Submission by
Australian Consumers' Association[1]
to
Senate Legal and Constitutional References Committee
Inquiry into the Privacy Act 1988[2]

Preface

The Australian Consumers' Association (ACA) is a not-for-profit, non-party-political organisation established in 1959 to provide consumers with information and advice on goods, services, health and personal finances, and to help maintain and enhance the quality of life for consumers. The ACA is funded primarily through subscriptions to its web site, magazines, fee-for-service testing and related other expert services. Independent from government and industry, it lobbies and campaigns on behalf of consumers to advance their interests.

Adequacy of the Privacy Act in the face of technological change:

In the view of the ACA, the Privacy Act has not set a framework to keep pace with developing technological challenges. Other 'instruments', specific Federal legislation like the Spam Act and industry codes like the ACIF SMS code and the ADMA m-commerce code, have been required to advance consumer protection beyond the provisions and outside the framework of the Privacy Act in areas with considerable privacy implications. We also see a problem developing where industry does to turn to developing Privacy Codes with regard to emergent technologies; examples are biometrics (draft Code lodged) and RFID (probably not now being drafted as a Privacy Code as such). In our view Codes were envisaged by the legislation as applying to industries, or more narrowly to parts of industries or even organisations. This could be characterised as a 'vertical' orientation. The development of codes to cover technologies that might be used by any number of industries could be characterized as 'horizontal'. We have a number of concerns about the re-purposing of Privacy Codes to this horizontal orientation, which are briefly listed here:

- Complaints handling tends to continue to be left to the OFPC, which begs the question as to why the Code was needed.
- However if complaints handling were to be accommodated within an industry body, reach and enforceability would be in serious doubt.
- Coverage, in the sense of companies understanding the circumstances in which the technologically specific code would apply and the boundaries to that in their operations.
- Coverage, in the sense of companies being subject to a number of codes, the operations of which would need to be harmonised.

[1] ACA File Reference 04F466/01; 21 February 2005; ACA contact Charles C. Britton, Senior Policy Officer, IT and Communications Ph: (02) 9577 3290; 57 Carrington Rd Marrickville NSW 2204
[2] http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/tor.htm

- The granting of Code registration may well be taken as an imprimatur to the further deployment of a technology, when this is not the function or purpose of the Code. The OFPC does not have the resources or expertise to approve technologies for deployment into the Australian market – it should not be required to act as if it did.

Commercial electronic messaging

While one might aim at technologically neutral rules to protect privacy, the hazards that become apparent in technological developments, such as electronic mail, have consistently created the desire to be specific about aspects of the technology. Specific interventions had been required to address the need to seek consent before electronic messaging, the need for functional unsubscribe facilities and the need for accurate and specific identification in the course of all commercial electronic messaging. These requirements emerged from the realisation that electronic messaging couldn't work in a free-for-all environment; that without control over the flow of messages coming at them, consumers will simply disengage from the channels.

This is a technologically specific challenge the supposedly technological neutral Privacy Act has failed to meet. Regulation and enforcement are undoubtedly best cast in terms of the behaviour to be stopped, rather than a list of technologies that should be prohibited, if only because a new technology will almost inevitably appear and upset the regulation. However, where the principle falls down is in risk analysis. This is where the Privacy Act has failed to provide a sufficiently flexible framework to be relevant or allow the regulator to gain traction on a contemporary issue. This has been compounded by the chronic resource shortages to the OFPC, discussed below. Assessing where the hazard lies in a new technology is quite technologically specific and can be resource hungry. In the case of email, the differentiating characteristics of the technology that became apparent are:

1. Automation, allowing high volume low cost generation of messages
2. Non-material output, which further reduces cost to the supplier
3. Instantaneous intrusion into the consumers' world in such a way as to allow an almost immediate response by the consumer
4. Interactivity because the degree that the consumers response is more or less immediately available to the provider

This highly interactive, immaterial, automated environment can be generalised as "electronic messaging". The last decade showed that such messaging without significant cost or regulatory restraints on the originator will impose considerable burdens on the consumer. The degradation of the email "info-commons" has comprehensively demonstrated that the only way e-messaging can work (for business as well as consumers) is on an opt-in basis – that is giving the consumer control. Email has been a significant challenge to our formal privacy framework, one it failed to rise to. The job has been given to the communications regulator, the AComA, soon to be ACMA. However, our fear is that notwithstanding the sensible Australian approach in the Spam Act, the public email space may well be permanently corrupt.

Video surveillance

The minor panic over the possible use of mobile phone cameras in swimming pool change rooms also shows how challenges to the operation of the "technologically neutral" principle can occur. It seems clear that it is unacceptable for anybody to take photographs of another person in a changing shed, and even less so to circulate these images in some way. This is a technologically neutral imperative. It shouldn't happen whether the pictures are taken in black and white with a box brownie, a small film camera, instant picture camera, digital camera, or camera in a phone, PDA, or pen - any device capable of recording image data can create an image that is offensive. It is also useful to observe that some advertisements for camera phones have portrayed behaviour that is on the edge of what is socially acceptable, and industry needs to exercise restraint.

The hazard is of miniaturised cameras in a taken for granted common object (the mobile phone), with the capacity to transmit the image to a remote party instantaneously. The solution is to identify exactly what the hazard from the new technology is in terms that can be generalised. Perhaps the key hazards of mobile phone camera technology in changing rooms in these terms are:

1. Cameras concealed or embodied in everyday objects- people may not notice their operation
2. Transmission of images can be instantaneous when the imaging device is coupled with electronic messaging systems.

What is clear however is that the Federal Privacy Act as currently couched has nothing to say on the matter. To the extent that regulation and enforcement is required to enforce what should be a glaringly obvious social convention, it would undoubtedly best be cast in terms of the behaviour to be stopped, rather than a list of technologies that should be prohibited. We do not however support the extension of the Act or development of other federal legislation to cover behaviour by individuals. We feel this is best left to social norms backed by general or specific[3] laws covering offensive behaviour in egregious circumstances. Where the Federal legislation could usefully be extended is to cover commercial surveillance

Policy discussion of surveillance is often in terms of the workplace. This is an important topic, however in our view there is a wider context. The issue of cameras becoming cheap and integrated into everyday products to the point of ubiquity challenges the notion of what is 'personal information'. In our view a surveillance photograph of a person in say a retail outlet is personal information about that person, whether or not it associated with another identifying qualifier. The need for surveillance protection in the privacy framework is not about the odd pest on the beach with a camera phone, but in shops from cameras and RFID devices, and on the Net from spy ware and snooping record companies. Camera, storage and transmission equipment are all dropping dramatically in price and size while becoming increasingly easy to operate and integrate with other systems. This raises the prospects of increasing amounts of business surveillance of consumers, monitoring of citizens by various authorities and increasing observation by consumers of others.

[3] e.g. specific offence of "filming for indecent purposes" (s.21G of the NSW Summary Offences Act 1988)

Surveillance is currently largely the province of the States, and in our view there is some necessity to consider general Federal surveillance legislation, certainly with regards to commercial environments where consumers may be monitored and tracked, whether in the context of the Privacy Act or other wise. As stated above, we believe this should be confined to commercial surveillance activity. Equally we are comfortable with the media exemption in the current Act, and similarly feel that surveillance legislation should allow media latitude in the techniques allowed gathering news and exposing misbehaviour. Hidden camera journalism may raise hackles, but it also exercises some restraint over shonky traders and advisors. Consumers could be the losers from overly vigorous constraint of media information gathering.

Radio Frequency Identity (RFID)

Clearly protecting personal information is no longer just a matter of what is in an electronic version of a filing cabinet, as embodied in the data protection paradigm fundamental to the current approach. The importance of addressing the surveillance aspects of personal information is also demonstrated by the concern about Radio Frequency Identity (RFID) devices in consumer goods that has gained considerable prominence recently (although we note the absence of a specific mention in the terms of reference for this Inquiry). Usefully thought of as invisible bar codes, the technology utilises small transponders to store product information that is read out when activated by a specific radio frequency signal. These devices are likely to become small and cheap enough to be embedded in practically every product a consumer might buy. Whether the business and consumer case for this can be made remains uncertain. However, that does not mean the challenge that prospect poses to our privacy and surveillance framework can be ignored.

RFID potentially brings all our possessions and purchases into the electronic realm, and thus has the potential to radically alter concepts and norms of ownership and personal information. In some of the positive scenarios for RFID product labelling, such as lifetime environmental management of products and capacity to manage product recall, this is not a bad thing. At the very least, if generally deployed and used in retailing, it will increase the 'data density' of our social environment enormously. Huge amounts of data will be available to be gathered, stored, analysed and used. This will present considerable technical challenges. Importantly while a technology must succeed technically it must also be sustainable in commercial terms and consumer acceptability. If the technology is used in a way that outrages consumers, then a regulatory response will emerge, which may range from restrictions on use and deployment, or perhaps even outright banning.

There is a need to ensure that risk assessment of RFID is made objectively and that that real risks are addressed and importantly are seen to be addressed. ACA is concerned that lesser or unlikely risks could end up blocking a potentially useful innovation if neglect leads to panic. ACA does not see the answer in RFID specific legislation. Many of the issues in RFID are challenges to existing and desirable generalist legislation. Many of the backend data accumulation issues should be covered in the Privacy Act, with appropriate treatment of what constitutes personal information. Other RFID issues are

actually about surveillance and need attention in surveillance legislation, alongside optical and other techniques. It is this environment that would perhaps be best placed to deal with issues of implantable tags.

Location-based service (LBS)

Fleeting pieces of information can be highly revealing about a person and may be something they definitely want to control. Mobile phone networks know with increasing accuracy where users are located. This also challenges assumptions about how privacy and personal information interrelate – is location information a component of personal information, and how can it be used – we do not believe the current Privacy Act clearly establishes consumer control over location information. We were also concerned with the approach from AComA in their Discussion paper on the topic that issues such as "maintenance of end-user privacy in the provision of commercial LBS, the 'ownership' of customer location information ... or legal liabilities" that - "resolution of such concerns is principally a responsibility of the telecommunications industry itself."[4]

The mobile telephony challenge is that while the fixed line reveals (more or less) where the customer is, this was not migrated into the wireless domain. Now the technological means are increasingly to hand for wireless devices to also know with increasing accuracy where the user is. This is something that does not match current consumer expectations of how the technology behaves. In our view, any LBS must be opt-in and constantly under the control of the consumer. We are not reassured that under the current settings this would necessarily be achieved. In our view the AComA and the OFPC must involve themselves as carriers start to experiment with LBS offerings.

We would endorse the EU approach cited in the AComA Paper, whereby "these data may only be processed when they are made anonymous, or with the consent of the users of subscribers to the extent and for the duration necessary for the provision of a value addressed service."[5] We have very little sympathy with the approach cited for the US, where "The FCC did not want to inadvertently constrain technology or consumer choice through the introduction of regulation while the LBS market was in a nascent state." In our view, unless the consumer controls the context in which the information is released, a business making an unsolicited location-based approach will have a high probability of being inappropriate, intrusive and quite possibly offensive.

Integrated Public Number Database (IPND)

The lack of knowledge by most consumers about LBS information possibilities would be mirrored in the current concern about the use of customer information in the IPND database, where what the customer reasonably expects to be done with their customer information is under critical examination. The fundamental paradigm of directory access understood by consumers has changed as a result of the development and deployment of database technologies. Use for individual reference, where a person consults or searches a

[4] Location Location Location The future use of location information to enhance the handling of emergency mobile phone calls, January 2004 http://www.aca.gov.au/consumer_info/location.pdf P8
[5] Location Location Location P26

directory to obtain listed information for a specific person, is being supplemented in commerce by the use of the directory data as a database. The key distinction in our view is the programmatic use of the data in a serial fashion, using an API (application programming interface) without human viewing or intervention. This is materially different to the traditional definition and use of the directory – both in scope and scale – and is outside the general expectations of the ordinary consumer when they supply their personal information for the purposes of receiving a telecommunications service.

We have urged the AComA, in response to their Discussion Paper on the topic[6], to adopt this distinction to ensure consumer control over their personal information is preserved. Customers should be informed and their consent sought before their data is used in such an unexpected fashion (and potentially new and novel ways in future). We have been concerned that the proposed Standard from the AComA has been substantially delayed (the submission period closed on 14 May last year and the Draft Standard still remains outstanding), and note the assurances given to Senate Estimates that it will be complete by the middle of the year[7].

An important broader issue is the use of customer contact data beyond the purview of the IPND, in the databases maintained by various companies from various sources. Beyond the regulatory scope of the AComA, the Federal Privacy Commissioner (OFPC) has an important role to play in ensuring that customer information is used consistent with the expectations of customers and that there is not systemic abuse of that data – we have encouraged the AComA to coordinate closely with the OFPC, perhaps even to the point of concluding a memorandum of understanding. Importantly, as is the case with spam, the AComA is the regulator of choice because it has a set of compelling enforcement and investigative powers (albeit too infrequently employed for the taste of ACA) and a resource base that substantially outclasses the OFPC. The fatal flaw of the OFPC is the meagreness of its powers and the paucity of its resources, something we return to below.

Spyware

The Internet is another environment where monitoring and surveillance are a constant threat to consumers, where a whole class of menace has emerged under the rubric of Spyware, which can either be loaded surreptitiously onto consumers' computer, or perhaps unwittingly installed by them with legitimate products, perhaps even giving permission in some part of a click-thru contract. These programs then beam all manner of information back to their originator, with the consumer none the wiser. We understand an evaluation is being made by Government of the adequacy of current law to counter the consumer detriment in the behaviour. The challenges of spyware are not all privacy issues – we are concerned about:

- Trespass and theft issues - who owns the computer?
- Costs –of bandwidth, software prevention, system downtime and instability, repair costs etc
- Ability to remove or inactivate the product or spying component/behaviour

[6] Who's Got Your Number? Regulating the Use of Telecommunications Customer Information http://www.aca.gov.au/aca_home/issues_for_comment/discussion/customer_info_disc_paper.pdf
[7] http://www.aph.gov.au/hansard/senate/commttee/S8078.pdf

- Contractual terms that purport to assert consent

However within this technology there are certainly challenges has to the privacy framework. There are issues of whether what spyware may be gathering is explicitly or strictly personal information. In our view it definitely works within the personal information space of the consumer, which needs to be protected.

There is also the question of remote access to the computers of consumers without their permission, as reported recently in a local court case:

> *Hundreds of thousands of Australian users of Kazaa are being stalked online by the music industry's hired gun, an American company that tracks down and then remotely enters home computers it finds swapping songs.*[8]

Consumers should have an enforceable right to know who is watching them, and to make them stop if they do not like it unless the watcher has some overriding authorisation such as a court order or warrant. We certainly do not consider private investigations of alleged copyright infringement to meet this test in any regard. However we do not think the OFPC has been spectacularly successful in defending the rights of consumers in this domain.

National identification environment

The shape of this system is well sketched by the recent Securities Industry Research Centre (SIRCA) report entitled "Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent".[9] As described, "a number of documents are relied upon as PoI[10] in a de facto framework, with the organizations that produce these documents being considered PoI issuers in the absence of a prescribed alternative."[11] The SIRCA report is seemingly judgemental of this 'complex and fluid' system, which is described as highly inter-dependent and overlapping. However, in our opinion, the situation revealed by the report is of a strong system, the very strength of which is related to its diversity. What is revealed is that the Australian identity system functions successfully as a distributed heterogenous environment. The picture that emerges is of a self-regulating, self-organising and self-healing system that has emerged without a central point of identity origination and control. There is no single point of compromise or failure, and this protects both consumers and commercial players. It is robust because it contains redundancies (overlaps) that provide a self-checking environment – one of the first lessons learnt in IT. There are many forms of identification in the market and participants chose those that are commercially relevant. Therefore in the opinion of the ACA, Australia does have a national identification regime today, one that serves most consumers quite well on a day-to-day basis.

It would be naïve and complacent not to acknowledge challenges within that regime. It does seem clear that some traditional authentication documentation and credentials such as birth certificates, drivers' licenses and various commercial statements are falling prey

[8] Spies trace music swappers SMH Kirsty Needham, Consumer Reporter December 3, 2004 http://www.smh.com.au/articles/2004/12/02/1101923273799.html
[9] http://www.sirca.org.au/news/releases/2003/0302FraudBook.html
[10] PoI = Proof of Identity
[11] SIRCA P20

to counterfeiting and forgery with the advent of technologies such as scanners, laser printers and colour photocopiers. N our view these challenges need to be met, not with an additional layer of electronic authentication, but by making existing processes more robust. This means designing better documents, and constructing document reference mechanisms that validate the credential in specific circumstances, without intruding unnecessarily on the personal identity of the individual holding it. Firms and their customers can then make their own business specific risk assessments based on identity elements relevant and proportionate to the business at hand.

This more business process specific, decentralised approach resonates with the PKI approach that seems to be gaining traction in the marketplace; that is embedded and application specific usage. As argued by Stephen Wilson, past chair of the Certification Forum of Australasia. He says:

> "PKI tends to deliver its greatest benefits — automatic paperless processing, reduced legal risk, lower cost of dispute resolution — in high value, specialist applications, where digital personae are application-specific, linked to credentials rather than personal identity."[12]

This is would be exemplified in the various credit card initiatives using this technology. The vision is more limited. It is not a general-purpose identifier. It cannot be used outside the credit card framework, but within that framework it is easy to use – in fact the consumer may not have any idea they are using anything as sophisticated as a digital signature. The risk equation is significantly balanced by the application specific domain for the identifier – it cannot be used for purposes unrelated to it original purpose. The credit card industry, while not without its problems at least has a record of delivering risk management as an integral part of its consumer proposition. Critically it draws on the contextual elements of identity authentication.

There is a definite consumer interest in secure identification. They want their electronic assets (such credit cards and bank balances) protected from e-looters. They do not want their information revealed to the wrong people. They have an interest in a robust transactional environment and would benefit from greater symmetry in the authentication propositions put to them – many marketplace assertions from business could do with a great deal more authentication! However, the push to greater authentication of identity assertions poses problems. There is the threat to identity from authentication propositions that seek to link authentication to a single individual 'super-identity', frequently but not necessarily based in some biological measurement. This challenges consumer legitimate control of their identities by creating linkages that are essentially unnecessary in many circumstances and inappropriate in others. It creates hazards for privacy as information is consolidated, exposed and shared in ways that the consumer may be unhappy about, if they are aware of them.

On the flip side, a key commercial (as opposed to marketing) interest in identification is non-repudiation – that is, once a consumer has committed to a transaction, making it so they cannot avoid obligations by saying "Oh, it wasn't me that entered into the arrangement". Usually this is not a problem in a standard cash transaction; anonymity is

[12] PKI without tears http://www.voiceanddata.com.au/vd/tech_speak/ts_112003a.asp

not a problem to most business once they have the money. In the paper world a physical signature achieves non-repudiation, such on a cheque; although in legally important situations witnesses are required the truly cautious will ensure all parties initial every page of an agreement. So in traditional domain the continuum of identification relates to the commercial 'strength' of the transaction.

Discussions of electronic identification sometimes ignore is this idea, which can lead to a polarised view of identity. In our view identification technology should only be used proportional to the purpose of the transaction when identity itself is material to the transaction, not just when convenient or as a matter of course. People should not have to identify themselves just to seek information or browse a system, to undertake transactions where identity is not material, even if they are in possession of some kind of validated identifier.

Smartcards

This is the problem with many smartcard proposals. Many technologists favouring a single robust identity for an individual and to many smart cards seem to be logical item to build as a token for that identity. Once a single highly authenticated identity is seen as desirable, pressure is on to build it as strongly as possible so that it can be used for as many purposes as possible. This is where many of the consumer issues and problems arise. We would regard it as naive and dangerous to assume that a single authentic identity is necessary or even desirable for most consumers. People act in roles in their lives, and have different identity requirements in each of them. Different people have differing degrees of need for or sensitivity to the protection of their personal information. Over-identification is a serious issue as electronic methods overtake the traditional physical means of transaction using smart cards for instance.

Superficially, maximum consumer utility for smart card technology seems to be enhanced by minimising the stack of cards problem. But multiple applications interoperating on the card, perhaps sharing core personal and authentication data in electronic communication with government and commercial enterprises poses a huge privacy risk. For example, to be issued a multi-purpose smart card that can undertake a variety of state government functions may require an evidentiary approach to identification such as a points-based check. This card may also then be used to undertake small personal transactions such as buying public transport fares. Thus an anonymous exchange now identified with a considerable degree of certainty. This hazard of over-identification is compounded when the identity document is machine-readable. If the identity contents of the smartcard are easily available to a reader, then a business can quickly scan a consumer's license at point of sale and compile a high quality identity linkage in their database very easily.

Because of these sensitivities in smartcard technology, we chose to make a submission about the Queensland development of a new driver. The proposal is for a smartcard-oriented license that will probably be the first major deployment of the technology in Australia. As such it will drive standards and set precedents that will shape future implementations of smartcards. The driver license has been and is shaping to become

even more important in the authentication environment navigated by the average consumer. This has emerged de facto and the smartcard implementation creates additional concerns and consequences. We are also aware of ongoing moves to harmonise state driver license schemes and streamline data exchange. Confined to the task of managing driver accreditation and law enforcement under appropriate privacy safeguards such harmonisation has potential to deliver public benefits. If the wider utilisation inherent in some of the consequences of the Queensland proposal are rolled out on a national scale, then a national identity card framework may well emerge. This should not occur unremarked.

The proposal raised the possibility of vastly expanded use of the driver license in commercial identity management. It contemplated what we see as a potentially dangerous combination of strong authentication technologies with smartcard payment technology most useful for relatively minor cashless transactions. ACA also has reservations about government (in the first instance that of Queensland, but potentially all State governments) being so deeply involved in commercial markets. This goes past mere standards setting. A digital signature scheme that is perceived to have the backing of government, a smartcard host that carries the critical mass of Government, State identity credential provision – these are all potentially contestable areas where industry development will be crowded by Government participation. This may deny consumers the benefit of competition, with resultant lack of innovation and higher pricing in a wide range of markets for goods and services. In our view Government should only enter markets for reasons of market failure. While the smartcard market is immature, and the technology has not delivered some of its more visionary promise, we do not think this sufficiently extreme to justify significant Government involvement in the marketplace.

One of the key selling propositions for smart card technology is as a cash replacement. An important part of substituting for cash is to maintain the anonymity of cash transactions. For the low value and trivial transactions that characterise the use of cash in the life an average consumer, creating the situation where an identifying electronic trail could result is inappropriate. Such electronic footprints may seem trivial and innocuous, but create an environment that could be used for tracking and tracing, and possibly more likely, commercial data mining and profiling exercises that seek to identify consumer characteristics and then target market individuals based on the result. The essential point is that a cash replacing smart card does not have to carry these consequences. However such a smart card married to a Driver License or other high value authentication credential, not only carries identifying information, but functions as a highly authenticated identity token, disproportionate to the transactions on which most commercial smartcard propositions are focussed. They should be kept separate and in our view the Driver License technology should be focussed on delivering secure driver licensing.

Technology must be designed and built so consumers are in control of what the technology does so that it actually improves the consumers' privacy. The electronic snail trail we leave can increasingly be a substantially complete and precise record of our lives documenting not only our whims but also our foibles, our consumer wants and deeds. It

may mean the demise of anonymity. The outgoing Federal Privacy Commissioner noted that "Complete anonymity is neither possible nor desirable in human society. However, a free society generally allows individuals to make appropriate choices about when, and to what extent, they reveal themselves to others."[13] In the estimation of the ACA the right to trade anonymously is a fundamental one, one that is indeed enshrined in the National Privacy principles. Shadow shopping is a key method of consumer organizations (and some regulators) to keep the market honest. Individual consumers use it when they shop around. Consumer transparency may enable better personalisation, but it will also allow companies to choose their marks better. Consumers are empowered by ability to choose what they wish to reveal when they wish. The OFPC should be resourced and empowered to make sure this remains a real choice for consumers as commercially driven technologies make it more difficult.

Biometrics

The ACA considers it imperative that any deployment of biometric technology is undertaken in a context of good privacy practice, clear assessments of technological capability and capacity, and adequate consumer protection. Unfortunately in our view, it is not at all clear this is the current direction for developments and deployments in this field. We provided comments to the Biometrics Institute about their Draft Privacy Code, which we understand remains with the OFPC for consideration as a registered Privacy Code. There is an obvious problem with an industry association developed code, which is that it applies only to members of that association. These difficulties are compounded in the case of the Biometrics Institute (BI) where the body covers a technology or indeed a set of technologies, rather than an industry. Comments were made previously in this submission about the re-purposing of the privacy code environment in an attempt to grapple with emergent technologies. Many organisations that might use biometric technologies would be covered by Privacy Codes that relate to their specific vertical industry (such as direct marketing, insurance or banking) and certainly be covered by the default OFPC arrangements. Hence the Biometric Code may cover a certain part of a transaction, but other portions would be subject to the generic arrangements. This would not produce certainty or simplicity for either consumer or company. In our view it was a mistake to submit the Code for registration as a Privacy Code. In our view the Code would have been better billed as a general Code of Conduct for Biometric Implementations. It would have been substantially privacy oriented, but could also have dealt more comfortably with important questions of technological reliability and transparency as well as consumer protection, risk management and redress.

One key observation is 'biometrics' is not a technology as such. The term encompasses the operation of multiple technologies, traditionally used individually but increasingly employed in concert. Biometrics could more usefully be described as a set of technologies, or perhaps be seen as a technique, defined by the use of technologically obtained information inputs and outputs. Critical definitional distinctions that do need to be made are between the biological information resident with the individual, the sampled image acquired by the biometric device and the identifier abstracted from that image.

[13] http://www.privacy.gov.au/news/speeches/sp1_04p.pdf

Thus we often detect the following terms referring to interchangeably as biometrics, but which should be separately defined and used precisely:

- Biological information - information resident with the individual.
- Biological sample – an actual physical sample from the individual containing some biological information.
- Biological record – a measurement or image that records aspects of the biological information of an individual.
- Biometric image - the raw sampled image or measurement of biological information acquired by a biometric device.
- Biometric identifier - the identifier abstracted from a biometric image by processing to suit a particular identification or authentication project.
- The latter two items could perhaps jointly, but carefully, be referred to as 'biometric information'.

Therefore we do not think the Committee should confine itself to biometric imaging data as suggested in the terms of reference, since all of these forms of data are associated with a person and are capable of use and abuse in subtly different ways.

Passports

The recent revisions to the Australian passport brought together concerns about smartcards, biometrics and the role of high integrity authentication credentials in the Australian domestic marketplace. Our chief concerns in regard to the passport review were with regard to the role the document plays in the identity system within Australia. The shape of this system was sketched above.

One area of concern was the headlining of the Passport Review as an initiative that "will strengthen the Government's ability to combat identity fraud." The Review was positioned in terms of identity fraud in general in Australia rather than with reference to travel identity fraud. Our concern is with the possible expanded use of the credential IN Australia rather than as a travel document in and out of Australia. This is particularly the case given the general unavailability of persuasive figures or studies on f importance of identity fraud in Australian society, the changing incidence of any offences and the utility of initiatives that aim to reduce identity fraud. We would have significant reservations were the Passport to become a vector into the domestic market for identity technologies that might have a place at the international borders of the world, but have scant relevance for the consumer at the supermarket checkout or bank branch.

It is obvious that passport issuance and replacement should be secure. What is substantially less obvious is the degree to which any putative current insecurity is contributing to what has already been established as hazy picture of actual identity fraud in Australia. Passports Australia 2003-03 Achievements and Challenges documents 535 detected cases of fraud in the period. This is not a large number compared with the 968,300 passports issued in 2002[14]. However, it is noteworthy that of these only 53 or just on ten percent were referred to the AFP – this is vanishingly small percentage (0.005%) of passports issued yearly. It does not seem likely to us that cases of actual

[14] SIRCA Report P70

identity fraud, as opposed to various mistakes and subterfuges to do with passport matters, would not be referred to the police. Therefore a comparatively minor contribution of passports to identity fraud in Australia can be inferred.

Biometric data will now be stored on Australian passports. However, the application of biometric in the field to achieve the stated objective of detecting fraudulent use of a passport must be regarded sceptically in the light of the shortcomings identified by competent observers in the field of biometrics. These views were well summated by the Economist editorial late last year, which observed:

> "For years, lobby groups have campaigned against biometrics on the grounds that they will undermine privacy and lead to the setting up of Big-Brotherish monitoring systems by governments. In fact, there is not much danger of this happening with today's flaky biometric technology. If and when it improves, such privacy issues will need to be addressed. But at the moment the greater danger is that governments are investing too much faith and too much money, with too little public debate, in an immature technology that is unlikely to improve the security of their citizens, and could very well reduce it."[15]

We are particularly alarmed by the connotations of a throwaway reference in the additional material forwarded about biometrics by DFAT, where it is stated:

> Based on initial results, several key reasons for an incorrect or low scoring match have been identified (e.g. smile with teeth showing, non-standard illumination, hair over the face, non-centred pose, glasses with dark tint). This has resulted in new passport photo guidelines being developed to ensure submitted passport photos will provide the best possible performance for biometric matching.

In the worst sort of technology push imaginable, we face the prospect of a requirement for citizens to submit unsmiling to imaging procedures, wearing standardised spectacles, with government standard haircuts, in a special official pose – a prescription that seems more suited to North Korea than to Australia. What emphasises the risible aspect to a otherwise potentially objectionable scenario is the later assertion that:

> Insertion of a biometric identifier in the passport will provide capability for face-match searching of terrorist watch lists at our borders ...

This would presumably work on the premise that suspects on such a list would be posed in the acceptable fashion, appropriately accoutred and accessorised.

There was scant reference in the production of the passport review either to technological neutrality or to technologically specific risk. There was no discussion about how the facial biometric might be managed to stop abuse and development of function creep. In this regard in our view it is worth considering the point made in the 2002-2003 Annual Report of the Federal Privacy Commissioner:

> "The border control environment will be an important test for the development of standards and codes of practice regarding the design, implementation and use of biometrics, both nationally and internationally.
>
> ...

[15] Dec 4th 2003 From The Economist print edition, Online article Prepare to be scanned at http://www.economist.com/science/displayStory.cfm?Story_ID=2246191

> Determining how a biometrics-based system is developed, however, is only part of the equation. It is equally important to put in place a robust accountability framework and, where possible, to place technological limitations on the biometric to prevent unauthorised use and to protect against gradual 'function creep'. Investing in technological safeguards of this sort can take us beyond mere rules that say what should and should not be done with sensitive data, to deliver functional limitations that better protect privacy."[16]

In this context it is useful to visit the latest expression of concern on the topic by the Economist (Feb 19-25 2005), which summarises as follows:

> … there is cause for concern. For one thing, the data on these chips will be readable remotely, without the bearer knowing. And—again at America's insistence—those data will not be encrypted, so anybody with a suitable reader, be they official, commercial, criminal or terrorist, will be able to check a passport holder's details. To make matters worse, biometric technology—as systems capable of recognising fingerprints, irises and faces are known—is still less than reliable, and so when it is supposed to work, at airports for example, it may not. Finally, its introduction has been terribly rushed, risking further mishaps.[17]

One of the cited limited purposes for which it is reasonable to use passport information is to be maintaining "identity integrity". Identity integrity in an Australian domestic context could encompass a wide variety of activities by any number of commercial and governmental entities. In our view the central thrust of the Passport should be its role in external travel by Australians. We should not deny the traditional role the passport has played in the domestic identity system, but avoid the unintended consequence of destabilising that system. This could occur by providing an impetus for new technologies that may well not be useful, or by providing a technologically enabled document that will find greater utility than currently the case. Either risks creating pressures that may create unmanageable tensions and outcomes. This aspect must be recognised in relation to any government sanctioned or provided identity token. Once again the OFPC should have a much more central role in providing authoritative whole of Government guidance on such matters, rather than being consigned to the role of carping bit player.

Success in extending the privacy scheme to the private sector:

ACA endorses the goal of a single, comprehensive, nationally consistent scheme for privacy protection in Australia. Such consistency makes the task of compliance by industry easier and cheaper. It facilitates education of all concerned, including consumers and scope for confusion by all parties reduced. However, we feel that events have unfolded to confirm our original reservations about the framework and to demonstrate flaws that were not anticipated, particularly weaknesses in terms of direct marketing and complaints handling. Our view of the self-regulatory regime established by the Act was of a weak default system and fractured self-regulation. We felt that from

[16] http://www.privacy.gov.au/publications/03annrep.pdf Page 41
[17] http://www.economist.com/science/displayStory.cfm?story_id=3666171

an initial goal of simple legislation meshed with a self-regulatory regime, the Act embodied considerable complexity based in legislative exception and definition, which would ultimately make the operation of privacy protection opaque and uncertain. We suggested it would fail to adequately protect the privacy of individuals.

The weakness of the default system has been demonstrated in the incapacity of the Office of the Federal Privacy Commissioner (OFPC) to cope adequately with the volume of complaints and enquiries generated by the passage of the legislation, and the related inability to engage policy development and debates, and to pursue audit programs in the public sector aspects of its mission. The fractured self-regulatory scheme anticipated has not developed because of the reluctance of industry to develop and register codes. The issues that seem to have delivered the greatest consumer confusion have been the small business exception, the role of consent, and the continued intrusion of direct marketing. The capacity of the legislation to deal with emerging technological challenges is also somewhat suspect, which is ironic in light of its much-vaunted 'technological neutrality'.

This is not to pronounce the legislation a complete failure. There have been modest steps in improving consumer awareness of privacy, and many companies have moved to adopt substantial compliance with the Act. However in our view, Australian consumers have not been as well served by the legislation as they might have expected. We are concerned that what is emerging is a patchwork of privacy protection, driven in various ways by divisions between public and private sectors of the economy, state and federal levels of government, specific economic sectors (such as health), emerging technologies all of which have subverted the aim of the legislation in this regard. Not least of the drivers for these divisions are the gaps embodied in the federal legislation (such as the small business exemption and employee record exception) that was intended to deliver the nationally consistent scheme.

Office of the Federal Privacy Commissioner (OFPC) resources and powers:

Resources

We are aware of and concerned by the delays and queues that have characterised complaints handling by the OFPC over the term of the Private Sector amendments to the Act. These in turn may well have fed back into a public perception of the Office as being incapable of delivering a satisfactory outcome. This is obviously at variance with the goal articulated by the OFPC as focussing the Office on providing "timelier, lower cost, satisfactory outcomes for individuals"[18]. Indeed our primary observation is that whatever merits of the strategic direction established, it has been overwhelmed by resource constraints, which have bound the Office tightly to one aspect of its compliance role, dealing with complaints from individuals. Public sector audits, inputs to policymaking and effective engagement of public education have all suffered, while at the same time, speedy complaint resolution has proven difficult to deliver. This is acknowledged in the Issues Paper by the OFPC into its review of its own operations, which indicates that

[18] http://www.privacy.gov.au/act/review/ispap2004.pdf P27

having identified complaint handling as a priority the Office diverted resources from other areas of responsibility. This clearly indicates that the strategic direction of the Office has been subverted by short-term contingencies.

The OFPC Issues Paper essays the argument in defence of focusing on conciliation rather than enforcement that "It could be argued that this appears to have worked well for most complainants to the Office."[19] We remain to be convinced that this is the case without confirmation by an audit of outcomes from the Office. Such an audit should be a permanent and regular feature of the operations of the Office. In our experience even comparatively successful ADR schemes have problems with abandonment of complaints by discouraged consumers. Our counter hypothesis would be that the OFPC has a high rate of discouraged complainants, abandoned complaints and unhappy consumers. Consumers must have confidence that if their rights are flouted, they can easily seek speedy and effective redress. This is not the case for privacy rights in Australia following the passage of the Act. The patchwork of protection noted above is in part to blame. It is a startling figure from OFPC research that "only 7% of respondents would report misuse of their personal information by an organisation to the Office of the Privacy Commissioner." [20] This could be because of scant consumer awareness of the Office – a likely scenario. However, the same research showed that 34% of respondents were aware of the existence of the OFPC[21]. This leaves a gap of some 27% of respondents who while aware of it would not use it for a complaint.

In our view one of the ways that the OFPC could encourage community confidence that privacy rights are protected is by more vigorous and apparent enforcement action. Action further than simple awareness-raising will be required to rehabilitate the reputation of the Office and convince consumers that there really is a viable avenue for privacy complaints at the OFPC. This would involve establishment of a resource stream to the Office sufficient to meet the complaints load and to discharge the other duties of the Office in providing policy advice, researching and anticipating innovation, and conducting audits and other active information seeking programs, such as shadow shopping perhaps. In our view a mechanism should be established that provides a funding stream to the dispute resolution activities of the Office that is commensurate with and scales to meet the volume of complaints coming to the OFPC. Preferably this funding would be provided by a scheme whereby organisations complained against bear the cost. Indeed our preference would be for a separation of the dispute resolution aspects of the Office from its regulatory functions – the two do not always sit comfortably in the same structure. As a regulator the OFPC should have a role in defining and monitoring the effectiveness ADR functions as well as being required to respond to systemic problems revealed by the individual complaints data.

We have little sympathy with any current complaints of compliance cost with the Privacy scheme. It is difficult to conjure a vision of a more bare-bones privacy framework. There is no required reporting and no mandatory recording. The OFPC has scant

[19] The Issues Paper P30
[20] The Issues Paper P28
[21] Community Attitudes Towards Privacy P13

investigative powers and none of audit in the private sector, and so cannot impinge seriously on commerce in that way. The Act, when not establishing exceptions and exemptions, sets out little more than reasonably sensible data management practice. The OFPC has no power to seek anything other than restitution and so has little capacity to impose direct cost on industry.

Where we have sympathy with industry is in the point that companies have in many sectors devoted some not-inconsiderable effort to ensuring they meet the prescriptions of the Act in a consistent and reliable way, while the resources assigned to the OFPC to achieve its mission in the private sector are derisory. In our view, while the OFPC has laboured mightily with the scant resources it has been given, the overall impression is that the Government has actually taken its own legislation a lot less seriously than the organisations to which it applies. If this persists, it inspires an atmosphere of demolition by neglect, scarcely a credible position for any organisation, let alone a regulator with an enforcement role, albeit a restricted one.

Powers

In our view the powers of the OFPC are too restricted. We do not advocate a draconian or a legalistic 'black letter' approach to this or most other areas of regulation. However a credible set of powers and penalties connects the regulator with the legal framework of enforcement, and ensures that more 'light handed' interventions have the weight of possible further action attached to them. We are also concerned about the disconnection of the OFPC from systemic issues by the complaints focus of the Privacy Act. While we certainly advocate that consumers should have access to fair and speedy on resolution of individual problems, in many respects to focus of our concerns are on systemic issues and general corporate behaviour.

From this perspective then, we argue that the Commissioner should:

- Have an audit power in relation to the private sector;
- Have the capacity to address systemic privacy problems outside the context of resolving an individual complaint and deliver an enforceable outcome;
- Have the power to fine an organisation that breaches privacy provisions;
- Be able to enforce any directions given in relation to findings after an own motion investigation;
- Be able to seek court enforceable undertakings;
- Be empowered to issue a standard or binding code to address systemic failings.

While there may be resource implications of such changes, these are not necessarily all negative. The prospect of more vigorous regulatory action may well lower the number of complaints over time, while enforceable fines would in fact yield revenue, albeit to consolidated government funds. Coupled with a more industry funded ADR scheme as outlined above, these changes could well mean the OFPC becoming a far more cost-effective instrument.