

Consumers' Federation of Australia

submission to

**The Review of the private sector provisions of
the Privacy Act 1988 (Cth) Issues Paper dated
October 2004**

December 2004

Table of Contents

<i>Part 1. Introduction</i>	3
1.1. About CFA	3
1.2. Executive Summary	3
<i>Part 2. A single, comprehensive nationally consistent scheme</i>	5
2.1. Single, comprehensive nationally consistent scheme	5
2.2. Other provisions of the Privacy Act – Interaction with credit reporting provisions	5
<i>Part 3. International issues and obligations</i>	12
<i>Part 4. Recognising individual rights</i>	13
4.1. Awareness of Rights	13
4.2. Community confidence that rights are protected	15
4.3. Approaches to complaint handling	18
4.4. Individual’s control over personal information	25
<i>Part 5. Balance of individual privacy interests with business efficiency</i>	27
5.1. Codes	27
5.2. Small business exemption	27
5.3. Direct Marketing	29
5.4. Compliance	33
5.5. Business efficiency and private sector contracting	34
<i>Part 6. Balance between privacy of individual and other social interests</i>	35
<i>Part 7. NPPs generally</i>	35
<i>Part 8. Matters that have an impact on the operation of the private sector</i>	35
<i>Part 9. Any other issues</i>	35
9.1. Abuse of the Privacy Act as an excuse	35

Part 1. Introduction

1.1. About CFA

Consumers' Federation of Australia (CFA) is the national peak body for consumer groups in Australia. CFA's 95 members include legal centres, health rights groups, local consumer organisations and public interest bodies. CFA's role is to put the view of its member organisations to government and industry and advocate on behalf of consumers. Established in 1974, our focus is primarily on advancing the interests of disadvantaged or vulnerable consumers.

1.2. Executive Summary

CFA welcomes the opportunity to make submissions to the Review of the *Privacy Act 1988* ('the Act') private sector provision. However, it is disappointing that certain issues of concern have not be specifically included in the terms of reference. For example, we are gravely concerned that credit reporting provisions of the Act (Part IIIA) are not being specifically reviewed, even though the CFA and other consumer groups have stated that their review is long overdue. Other specific issues which may be seen as outside of the terms of reference include the need for the Act to encompass other areas such as surveillance, intrusion, and privacy of the person; the exemption for employee records; the exemption for political acts and practices; and genetic privacy. Further submissions in respect of these issues have been made by the Australian Privacy Foundation ('APF').

We also agree with the view expressed by the APF that the Privacy Commissioner needs to take a more proactive role, both in this review, enforcement and otherwise, in advocating for privacy protection.

CFA contends that there are four main areas of the National Privacy Principles in need of urgent reform. The areas identified are not meeting the principles of the fair handling of personal information.

- 1) **Bundling of consents.** CFA agrees with the comments of Malcolm Crompton, the Federal Privacy Commissioner noted in his press release dated 23/5/02 in relation to bundled consents. Consents bundled together cannot be considered freely given as the individual is often faced with "sign or no deal". Legislative reform is required to address this issue as there is little or no evidence of organisations voluntarily "unbundling consents".
- 2) **Timing of disclosure.** CFA considers that targetted disclosure is critical to the individuals understanding of how and when his/her personal information

is being used. Upfront disclosure only is insufficient and leaves an individual with the perception and the reality that s/he does not know what personal information is being used and disclosed and when.

- 3) **Direct marketing and opt-in.** NPP 2.1(c) is inconsistent with good privacy practice. An opt-out system is entirely inappropriate and the legislation must be revised to make direct marketing opt-in. Direct marketing can be highly intrusive and the mechanisms to "opt-out" vary widely, are difficult to use and poorly disclosed.
- 4) **Improved complaint handling.** Complaint handling by the OFPC is completely unsatisfactory. There are 3 key reasons for this: 1) Decisions are not made instead the OFPC ceases to investigate under section 41 of the Act. This means there are no detailed published decisions which can be scrutinised. 2) There are no detailed guidelines and policies to guide individuals through the complaints process 3) Complaints are processed very slowly. These matters in combination amount to a denial of natural justice and procedural fairness.

In this submission, CFA will argue that the OFPC and the legislative regime with respect to privacy are far from satisfactory.

Part 2. A single, comprehensive nationally consistent scheme

2.1. Single, comprehensive nationally consistent scheme

CFA submits that a single, comprehensive, nationally consistent scheme is essential for privacy protection for consumers in Australia, while at the same time making compliance easier, cheaper and less resource-intensive for industry. It has the potential to increase consumer understanding and reduce confusion.

However, the current model has not been as successful as anticipated, particularly in terms of direct marketing and complaints handling. The Office of the Federal Privacy Commissioner (OFPC) as enforcement agency has not been able to cope efficiently and adequately with the volume of complaints and enquiries generated by the passage of the amendment legislation, and has not been fully able to engage policy development and debates. It is bitterly disappointing that the OFPC has had to re-allocate resources away from the audit programs in the public sector.

The self-regulatory regime that has emerged is a patchwork driven by divisions between public and private sectors of the economy, state and federal levels of government, specific economic sectors, and emerging technologies, all of which have subverted the aim of the legislation. In particular, gaps in the federal legislation, such as the small business exemption and employee record exception that were intended to delivery the nationally consistent scheme have been a major driving force for these divisions.

2.2. Other provisions of the Privacy Act – Interaction with credit reporting provisions

CFA has long been concerned with the credit reporting provisions in the Act and has in fact been particularly active in advocating for the review of the credit reporting system. We are disappointed that credit reporting is not under review in this instance, but would like to comment on issues and problems with the credit reporting provisions in their interaction with the private sector provisions.

CFA contends that the NPP's do not interact clearly and effectively with Part IIIA of the Act. In our view, Part IIIA of the Act is in conflict with some of the privacy principles and needs urgent reform to ensure those conflicts are rectified.

2.2.1. Use and Disclosure (NPP 2)

The issue of consent (NPP 2.1(b)) to the disclosure of information is discussed in

more detail below. NPP 2.1(a) sets out when information can be disclosed for a secondary purpose. In the case of credit reporting, information is collected from individuals upon application for a loan or other credit. Part IIIA of the Act allows for the person's information to be listed in a credit report when the person is more than 60 days in default. We contend that this is a secondary purpose as the primary purpose for the collection is the assessment of the loan application.

To our knowledge NPP 2.1(a) has never been considered in the context of disclosing information to a credit reporting agency as credit providers always (to our knowledge) obtain the consent of the individual to the disclosure.

The problem here is that the consent is bundled into a group of other (sometimes unrelated) consents in a loan application form. We agree with the comments of the Federal Privacy Commissioner issued in a press release on 23/5/02 on this point.

CFA considers that the bundled consent issue has not been addressed by industry. We recently downloaded standard loan application forms online from major banks and found that in every case bundled consents were used. Examples are attached. It is clear that industry is reluctant to address this issue and this NPP is in need of urgent review to specifically include a principle forcing the unbundling of consents in relation to personal information. We would further add that any principle would require clear disclosure to the individual of their rights in relation to the separate consents.

CFA considers the timing of disclosure as being a critical issue in relation to the interaction of NPP 2 and part IIIA of the Act. It is absolutely essential that disclosure occurs at the relevant time that information is to be disclosed. This is the principle underlying NPP 2.1 (b). Currently, this is not the case with credit reporting of defaults and clearout listings. Often the individual consents to the listing of the default at the time of the application, which is often years before the actual default is listed. At the moment there is no requirement for the individual to be informed when the default is listed. We contend that but for the consent obtained by the credit provider this practice would be in conflict with NPP 2.1.

Based on the casework and advice experience of many CFA members, individuals expect that (and this is a reasonable expectation in our view) s/he will be informed when his/her information is disclosed to a credit reporting agency. Many of our member casework agencies that give advice on credit reporting issues have received calls from individuals that only became aware of a disclosure (for example, a default listing) to a credit reporting agency years after the actual disclosure. This is usually discovered when the individual applies for credit and is rejected.

A more disturbing problem associated with this is that this means identity fraud also can go unnoticed because of the failure to disclose. CFA believes that individuals need to know as soon as possible about any identity fraud so the

relevant authorities can be informed. Further, in some circumstances undetected identity fraud can actually lead to issues of national security if the identity fraud remains ongoing for some years undetected.

Case Study A

P was contacted out of the blue by a debt collector, X Collection, regarding an alleged debt to a major bank that they had bought. He had never had any dealings with either X Collection or the bank in question, but they insisted that it was his debt, citing that it was the same name and the same date of birth. X Collection listed P as a 'clear-out' on his credit report, but refused to investigate whether or not there might have been any errors, and instead told P to contact the bank directly to request copies of the original credit applications.

The Consumer Credit Legal Centre (NSW) Inc. assisted P in his negotiations with the bank, which admitted that they no longer held any documents since it had been 9 years since the account was opened, and agreed to abandon the debt.

However, the process of getting the incorrect listing removed from P's credit reporting was even more difficult. The bank refused to assist because it was X Collection that made the listing, and X Collection took a long time to take steps to correct it.

The above Case Study illustrates the ease with which identity fraud can occur and the adverse consequences of that identity fraud. The whole incident took a long time to resolve and caused P a lot of unnecessary stress. Further, the incorrect 'clear-out' listing would have prevented P from applying for credit successfully. In the current political climate where national security is of such prominence in public debate, it is essential to address issues of identity fraud and privacy and their impact on national security.

2.2.2. Data quality (NPP3)

Firstly, an important NPP principle is data quality (NPP 3). There is considerable concern that a significant number of the listings notified to credit reporting agency Baycorp Advantage Ltd ("Baycorp") are inaccurate. Currently, credit reporting operates on the "honour system". That is, Baycorp accepts a default listing from a credit provider and records the listing on the consumer's credit report without checking the accuracy of the listing by viewing relevant documentation. As a result, the accuracy of credit reporting information is heavily reliant on the systems in place by the credit provider to ensure the accuracy of the information listed.

There are at least 2 cases (which we are aware of) where Baycorp have found that the listings made by certain credit providers are highly inaccurate and accordingly banned those credit providers from accessing the credit reporting

system. Those credit providers are One.Tel and First Netcom Holdings Pty Ltd. In August 2004, 65,000 default listings by One.Tel were removed for being potentially inaccurate because the company did not have proper systems in place to update customer credit default listings once a debt had been paid. This indicates that it is possible to have systemic inaccurate listings from credit providers. It also begs the question as to whether appropriate audits and systems are in place to ensure systemic and one-off inaccuracies do not occur. Given both the One.Tel and First Netcom listing inaccuracies were in place for some years before detection, this would indicate that there are not adequate systems in place to ensure data quality of credit report listings.

2.2.3. Other issues in relation to credit reporting

The very wide definition of credit provider under Determination number 1 means that some very small businesses have access to the credit reporting system. Those small business are not required to comply with the NPP's but even if they are there is some doubt that they have comprehensive procedures in place to adhere to the principles.

Some of the other problems in relation to credit reporting in the context of debt collection are documented in a research report by the Consumer Credit Legal Centre (NSW) titled 'Report in relation to Debt Collection'¹. In addition to a discussion of the poor regulation of the current reportings system, the report documents common problems with respect to credit reporting in the context of debt collection, some of which include:

- Debtor being threatened with having a default listed, or actually having a default listed, as a collection tool, including as a means of locating the debtor;
- being listed for a default, or 'a serious credit infringement' without the debtor's knowledge;
- being listed for very old and/or very small debts;
- inaccuracies occur easily but are difficult to correct;
- insufficient control of access to the system;
- ineffective regulatory oversight;
- non-compliance with information privacy principles.

While CFA has long advocated for a review of the current credit reporting system, we are gravely concerned that some industry players have advocated for the current system to be further extended through positive credit reporting, which provides lenders further access to more information on borrowers.

There are a number of reasons why positive credit reporting should not be introduced. Firstly, the current system does not provide for a standardised way

¹ "Report into Debt Collection", Consumer Credit Legal Centre (NSW) Inc, April 2004, Sydney.

of reporting. Some lenders never list defaults, some are not even aware of credit listing, and some others list and threaten to list very old and small debts. This haphazard and arbitrary nature of the system exacerbates its inherent unfairness and ineffectiveness, and any extension of this system through positive credit reporting would simply compound the problems.

Secondly, we are aware that some lenders are calling for 'positive credit reporting', claiming that it would mean lower interest rates, better risk assessment, and wider access to credit. However, none of these claims are substantiated, and are, in fact, misleading. 'Positive credit reporting' would potentially increase lending, so that even if the 'default rate' is claimed to remain the same, it would increase the number of people who may find themselves in default and suffering financial hardship.

Thirdly, CFA is of the view that there is presently considerable information available to credit providers that they do not use. Our casework experience suggests that credit providers are not using information they already have to hand in risk assessment. In relation to credit cards in particular the following occurs with disturbing regularity:

- Borrowers are given credit limit increases to enable them to borrow amounts that, on the basis of the income stated on their original application form, they clearly can not afford. No attempt is made to determine whether that income has increased. Further, in many cases such application forms clearly state that the borrower is an aged pensioner or a disability support pensioner, making an increase in income highly unlikely.
- Borrowers are given credit limit increases when they are in default on other accounts with the same lender.
- Borrowers are given credit limit increases when they have struggled to meet even the minimum payment on their existing account and this is apparent from even a cursory examination of their account statements.
- Borrowers are granted credit card accounts when they already have multiple cards (or other loans) with the same lender, and the application form does not ask about whether or not they have other cards or accounts and their respective credit limits.
- The lender is also able to check the borrower's other current credit providers, which are listed under the current reporting system.

Further, borrowers usually sign consents as part of their credit application that would readily allow credit providers to make other inquiries to ascertain credit worthiness. These consents are rarely used.

The current listing system is more than sufficient for a credit provider to make a clear credit assessment of applicants if utilised properly, and any extension of the system to include 'positive reporting' would be entirely unjustifiable.

Lastly, positive or full credit reporting is fraught with privacy and security risks. While in theory access to a one-stop source of information for credit providers in assessing credit risk may sound like a good idea, in practice this means that a large database of information about millions of people is maintained by one or more third parties. If the current system is used as a model, these third parties are private sector, profit motivated businesses that effectively sell this information (or access to it) with no particular accountability to the consumers affected by their actions. The addition of more information on this system (potentially a manifold increase in the amount of data) carries with it a number of serious risks:

- the errors that occur in the current system will increase in proportion to the amount of data, magnifying the above effects;
- this data would be potentially very valuable and the temptation to sell it for marketing and other unauthorised purpose could be difficult to resist (if only by unscrupulous employees);
- this concentration of electronically stored data could also be the target of identity fraudsters and other people with illegal intent.

We submit that the burden of establishing sufficient benefit to outweigh these potential risks needs to be very heavy indeed.

The CFA is also concerned that the consumer credit industry is promoting a view about the causes of consumer financial problems that serves the interests of industry. The message appears to be that:

- Industry lending practices have little to do with consumer debt overcommitment;
- Consumer debt overcommitment can be significantly addressed by:
 - Improving consumer financial literacy; and
 - Allowing lenders to access more personal credit information; and
- The sector wants access to more personal credit information so that it can reduce debt overcommitment.

We do not believe that any of the above is true, and we find the current industry enthusiasm for “addressing the problem of credit defaults” to be misleading.

We have seen evidence of self-serving industry responses to these issues in the past, such as a report published by Visa².

More recently we have seen Mastercard publish research that was used to exaggerate claims that extending the credit reporting system would reduce defaults (only one of a number of likely scenarios according to the sourced research) and playing down the impact that “positive” credit reporting could have

² See the consumer response to such a report at http://www.consumersfederation.com/documents/ResponsetoClaimsmadebyVisa_000.pdf

on increasing consumer debt. We are aware of the establishment of two industry forums, or coalitions, raising “concerns” about consumer overcommitment and issues, while promoting “positive credit reporting” and financial literacy as a way of reducing consumer defaults.

There are a number of problems with the accuracy and integrity of the current credit reporting system. Any attempt to extend the system would magnify those problems. Consumer privacy is essential and the integrity of the existing credit reporting system must not be in doubt before considering any proposal to extend that system. Further, there must be a sound justification for attempting such extension and we do not believe any such justification has been made out to date.

Part 3. International issues and obligations

CFA provides no comment in this aspect except for our general preference for Australia to follow international best practice with respect to privacy. We endorse the APF's submission on this point that providing Australians with a 'world's best practice' level of privacy protection in relation to the private sector requires action in several mutually interacting areas:

- Greater cooperation between federal and state and territory governments to achieve consistency and clarity in statutory privacy protection;
- Amendments to the existing provisions of the Act, eg, changes to the NPPs and complaints handling provisions, harmonisation of the IPPs and NPPs, and a winding back and rationalisation of the exemptions and exceptions;
- New statutory tools and mechanisms to support compliance and to assist in building a broader culture of respect for privacy (such as requirements for privacy impact assessments and privacy management plans);
- Greater resources for enforcement and promotion of privacy, including for the OFPC.

Part 4. Recognising individual rights

4.1. Awareness of Rights

4.1.1. Evidence of levels of awareness of privacy amongst the community.

The level of general concern about privacy and some form of 'right' to privacy is quite high, however the awareness of what privacy rights are and how to enforce them is abysmal.

Over 90% of respondents to the OFPC-commissioned research *Community Attitudes Towards Privacy 2004*³ indicated that the following were invasions of privacy:

- A business that you don't know gets hold of your personal information (94%)
- A business monitors your activities on the internet, recording information on the sites you visit without your knowledge (93%);
- You supply your information to a business for a specific purpose and the business uses it for another purpose (93%);
- A business asks you for personal information that doesn't seem relevant to the purpose of the transaction (94%);
- Just 11% of respondents indicated that they had no concerns about giving out information. Clearly these figures indicate an awareness of privacy and concerns that the community's right to privacy is being breached.

Unfortunately the awareness of privacy laws and protections does not match up to the level concern in the community. Only 60% of respondents claimed to be aware of the Federal privacy laws. On its own this poor awareness of the Federal privacy protections would be alarming but efforts to measure what this 'awareness' entails showed only 23% of respondents were able to correctly identify 3 true or false statements regarding privacy protection. Furthermore only 34% of respondents were aware of the existence of the Federal Privacy Commissioner and only 7% said they would take a dispute to the Privacy Commissioner.

The 'true or false' statements are particularly concerning as it indicates there is a significant portion of society who think they understand their privacy rights and are, presumably, acting according to their understanding but are in fact wrong about the rights and ignorant of the remedies available to them⁴.

³ *Community Attitudes Towards Privacy* prepared for the Office of the Federal Privacy Commissioner by Roy Morgan Research 18/6/04.

⁴ A particularly sad example of this is *Ibarcena v Smyth* [2000] FCA 1942 where the applicant withheld information about his social security entitlement which he mistakenly believed he did not need to supply and subsequently lost his rent rebate and was evicted from his public housing.

4.1.2. Impact of such levels on operation of the Privacy and ability of individuals to exercise their rights.

As can be expected this poor understanding of privacy rights leaves people unable to protect themselves and properly assert their rights. During the 2003-4 financial year the OFPC received 1276 complaints and 20,207 hotline enquiries.

There is no indication of what actions, if any, might be taken by those who are unaware of or unwilling to go to the OFPC. A safe assumption is, perhaps, that people simply do nothing not knowing what else to do. However we do know in the area of credit reporting that some people are willing to use expensive private agents to resolve complaints that could have been taken to the OFPC for free. We submit that the preference for private agencies over the OFPC by those who believe their privacy rights have been impinged upon is quite worrisome and undesirable.

An additional concern is the number of people who have a mistaken understanding of their rights in this area. As indicated above a significant number of people enter into agreements and/or supply or refuse to supply information based on false assumptions.

4.1.3. Effectiveness of information provision requirements of the private sector provisions in raising individual awareness of privacy

As indicated the awareness of privacy issues is quite high but the actual understanding of the privacy protections is low. Information provisions do not provide consumers with the basic information they require to make informed decisions or on how to handle complaints. Privacy information, often lengthy and unclear, is disregarded by most consumers.

As such the information provisions do not appear to have had a significant impact on consumer awareness and certainly have not had a significant effect on consumer perceptions of business attitudes towards privacy. OFPC research indicates that 81% of respondents felt that customer details held by commercial organisations are often transferred or sold.

4.1.4. Ways of improving awareness of privacy rights.

As was indicated above almost half the nation has no idea about the existence of Federal privacy laws or their application, and half of those that do know they exist don't know what they are or are wrong about what they are. An improved awareness of privacy rights needs to focus on ensuring that people have a correct understanding of what those rights are.

The OFPC has already made some efforts in an attempt to improve awareness of privacy rights as indicated in their Issues Paper, s 4:

“Individuals cannot best exercise their rights if they are not aware that they have them. Accordingly the Office has sought to give individuals as much information about privacy rights as possible through mediums such as the Office’s information hotline, its web site which includes all its publications as well as answers to Frequently Asked Questions, media comments, media release, speeches, case notes, online compliant checker, multi-lingual web pages, guidelines, information sheets, brochures and the annual report.”

Yet this effort has been unable to reach one in two Australians – clearly something more is needed than mere information provision via the above means to properly raise community awareness. We would submit that greater effort is needed to vigorously and publicly enforce the privacy protections in order that ‘justice is seen to be done’, and we recognise that this is not possible without proper resources. For a more detailed discussion of under resourcing of the OFPC please see Part 4.3 below.

We believe that more work needs to be done in providing access to information when it matters: when information is initially supplied and when problems arise. Improved information notices would go some way to satisfying the former, the latter however is a more difficult matter and warrants serious consideration.

4.1.5. How privacy notices could be improved to raise awareness of privacy rights.

Given the low level of awareness in the community it seems that privacy notices could be improved by requiring a summary of the notice to be provided. Lengthy and complex notices are not useful for people who are unaware of their basic rights and obligations in the area. The notice requirements would also be more useful if they were to apply to dispute situations. A lengthy notice is more relevant, and more likely to be read, by someone in a privacy dispute with an organisation.

4.2. Community confidence that rights are protected

4.2.1. Evidence of levels of community confidence that privacy rights are protected.

There is a great deal of reluctance to provide information, partly stemming from an expectation that information, if provided, will end up being misused. There is a community expectation that information provided is not safe or respected.

There is a belief that most information is traded and sold by business. Only 11% of people are not concerned about providing information to others.

The primary motivator for people not providing information is due to privacy concerns. In the absence of a proactive regulatory response, research indicates that the community turns to its own proactive measures such as leaving information off forms (45% of people sometimes leave information off deliberately), deliberately providing false information and outright refusal to do business (42% of people has refused to business with a commercial entity due to privacy concerns). These measures stop the flow of information in the first place rather than relying on their privacy rights to protect information provided, revealing the lack of confidence in the community.

4.2.2. Ways that the Office can encourage community confidence that privacy rights are protected.

The community cannot have confidence that a right will be protected when they are unaware of what that right is. Information is the first step towards community confidence but, as indicated above, something more than mere information will be necessary to improve confidence. Community confidence would be greatly improved by observing the OFPC actively engaged in protecting the public, and in particular proactively conducting audits and enforcement. Unlike the current reactionary policy and powers of the OFPC there needs to be a move into the public arena to raise community confidence.

Encouraging a better understanding of what privacy rights exist would also go a long way towards encouraging confidence that privacy rights are protected. Where people are misled as to their rights they are also misled as to what the OFPC can do for them. Bringing claims to the Commissioner which only fail would result in the complainant losing confidence in the system.

4.2.3. Ways that organisations can encourage community confidence that privacy rights are protected.

Organisations need to recognise the circumstances and situations that the community is most sensitive to and act to ensure that information is only obtained where necessary and as it is intended by the provider. The primary concerns of the community are personal details (phone number, address etc) and financial details (income, bank accounts etc). When obtaining information about these areas the organisation needs to make clear the need and use of the information and not take advantage of exceptions or perceived loopholes in the NPPs to use that information for what the community would consider a different purpose.

Providing clear information about purpose and use for which information is obtained is vital to improving confidence. Current practices, such as that of 'bundled consent', reinforce the view that organisations will do whatever they want with the information provided, including selling or otherwise misusing it. The community cannot have confidence that their rights will be protected while such practices are the norm.

Public confidence would be improved if organisations were to provide complaint resolution systems. At present the community, generally unaware of the OFPC, is left with no avenue of redress when a problem arises. Complaint resolution services would be an important initial contact point for the community, easing concerns about the provision of information.

The community would also benefit from organisations undertaking privacy audits. Under the current regime there is no proactive action on the part of the OFPC in this aspect, leaving a void in the privacy protection arena. Organisations undertaking this themselves would promote confidence in their use of information and the value of their privacy statements and policies.

4.2.4. Ways to encourage community confidence that privacy rights are protected online.

The onus, both in fact and perception, to provide privacy protection online falls very much onto the community. As a result community confidence in privacy in this area is quite low. This area is widely distrusted (only 9% of people currently trust internet retailers with private information) and has a reputation of privacy abuse. Measures such as:

- Using a Firewall
- Rejecting Cookies
- Using a Spam Filter
- Using Temporary Email Accounts
- Use Software to Protect Anonymity
- Use Anti-Virus Software (which must be regularly updated)

are all necessary and must be employed by the community to protect privacy. The scope of the task is quite large and discriminates against those without the time, education and money to adequately protect themselves. Many simply find the effort too taxing and refuse to enter or do business online.

The only way to encourage confidence in an online environment is to move this onus back onto organisations to respect privacy rights and this can only be done if the OFPC takes proactive action to enforce those rights and undertakes compliance audits to provide the community with a greater confidence that breaches of privacy online will be discovered, investigated and prosecuted. Any effort that reduces the workload of the community when conducting online

dealings would serve to boost confidence in this area.

4.3. Approaches to complaint handling

4.3.1. Complaints

We have had the benefit of reading the draft submission of Professor Graham Greenleaf to the Review and we endorse the submission and recommend his specific submission and their reasoning, including:

- The OFPC should publish online a comprehensive manual of its complaint resolution policies and procedures, and keep it up-to-date.
- The OFPC should reform its procedures for reporting privacy complaints as follows, of which the first and second recommendations are by far the most important:
- *Criteria of seriousness* A set of publicly stated criteria of seriousness on the basis on which a Commissioner's Office decides that a summary of the complaint resolution should be published. The following seven criteria of seriousness are recommended for consideration.
 - a. If a complaint involves the exercise of enforcement powers by a Commissioner, (where a Commissioner has such powers) then this is a strong indicator that it is significant, unless it is merely repetitive of many other complaints. If the numbers are small, all such complaints should be reported to avoid any need for selection.
 - b. Although a complaint is dismissed because it does not involve a breach of IPPs or an Act (or for another reason), it is still significant if its dismissal involved a new interpretation of the law (or its application in a significant new context). It may also be significant in demonstrating that certain practices of public bodies and companies do not breach privacy laws (which may or may not be controversial).
 - c. Although a complaint is settled to the satisfaction of the parties, it is still significant if it involves a new interpretation of the law (or its application in a significant new context). Mediation may involve conditions being imposed on what can be reported, and requirements of anonymity, but is not in itself a reason for non-reporting.
 - d. If a case involves a different example or a remedy, or the provision of a remedy on a scale which is new, it is significant even if no new interpretation of the facts is involved.
 - e. Even if a complaint involves no new interpretation of law, or no new/greater remedy, repeated examples of very important types of complaints are worthwhile. However, separate but similar complaints should not be bundled together, as this confuses the facts of cases and impedes consistent citation mechanisms.
 - f. Findings that are contested by one of the parties to the complaint are usually worth reporting, as they may indicate both significant areas of

disagreement within the community (and so law reform might be desirable), or areas where the Commissioners' interpretation of the law could be questioned.

- g. The criteria of 'seriousness' will change over time, with illustrative complaints being more valuable in the early years of administration of new legislation, even if no significant interpretations or remedies are involved (eg first application in an industry).
- ***Adherence to criteria*** There should be confirmation in each Annual Report that the criteria for reporting adopted by the OFPC have been adhered to. Statistics on the ratio of published summaries to resolved complaints should also be published.
 - ***Naming complainants*** Complainants should be able to elect to be named in reports, except where this is inconsistent with a mediated settlement.
 - ***Naming private sector respondents*** In relation to private sector respondents, the OFPC does not identify respondents in reported cases. The detailed study suggests four criteria which favour identification and five criteria against identification of private sector respondents (it recommends general identification of public sector respondents). These factors may justify a default position of non-identification, provided it is coupled with a readiness in Commissioners to identify where the interests of the complainant, others who may have been harmed by the conduct, or the public interest, justify identification, and subject to any strong reasons which would make identification unfair in the particular case. This is of course subject to the requirements of the Act.
 - ***Level of detail*** Commissioners need to ensure that their complaint summaries contain sufficient detail for interested parties to obtain a full understanding of the legal issues involved and the essential steps in the Commissioner's reasoning leading to their resolution. In relation to remedies, sufficient of the factual circumstances are needed for the adequacy of the remedy to be understood in relation to the seriousness of effect on the complainant, and to allow comparison with potentially comparable complaints (subject to the privacy interests of the complainant).
 - ***'One stop' reporting*** Privacy Commissioners should report on their own websites at least minimal details of appeals and judicial review of their own decisions, and of other Court and Tribunal decisions concerning the Acts they administer.
 - The OFPC should publish, at least annually, statistics of the remedies obtained where complaints are settled with some remedy being provided to the complainant, including statistics of the numbers of cases in which compensation was paid and the amounts of compensation paid.
 - ***Rummery and Federal Privacy Commissioner [2004] AATA 1221 (22 November 2004)*** should be considered as a warning that all aspects of the Commissioner's practices concerning the awarding or negotiating of compensation may need review, and in particular those practices need to be more transparent so as to be susceptible to external comment, criticism

and comparison with awards in comparable jurisdictions (as the AAT attempted to undertake in *Rummery*).

- The lack of merits review of s41 decisions can best be addressed by providing complainants with the rights to insist on a s52 Determination, once there is a right of appeal against s52 Determinations.

The OFPC's approach to handling complaints leaves much to be desired. The CFA's experience is that the complaints handling process is inconsistent, inefficient and lacks transparency. We believe that large numbers of individuals 'drop out' of the system. While some problems are quickly resolved, more complex problems or problems involving less co-operative organisations can be much more difficult to resolve.

In the context of credit reporting, the lack of transparency is particularly evident. In February 2004, 60 people contacted Consumer Credit Legal Centre (NSW) Inc in the context of a survey in relation to debt collection to express their dissatisfaction with the credit reporting system. Of those 60 callers, 29 alleged that their credit reports contained inaccuracies, and a further 23 contended their report was accurate but unfair in the circumstances. In attempting to get the inaccurate or incorrect listing removed, only 6 had made a complaint to the OFPC, and of those, there was only 1 instance where the incorrect listing was removed. CFA is concerned that the OFPC is able to investigate only around 50% of complaints within 60 days, and that sometimes it may even take more than 6 months for a complaint to be even dealt with.

The publicly available guidelines published by Baycorp are very broad. We are often unaware of the internal approach taken by Baycorp in relation to a number of issues. We are therefore unable to identify whether Baycorp (or a credit provider member) has acted outside accepted guidelines, or whether it may need to dispute Baycorp's interpretation of the legislation. This limits our ability to act quickly in relation to consumer complaints. We are also concerned about the lack of information provided to us when we raise issues of what we believe may be a repeated or systemic problem. While our client's problem may be resolved, we are rarely advised whether there has been any response to what might be a broader problem with a particular credit provider. We believe that the OFPC provides advice to Baycorp that goes beyond the Advices published by the OFPC, and that consumer advisors should be aware of what that advice is.

In the case of credit reporting, a complaint is required to be made in writing 3 or 4 times, to Baycorp, then the OFPC, then the credit provider, then back to the OFPC. The OFPC requires written proof of complaint to the credit provider before the OFPC would investigate. This requirement to complain in written form three, or possibly more times cannot be said to be an effective complaint mechanism.

We believe that a complaints procedure which refers the consumer back to the credit provider is unworkable. We also believe that under the Privacy Act and the Credit Reporting Code of Conduct, it is the credit reporting agency's responsibility to undertake any research and liaise with the relevant member when a credit report is disputed by the consumer.

An issue of even more concern is the lack of procedural fairness in the complaints handling procedure. CFA is concerned that the OFPC completes partial investigations of matters and then declines to investigate the matter further pursuant to the Act. Consideration of all the evidence and having an appropriate process in place for the OFPC to make a final determination regarding a complaint is essential to ensure procedural fairness.

Case study B

In or around March 98, C raised with the car yard the issue of a false deposit disclosed on a sales contract. The false deposit allowed the car yard to arrange finance with an unrelated credit provider. A credit provider closely related to the car yard then listed a default for the amount of the false deposit. C made a detailed complaint to the Privacy Commissioner and the Office of Fair Trading ("OFT") in May 98. The Privacy Commissioner initially appeared to investigate the matter on the basis that a debt was owed though no documentary evidence to that effect existed. The Privacy Commissioner asked C to answer a number of questions including whether he had ever been notified by the credit provider that they intended make a listing. This was despite the fact that C's primary complaint was that he had never had any dealings with the credit provider.

The Privacy Commissioner refused to investigate the matter further until the OFT's investigation were finalised, despite the fact that in the interim C's ability to access further credit was severely limited.

In Aug/Sep99, the Privacy Commissioner recommenced investigations when the OFT failed to provide satisfactory compensation to C.

C in the intervening 18 months requested credit on two occasions and on each occasion was refused on the basis of his credit report. In one instant he had the opportunity to refinance his fixed loan contract with an interest rate of 22% to a much lower rate.

The credit provider, despite requests to do so, failed to produce any evidence substantiating the existence of a contract between the parties, the existence of a privacy act authorisation or of any notification to list with the CRAA.

Yet despite this the Privacy Commissioner refused to award compensation, but as the credit provider had agreed to provide staff training and remove the default listing the Privacy Commissioner was not willing to take the matter further. 22 months after the initial complaint, this recommendation was made.

C was so disillusioned with the process that he decided not to take the matter further.

Case study C

Mr D was a new immigrant. His English was poor and he cannot read or write English. On 22/3/01 he entered into a contract to buy whitegoods under a loan agreement. Every month he would pay instalments in person to the retailer as he was not aware of any other means of payment.

On July of that year he moved residence from Adelaide to Sydney. He assumed that he would be able to pay using the same method as the retailer had an office in Sydney. He contacted the retailer and enquired the best means of making payment. He was told that he could only pay in cash in person. As he lived in Sydney he could not do this.

On the 14/12/02 the retailer listed Mr D as a “clearout”. This is similar to a default but with more serious consequences. It is listed for seven years instead of the five years for a default listing. Further it is used to indicate a fraud or a serious credit infringement. Mr D had committed neither fraud nor given indication of an intent to not pay the loan.

Mr D was contacted by a debt collector and then paid the debt in full when he was told how to do this. A year still remained on the loan contract at the time he paid out the loan in full. The listing of a “clearout” remained on his credit report. The retailer was contacted by CCLC and asked to remove the “clearout” listing as it was inaccurate. The retailer refused and a complaint was sent to the Privacy Commissioner. However, the Privacy Commissioner dismissed the complaint under s. 41(2)(a) and declined to investigate the matter.

From the advice and casework experience of many CFA members, the response from the OFPC in Case Study C is a common occurrence. In this respect, many consumers are further frustrated by the process. As illustrated by *X v Commonwealth Agency* [2004] PrivCmrA 4, complaints are often dismissed under s. 41(2)(a) if the Privacy Commissioner is satisfied that the respondent has dealt adequately with the complaint, even if the complainant does not agree. We endorse the position of Professor Graham Greenleaf as espoused in his submission to the Review that in these cases, the Privacy Commissioner should proceed to make a determination under s. 52 of the Act.

4.3.2. Determinations of the Commissioner

A number of CFA member groups were involved in the four representative complaints to the OFPC regarding the TICA Default Tenancy Control Pty Ltd

(TICA) in 2003. The Commissioner's determinations were handed down in April 2004. These determinations highlighted a serious weakness in the Act in relation to the Commissioner's powers when a complaint is substantiated.

The Commissioner found that he did not have the power under Section 52(1)(b) to prescribe how TICA should act, but was limited to making recommendations under section 27. This was a wholly unsatisfactory outcome. It is not enough that the Commissioner can determine that a certain course of conduct not be repeated or continued. What is needed is a clear decision about what is appropriate behaviour. A "recommendatory" power under section 27 is easily subverted or even ignored. This is exactly what has happened in relation to TICA.

For example:

- the Commissioner recommended that TICA "provide access within ten working days" for consumers who lodge a request for access to their personal information by mail (complaint 1, page 18). TICA's interpretation of this recommendation means that consumers with listings will probably wait for 20 days to get details of a listing. Obviously most people will still need to call the 1900 number rather than wait for the postal service. Calls to the 1900 number are charged at \$4.50 per minute. In reality, TICA is making a mockery of NPP 6.4(b) - very few consumers are able to lodge a request for access at no charge.
- the Commissioner recommended that TICA develop a dispute resolution process. Consumers who wish to ring TICA about their dispute, can only do so using the 1900 number. This is not an adequate process.
- the Commissioner recommended that TICA delete history listings after four years. We can find no reference at all to this on the TICA privacy policy on the website.

These are just a few quick examples. (We have not covered in this submission, other ways in which TICA is subsequently breaching the Privacy Act since the determination. Some of these are the subject of individual complaints.)

The end result will be that CFA member groups will continue to make representative complaints, probably in an endless loop. It would be far more helpful for industry and consumers if the Privacy Commissioner could set out the details of appropriate conduct in the first place, both in this case, and more broadly in cases with other organisations in the future. CFA recommends that section 52 be amended to allow the Commissioner to prescribe acceptable courses of conduct.

4.3.3. Ways to improve the community's ability to exercise their rights.

The introduction of the private sector provisions in the *Privacy Act* has had a direct impact on the complaints handling capabilities of the OFPC. The number

of complaints has increased but there has been no substantial increase in funding. It has also meant that the OFPC is no longer able to conduct audits of the public sector.

In February 2004, in answering a question from Senator Ludwig at a hearing of the Senate Legal and Constitutional Legislation Committee, the then Privacy Commissioner Malcolm Crompton said that he was aware of at least 5 pieces of legislation and bills before the Parliament at the time that may have an impact on people's privacy, and that their implementation may result in more complaints to the OFPC⁵. However, in each of the cases, no addition funding to deal with the increase in demand was allocated.

On 5 February 2004, Mr Crompton said in a radio interview with Chris Uhlmann on ABC 666 Canberra that,

“What has happened is that we have had a surprising response to the wider private sector privacy law that came into place a couple of years ago where our complaints workload has gone up five-fold – quintupled. Unfortunately we were only funded for a doubling of the complaints workload before that came into place and we haven’t been given further funding. What we have had to do instead has been to reallocate resources within the office into the complaints area. Got a lot more people doing work in there, but unfortunately it’s not enough to clean up the backlog, so much as to try and stop the backlog getting any longer. So we’re doing our best but there is a very finite resource restraint unfortunately.

“I’d like to be able to offer a better service than I am able to offer. Up to now for example in the areas that directly affect individuals I have literally had to cancel the audit program that the office is empowered under the law to conduct. That means I am no longer able to audit federal agencies or credited organisations for the way they do their business simply because I haven’t got the resources. I have moved them instead into trying to handle the individual complaints that people make, because I think that is the first line that we have to offer to people. But even having done that and reduced resources in other parts of the office unfortunately I haven’t been able to reduce the backlog.”

The resourcing of the OFPC is essential on a number of fronts. Firstly, more resources need to be available in order to improve the complaints-handling capabilities of the OFPC; secondly, the OFPC must be resourced to undertake all of its duties authorised under the Act including the auditing of the public sector; thirdly, as discussed above in Parts 4.1 and 4.2, community awareness is difficult to improve without further resources.

⁵ Senate Legal and Constitutional Legislation Committee Office of the Federal Privacy Commissioner, 16 February 2004, Question 29. The five legislation and bills in question were *Higher Education Support Act 2003*, *Migration Legislation Amendment (Identification and Authentication) Act 2004*, *Spam Act 2003*, *Australian Sports Drug Agency Amendment Bill 2004*, and *Privacy Amendment Bill 2003*.

4.4. Individual's control over personal information

Fundamental to problems in the area of an individual's control over his or her personal information is the Act's distinction between primary and secondary use of the information. While the legislative requirements, including consent, for the use of information for so-called secondary purposes, described in NPP 2, may be clear to those familiar with the Act, the vast majority of individuals fall outside this definition. It is reasonable to contend, therefore, that most individuals applying formally for a particular product or service, may fail to detect any shortcoming in the product or service provider's privacy statements. Such a shortcoming may include a failure to adequately distinguish between primary and secondary purposes in relation to the use of personal information.

In the case of a 'bundled consent', where an organisation typically seeks a blanket sign off to use personal information for multiple purposes, the reality is in many cases: no sign-off, no product/service. In other words, there is a complete absence of choice, let alone informed consent, on the part of the individual.

Further, we are in agreement with the views put forward by Electronic Frontiers Australia Inc ('EFA') in their submission to this Review that 'bundled consent' obtained does not constitute proper consent to use and/or disclose the information for secondary purposes. They state that "Individuals cannot give free and informed consent when they are presented only with broad and/or vague statements concerning possible uses and disclosures, and/or told that services will not be provided if they do not "consent" to the bundle. However, as we see no purpose in using bundles unless the organisation is assuming these result in valid consent, it would appear individuals' personal information is being used and disclosed for purposes for which they did not consent and would not reasonably expect (i.e. in breach of NPP 2.1(a))."

Some organisations utilising such an approach will no doubt argue justification in the interests of business efficiency. However, among the less ethical operators, there may be multiple reasons for seeking an all-encompassing privacy sign-off. In some cases, the motivation is to derive revenue from secondary use of personal data. In the case of some fringe lenders, a bundled consent may support a broader range of options for pursuing a defaulting debtor.

Case Study D

Finance Corp contracted with Mr Purchaser to advance \$1,000 over 2 years at 35% pa over 2 years to purchase a car. After adding an establishment fee of \$1,100, the total amount advanced was \$2,100. Allowing for interest, the amount repayable exceeded \$3,000, significantly in excess of the amount originally contemplated by Mr Purchaser, and, in fact, in excess of his ability to

repay. The credit contract featured the following all-encompassing statement:

I hereby authorise Finance Corp or their agents or employees to discuss any information about my account with anyone.

It is clear that the individual is frequently faced, in contracting for goods or services, with privacy statements that are at best confusing, due either to their verbosity or convoluted terminology, or at worst designed to diminish the individual's ability to protect his or her personal information from misuse. The legislative intent of the NPPs must be strengthened by imposing unequivocal requirements on organisations offering goods and services. Firstly, standards should be mandated for the presentation of privacy clauses relating to positioning in document, type size, line spacing and maximum number of words. Plain English should, of course, be encouraged. Secondly, the wording related to the primary use of collected data must be physically separated from statements relating to the secondary use of data. Thirdly, the individual must be explicitly required to "opt-in" to the use of personal information for each individual non-primary use of personal information that is contemplated by the contract, although in some cases we contend that some secondary uses can be mandatory, e.g. insurance claims investigation, that notice and acknowledgement may be sufficient. Fourthly, any attempt by an organisation to make delivery of a product or service dependent on an individual's consent to use of data for non-primary purposes should be re-examined.

It will be important to ensure that internet applicants are equally protected alongside users of more traditional channels. Implementation of the above requirements for electronic commerce may need specific design focus to ensure maximum effectiveness.

Part 5. Balance of individual privacy interests with business efficiency

5.1. Codes

We agree with and endorse the submissions made by the APF in relation to this topic, namely, that if the Code provisions in Part IIIAA are to remain,

- Codes should be disallowable by Parliament – they amount to subordinate legislation, and it is not appropriate for the Privacy Commissioner to be able to vary the law without parliamentary oversight and approval
- The Privacy Commissioner should be able to initiate a Code – as the HK and NZ Commissioners can and have done.
- The Privacy Commissioner should be required to make public the submission by a code proponent dealing with public consultation and how they have addressed input.
- The Courts should be expressly deemed to have notice of codes in the Register kept by the Commissioner
- The Commissioner should be able to review any decision of a Code adjudicator, not only determinations (s18BI)

5.2. Small business exemption

5.2.1. Whether the benefits of the small business exemption outweigh the disadvantages for business and for individuals.

CFA submits that the small business exemption is ill-conceived and should be removed altogether, as it effectively exempts 94% of all Australian businesses from the application of the Act⁶. Further, some of the most intrusive activities are carried out by very small organisations, and even sole traders, for example, private detectives, debt collectors, internet service providers and dating agencies.

In several key areas we consider that the benefits of the small business exemption do not outweigh the disadvantages for business and for individuals.

The key areas are industries that control large amounts of personal information and that also have access to the credit reporting system. Two particular industries are telecommunications and finance. Notably both industries were traditionally dominated by large companies that would not be classified as small businesses for the purposes of the Act. This is no longer the case and there are now many

⁶ According to information provided by the Department of Employment, Workplace Relations and Small Business to the Standing Committee on Legal and Constitutional Affairs' inquiry into the provisions of the 2000 Bill.

businesses in both finance and telecommunications that would fall under the small business exemption.

Further, the small business exemption, together with the application of section 13B of the Act (related bodies corporate), may provide large organisations the opportunity to evade their responsibility by transferring data collection activity to a smaller entity within their corporate structure.

We consider this to be inappropriate and believe there is a public expectation that strict privacy laws should apply to the sensitive personal information that relates to the purchase of credit and telecommunications services.

5.2.2. Whether the provisions are sufficiently clear about to whom the small business exemption applies.

Although the exemption is reasonably clear it is impossible for a consumer to determine with any certainty whether the small business exemption would apply to the business s/he is dealing with. Given that the majority of consumers have little or only some knowledge of the privacy laws⁷ consumers are not going to be aware of the application of a small business exemption. In effect, it is possible that consumers are dealing with many small businesses on the erroneous assumption that privacy laws apply when this may not be the case.

5.2.3. Any other issues that arise in relation to the small business exemption.

Many consumers deal with banks on the basis that there is some knowledge by consumers that banks are regulated and in particular, there is a general awareness of banker/customer confidentiality.

The concern is that if the consumer default on a loan the bank often sells the debt to a debt collector. If that debt collector has a small business exemption the strict confidentiality the consumer expected when entering into the loan has now been eroded often without their knowledge.

Again, a small business exemption should not apply in these circumstances. A consumer should be able to expect that the privacy rights that consumer had upon entering the loan are preserved for the life of the debt.

⁷ 69% of consumers surveyed had only some or little knowledge of the Privacy Laws see *Community Attitudes Towards Privacy* prepared for the Office of the Federal Privacy Commissioner by Roy Morgan Research 18/6/04 p.19

5.2.4. Is the \$3 million or less threshold for small business still appropriate?

We contend that the small business exemption is not flawed for the reasons set out above, whether it be based on business size or by any other method. There may be room for arguing that some smaller businesses may be exempt from any formal requirements to take particular actions, but the core requirements of the NPPs should apply to all organisations regardless of its size or annual turnover.

All organisations should be required to answer enquiries (NPP 5), and to give access and make corrections on request (NPP6). They should also be held accountable after the event for justifying their collection and use (NPPs 1.1 and 1.2) and for any data quality or security breaches (NPPs 3 and 4).

5.3. Direct Marketing

5.3.1. Appropriateness of the opt out provisions and NPP 2.1(c) generally and different protection that applies to information used for direct marketing according to purpose for which information collected and whether this raises issues for individuals or business.

Direct marketing can be defined as communication directly with individuals rather than through intermediaries, or where the communication supports some degree of interaction between the marketer and the individual, with an emphasis on gathering data about targets, usually with the creation of a database or list of respondents⁸.

In 1997, it was estimated that over 50% of advertising in Australia was spent on direct marketing communications⁹. There is evidence that this is a rapidly growing industry. According to the Australian Direct Marketing Association, in 2003 direct marketing expenditure grew 9%, representing over 32% of all media spending. Between January and December 2001, over 13,800 individual direct mail campaigns aimed at Australian consumers were recorded by AC Nielsen MailTrack¹⁰.

The rate at which this industry is growing can be largely attributed to the different ways in which direct marketing can be conducted with increasing use of new technologies. With the advent of the Internet and e-mail, direct marketers can reach more people than originally able via a telephone or a fax machine. Each

⁸ Clarke, R. (1998) 'Direct Marketing and Privacy', Proc. AIC Conf. On the Direct Distribution of Financial Services, Sydney, 24 February 1998, available at:

<http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html>.

⁹ Edwards, R (1997), quoted in Clarke, R. (1998) 'Direct Marketing and Privacy', Proc. AIC Conf. On the Direct Distribution of Financial Services, Sydney, 24 February 1998, available at:

<http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html>.

¹⁰ Statistics available from www.adma.com.au.

new innovation brings different ways in which the privacy of individuals can be affected.

The NPPs allow for personal information collected to be used for direct marketing in four different ways. The first is where direct marketing is the primary purpose of collection, for example, questionnaires, usually with prize draws as incentive. The second category is personal information that is collected for a purpose (primary purpose), but the organisation wishes to use or disclose it for direct marketing purposes (secondary purpose). In this case, the personal information can be used for direct marketing if the direct marketing is related to the primary purpose, and the individual would reasonably expect the organisation to use or disclose it for direct marketing, then there is no need to obtain the individual's consent¹¹.

The third and fourth ways involve direct marketing as a secondary purpose which is *not* related to the primary purpose or not within the reasonable expectations of the individual. Such information can be used for direct marketing if the individual has consented to the use or disclosure¹². Alternatively, it is permissible if the following 5 conditions are met¹³:

- (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
- (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
- (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
- (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
- (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically.

It is evident that the direct marketing provisions in the NPPs heavily favour business interests over those of consumers. All of the above four categories start with the assumption that personal information can be used for direct marketing, which has been described as 'privacy-unfriendly' or even 'privacy-hostile'.

¹¹ NPP 2.1(a).

¹² NPP 2.1(b).

¹³ NPP 2.1(c).

For the average consumer, the distinctions between information collected for different purposes may not be clear-cut. From applying for a credit card to entering into a draw at the local shopping centre, a person may be providing information to organisations without thinking what the purpose may be, or the implications of their giving that information. Most business activities can be argued to have the secondary purpose of direct marketing. The distinction is too fine to warrant any difference in treatment.

With respect to NPP 2.1 (a), there are some definitional issues. In most business transactions, if not all, marketing can be justified as related to the purpose of data or information collection, even if loosely. More importantly, for the NPPs to be consumer friendly, consumer understanding is essential, and it is difficult to see consumers being able to judge whether or not their personal information being used for direct marketing is related to the original purpose of collection.

With respect to NPP 2.1(c), information can be used for direct marketing if the 5 conditions are met. Businesses start with the assumption that the information can be used for direct marketing, unless the individual actively seeks to 'opt-out'. CFA submits that the 'opt-out' approach is not appropriate, rather, information should be used for direct marketing purpose only if consumers 'opt-in'. This would give the consumers some control over the use or disclosure of their information. There needs to be greater emphasis on putting control back in the hands of the consumers rather than leave them to the whim of business marketing gurus. Consumers must be able to make a conscious choice, and we submit that this can be better achieved with an 'opt-in' approach.

As stated in the Issues paper, the problem with the opt-out approach can also be attributed to its reliance on complaints as the main enforcement mechanism. We contend that this model of compliance is unworkable. Firstly, marketing is such an invasive area of consumers' lives that they have almost come to expect it, and more often than not they may not realise the extent of the intrusion of their privacy or any breach of the privacy laws. Secondly, a breach of privacy may be a great irritation to many, but in most cases a single incident will not cause much tangible damage to warrant the time and effort of making a complaint. Coupled with the problems with the definitions of primary and secondary purpose as outlined above, we question the effectiveness of an approach that relies on consumers being aware of problems and making a complaint as the main enforcement mechanism for the provisions.

5.3.2. Evidence about the incidence of complaints to organisations about the application of 2.1(c).

Case Study E

K went to a website that offered a free property market valuation as she was thinking of selling her property. After filling in an online survey in which she

gave a lot of information about her property, including the standard information such as number of bedrooms, but also the more in-depth details such as the age of the building, size of dwelling, any renovations done, easements and so on. While she thought that this was a lot of detail to give, she assumed that the process was automated by a computer and would not be processed by any actual person. At the end of the survey which took over half an hour, she received a message that said they could not give a valuation in her area (even though it was one of the bigger suburbs in Sydney) and that a "consultant" would contact her soon.

Disappointed and annoyed, she thought nothing more of this. However, about one month later, she got an e-mail from a real estate agent in her area, with her property address and other contact information, asking her to contact him for a discussion about selling her property.

She ignored the e-mail, but a week later she started receiving weekly News Bulletins from the same real estate agent. Apparently she had been added to their mailing list without her consent.

She felt that information about her property, and the fact that she was thinking of selling her property, were highly confidential. Especially because she specifically did not want to deal with a real estate agent in the first place that was why she went to what she thought was an independent evaluation service.

She went back to the website and read the Privacy Policy, which stated in part:

"Persons who supply us with their information on-line will only receive contact from us and/or our consultants with information regarding the enquiry they have placed on-line."

She wrote a letter of complaint to the website address demanding to know why they had breached their privacy policy and asking for details of all the information that they collected about K and her visit to the website, their deletion thereof, and asked them to refrain from selling, or otherwise giving such information to anyone, including any "consultants" affiliated with the website, and any other real estate agents.

K never received a response from them, but the News Bulletins stopped arriving in her e-mail inbox. She wanted to pursue the matter further, but she did not know where to go from there.

In the context of finance brokers, the Consumer Credit Legal Centre (NSW) Inc found in a survey in 2003 that 21% of brokers used cold calling as a method of initiating contact with potential clients. Of 32 caseworkers that reported their clients experienced problems with finance and mortgage brokers, 41% reported that their clients had received unsolicited calls or visits from brokers sometimes

or often.

5.3.3. Business practice in relation to opt out and whether or not organisations are providing it even when not required to do so.

The CFA is aware that the Australian Direct Marketing Association runs a free service for consumers to register on their “Do Not Contact Opt Out” list. The list is a registry of people who have indicated they do not want to receive marketing offers by mail or by telephone, and is available to their members for subscription. To use the service, consumers are asked to fill in an online survey with full details. The service does not directly include removal from current lists, but some marketers who regularly clean their lists using the preference service may remove the consumer from an old list. It will prevent companies from adding the individual’s information to new lists. As the NPPs indirectly require companies to keep a record of consumers who have opted-out (follows from 2.1(c)), according to the ADMA, regular use of this list can help ensure they meet their obligations.

While this seems to be a good initiative, we question the logic in providing a whole lot of personal information to a third party organisation in order to opt-out. The system also has its problems because of the general lack of awareness of the community about the service. Further, the service only caters for the minority of people who do not want to be on any list at all. The CFA submits that most consumers may want selective control, which is not catered for by this service.

5.3.4. Ways of addressing any issues that arise in relation to privacy and direct marketing for individuals or business.

The distinction between primary and secondary purposes is difficult to comprehend, and afford no adequate protection to consumers. Clearly they are designed for the benefit of business efficacy and marketing. Privacy of consumers needs more robust consumer-oriented protection.

Further, it is clear that the ‘opt-in’ approach needs to be adapted in this context. The *Spam Act* is a good example of how it can be done in practice. Marketing communications need to be based on consent or ‘opt-in’ arrangements. NPP 2.1(c) needs to reflect this.

5.4. Compliance

We endorse the APF’S submission’s to the Review on this point. Consumer representations are at the forefront and many of our members see systemic issues

again and again. Individual complaints or even representative complaints are very inefficient. The OFPC should be more proactive in addressing systemic issues.

We agree wholeheartedly that there has been a general failure by the OFPC to recognise the important role of consumer representative groups in the implementation of the regulatory regime. The OFPC should give priority to dealing with systemic concerns raised by consumer representatives, and other third parties including the media, without requiring a specific complaint to be brought, involving major resource effort and delays. Most importantly, this is also a view shared by the Federal Attorney-General, Philip Ruddock. When asked in a radio interview by Chris Uhlmann on ABC Canberra on 11 February 2004 if the Privacy Commissioner had enough money to do his job, he replied:

“Well the question you have to look at is whether or not he is getting an artificially large load of cases because there is a systemic problem. I mean he is claiming there’s been a five-fold increase in complaints and that what has happened is that his budget has only been doubled. I mean there has been a substantial increase in resources that the Privacy Commissioner has received, but you have to look at the question, and we would do this in a budget context, about whether more resources are appropriate given just that there’s an increase in the number of complaints, or whether you’d look behind the complaints and ask yourself whether there’s a systemic problem that needs to be addressed.”

Further, in CFA’s experience there is no culture of compliance and there is no incentive for respondents to complaints to correct systemic flaws. In most cases, the worst outcome for a respondent is that they must amend the records. With respect to credit reporting, the cost of dealing with a small number of complaints is apparently less than the cost of ensuring the data is accurate in the first place.

As outlined above in Part 4.3, there is a lack of information provided to us when we raise repeated or systemic problems. While the specific complainant’s problem may be resolved, we are rarely informed whether there has been any response to what might be a broader problem with a particular respondent. We understand that the OFPC sometimes provides advice to major respondents that goes beyond anything made public - consumer advisers should be aware of what that advice is.

We are also strongly of the view that the OFPC audit powers should apply to private sector organisations and compliance with the NPPs.

5.5. Business efficiency and private sector contracting

CFA is concerned that the privacy standards are not upheld when an organisation contracts out certain functions of the organisation. This is particularly potent combined with the small business exemption (discussed

above in Part 5.2).

Part 6. Balance between privacy of individual and other social interests

The CFA has made substantial submissions in this aspect above, for example in the context of credit reporting.

Part 7. NPPs generally

No further comments. See submissions above.

Part 8. Matters that have an impact on the operation of the private sector

No further comments. See submissions above.

Part 9. Any other issues

9.1. Abuse of the Privacy Act as an excuse

We agree with the submissions of the APF with respect to this. It seems that organisations are all too willing to use the 'privacy laws' as an excuse when it suits them but as discussed throughout this submission there are also many instances when they do not comply with the Act or the NPPs.

We endorse APF's view that there should be some sanction to act as a deterrent against wilful misrepresentation of the Act, for example, empowering the OFPC to issue or require 'corrective statements' to be published at the expense of the organisation, and repeated misinformation should attract more severe sanctions.