed to provide information concerning individuals.

It must be recognised that there are many kinds of data banks, differing significantly with respect to—

- Size,
- Coverage,
- Content,
- Whether public or private,
- Sources of the information,
- Purposes for which the information has been obtained and stored,
- Nature and sensitivity of the information.

The problems of privacy are much more acute in some cases than others, and it would be inappropriate for the full apparatus of controls required in some cases to apply in all cases.

It is envisaged that any legislation implementing these proposals will provide for the exception of certain categories of data banks from the general provisions outlined below, and that in respect of these data banks which are prescribed, it may be necessary for different controls and regulations to apply to differing categories of data bank.

### Protection of the Individual

The Australian Computer Society recognises that, as a group of citizens, its views on the nature of privacy are of no more (or less) significance than those of any other groups of citizens, but, being concerned at the way computer based files can be used, the Society considers that a person should have the following rights, to ensure that personal and private information about him is not misused:

- (i) The right to know who is keeping records about him in a prescribed data bank.
- (ii) The right to have reasonable access to all data relating to him held in a prescribed data bank.
- (iii) The right to have made available to him at regular intervals, or whenever a change is made, the details of all prescribed data relating to him.
- (iv) The right to challenge by personal appearance

## The ACS, 1973

We recognise only too well the increasing need for, and use of, large masses of data in many spheres of our everyday life. One of our basic aims as a Society is, of course, to extend the use of computers. The requirements of the computer user, as a person with a legitimate piece of work to do, as well as the individual need to be considered. While we believe that every effort should be made to introduce controls which will ensure the privacy of the individual, we think that care should be taken, at the same time, to avoid creating unreasonable barriers to the continued and beneficial development of computers and information systems.

# Emergence of a legal framework: A timeline of data privacy in Australia

1969, Zelman Cowen, ABC Boyer lectures, *The Private Man*

1973, “Data Banks and Privacy – The Attitude of the A.C.S.”, Australian Computer Society, Australian Computer Journal 5(1), 39-41.

1976, Australian Law Reform Commission receives “privacy” reference

1980, ALRC discussion papers on privacy, public hearings

1983, *Privacy*, ALRC report 22

1988, CofA, *Privacy Act 1988* – key Australian information privacy law

2014, Privacy Act 1988 amended with new Australian Privacy Principles (APPs)

2014, *Serious Invasions of Privacy in the Digital Era*, ALRC report 123

2017, OAIC and Data61 CSIRO, The De-Identification Decision-Making Framework

## What makes privacy a difficult issue: Competing and overlapping interests

- **Efficient and effective service delivery**
- **Freedom of expression; news; art**
- **Innovation**
- **National security**
- **Transparency and accountability; historical accuracy**
- **Delivery of emergency/essential services**
- **Prevention of crime and violence; protection of vulnerable people**
- **International standards and obligations**
- **Certainty and clarity (avoid fragmentation, inconsistency)**
- **Adaptability to new technologies (flexibility, forward-facing)**
- **Open justice**
- **Access to justice (simple, fair, affordable)**

## Australia's Privacy Act

regulates the collection, use, disclosure and other handling of personal information

**'Personal information' is:**

**information or opinion about an identified individual, or an individual who is reasonably identifiable, whether or not true and whether or not in material form.**

**'Sensitive information' is given greater protection**

### 13 APPs

1. open and transparent management of personal information
2. anonymity and pseudonymity
3. collection of solicited personal information
4. dealing with unsolicited personal information
5. notification of the collection of personal information
6. use or disclosure of personal information
7. direct marketing
8. cross-border disclosure of personal information
9. adoption, use or disclosure of government related identifiers
10. quality of personal information
11. security of personal information
12. access to personal information
13. correction of personal information

# Privacy Act applies to 'APP entities'

1. Australian Government agencies
2. private sector organisations with a turnover of more than \$3 million

For example: banks, large retailers, government departments and utilities providers

Exempt organisations may include many small businesses, NGOs

Exempt organisations may do things that have an impact on individual privacy.



## **Other laws relate to:**

- **Health information privacy (Commonwealth and State Acts)**
- **Communications privacy (Telecomms Act; TIA Act)**
- **Surveillance laws (State and Commonwealth criminal codes)**
- **Harassment and stalking (State and Commonwealth criminal codes)**
- **Industry codes (eg in broadcasting; Press Council)**
- **Common law (eg breach of confidence; but no common law for invasion of privacy)**

## **Some current risks of big data:**

- **Discriminatory profiling**
- **Data breaches; identity theft**
- **Re-identifying anonymous data**
- **Accumulation of inaccurate government/private sector data**
- **Trade in personal data**
- **Misinterpretation**

## Legal responses: Europe's General Data Protection Regulation (GDPR)

### Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability principle

### Lawful basis for processing

### Individual rights

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making including profiling

# ADM and Profiling under the GDPR

- automated individual decision-making —making a decision by automated means without any human involvement;
- Profiling: automated processing of personal data to evaluate certain things about an individual. Can be part of an ADM process.

## ADM only permitted under the GDPR when the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

## GDPR creates requirements to:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

## Questions:

- Should we have a right to be forgotten in Australia?
- Should we have a right to explanation?
- Do we need restrictions on ADM?
- How will privacy change in the digital age?