Submission by
Australian Consumers' Association

to
House of Representatives Standing Committee on Legal and Constitutional Affairs

Inquiry into Privacy Amendment (Private Sector) Bill 2000

Introduction

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 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.

The Australian Consumers' Association (ACA) has long advocated and anticipated legislative privacy protection for Australian consumers – we regard such legislation as a necessity. We consider that the Privacy Amendment (Private Sector) Bill 2000 makes a good start in defining the principles that should govern the regulation of the collection and use of personal information in Australia. However we feel that the framework for the operation of privacy protection that is established has flaws. In our opinion, these flaws will undermine the good intentions of the Bill. The self-regulatory regime is not defined as a co-regulatory model capped by an Authority with real power, serviced by an complaints office of last resort, but rather as a weak default system and fractured self-regulation.

We also have a number of concerns with the details of the Bill, which will be presented below. We feel that from an initial goal of simple legislation meshed with a self-regulatory regime, the shape of the Bill embodies considerable complexity based in legislative exception and definition, which will ultimately make the operation of privacy protection opaque and uncertain. In its current form it will fail to adequately protect the privacy of individuals. We make specific recommendations for the improvement of the Bill from the consumers' perspective. These are summarised at the end of the document. Some of these recommendations are made in a cascading way, that is our primary recommendation may be followed by a further recommendation 'in any event', which applies if our prior recommendation fails.

The Framework

The ACA does not object in principle to the self-regulatory approach to the protection of privacy in Australia. However, it is our view that the proposed method has several basic flaws that will undermine the objective of effective privacy protection for Australian consumers. These basic flaws then serve to compound concerns about details of the Bill, since the margin for tolerance of the need for interpretation and flexibility is smaller. The flaws as seen by the ACA are:

1. The absence of an enforcement authority, to monitor the operation of the self-regulatory system. In the event of self-regulatory failure, such an authority should be able to take action, both to redress offences against individuals, but also to issue credible penalties against industry players. **Recommendation:** That the Bill be amended to provide penalties which apply to serious breaches.[1]
2. The lack of an appeal mechanism weakens the proposed structure of self-regulation. Such a mechanism could review various code authority decisions and create precedents relating to the interpretation of various elements of the Act. In the absence of such an appeal process, it our concern that the multiple aspects of the Bill which involve interpretation of what is reasonable, impracticable, practicable, serious and imminent, frivolous, excessive, related etc will come to be treated in different ways by different Code Authorities. This will in all likelihood evolve what might be termed 'privacy silos', where the experience of privacy protection for a consumer will vary from sector to sector, and even within sectors as different industry associations create Privacy Codes.
   Recommendation: That the Bill be amended to provide a mechanism by which decisions of industry Code Authorities can be appealed to the Privacy Commissioner, and that his findings become precedents for other Code Authorities. At the least a system of review under which the Privacy Commissioner can issue binding interpretation should be provided.[2]
3. The Commissioner has uncertain powers to approve, audit and discipline recalcitrant players. **Recommendation:** The Commissioner should be empowered, and indeed required, to undertake self directed research, and own motion investigations and audits, extending across the full range of code administration schemes, not just the default scheme.[3]
4. ACA has serious concerns relating to health provisions in the Bill. These relate partly to the self-regulatory approach of the legislation and partly to the way in which the health provisions are framed. As currently stated in the provisions, the consumer's right of access to their health records are substantially undermined by the range of 'exceptions' that can be used to deny access to health records. The right of access in this Bill is substantially weaker than that under legislation which gives consumers a right of access to public sector health records (Freedom of Information legislation and, in the ACT, the Health Records (Privacy and Access) Act 1997.

   In light of the fact that the Government has canvassed the possibility of a new national identifier for health records that will link records across private and public sectors, it is important that all health records have consistent rules with regard to access and the right to correct incorrect details. Given the new uses for health information, there are strong arguments for removing these parts of the Bill and dealing with them in specific health legislation so that right of access will be treated consistently across the private and public sectors. Alternatively, health should be dealt with as an enforceable code that is directly supervised by the Privacy Commissioner rather than voluntary codes administered by industry groups.

1
2
3

Recommendation: That health provisions **either**; be removed from this Bill and dealt with under a separate code **or** that health is dealt with as an enforceable code directly supervised by the Privacy Commissioner.[4]

Recommendation: That the provisions in relation to access to records be amended to be more consistent with public sector legislation that provides access to health records (See suggested amendments in relation to Principle 6.1 and 6.2.).[5]

Recommendation: That privacy provisions in relation to third party access to identified health records be amended so that access is only available to de-identified data where consumer consent has not been obtained (Principles 10.3 and 10.4).[6]

Definitions

A number of terms used in the Bill are critical to the successful operation of privacy protection, but are undefined. In the context of the Bill their meaning cannot be left to commonsense, and without the appeal or review system referred to above to ensure consistency of interpretation across the 'privacy silos', in our opinion the Bill needs to deal with them explicitly. The key terms, and the issue requiring definitional clarification are:

Use

Particularly relevant in relation to the use or otherwise of personal information by related bodies corporate (Clause 13B), where conditions on 'use' are the primary safeguard for the sharing of data across organisational boundaries. A key issue is 'non-use' – that is ensuring that screening of data by the supplying organisation is covered. This addresses the problem of *redlining*. Has your data been used is a related entity requests only customers who generate a certain margin, or who live in certain post-codes. The excluded consumer may then have been denied a market offering or advantage by entity B, based on their personal information supplied to entity A, without B having ever used it in any commonsense way. Is it a use of information simply to *store* it, in other words to possess it? Does reading or browsing a record imply use of it, or is it only when action results that use eventuates? What crystallises use? It seems useful to borrow some of the words quoted in the Explanatory Memorandum to the Bill from the EU directive Article 6 relates to the fair processing of personal data.

Recommendation: That *Use* of personal information is defined as any operation or set of operations performed on personal data including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, including but not limited to the participation of that information in a decision to do or to omit to do, an act, and the utilisation of that information in any act.[7]

Purpose

4

5

6

7

Does the purpose of information change if it is computer processed in some way? For example if purchasing records are correlated in such a way as to infer information about the health status of an individual, what is the purpose of the information derived – indeed has it been collected?
Recommendation: *Purpose* is defined to ensure that information applicable to an individual that has been derived from personal information collected from the individual is protected to the same degree in terms of purpose and the operation of the other NPPs.[8]

Collection
Is data collected if it is derived by means of a correlation or inference from other data held by an organisation? If so, what is the purpose of the information?

Has data that has been updated or corrected been collected? If so, is only the data items so processed been collected, or does the whole record (undefined) inherit this property? Indeed, do related records (the record set) pertaining to the individual also inherit the collection at this point? If not, where is the boundary drawn?

These questions are germane to the notion in 16C(3) that National Privacy Principles 2 (Use and Disclosure) and 6 (Access and Correction) will not apply to existing data. Does the process of updating a data item move it into the privacy regime or not, that is, is it then collected after the operation of the section? There are obvious practical difficulties that then apply if for instance, address information is changed, but date of birth is not. An organisation would then be tasked with providing different coverage under the privacy principle to various items in a common record. On the other hand, if collection were to be denied for an update, then the existing data records will never move into the purview of the privacy regime, creating a much more sweeping exemption than may have been intended.
Recommendation: That *Collection* be defined to include update and correction of data items as well as original *de novo* collection, and that the collection of one item in a data set (defined as the set of data records related to a particular individual in an organisation) should then be deemed to have been collected at that point.[9]

Other terms that may, if left undefined create unintended consequences in a loosely managed self-regulatory system, are **Disclose, Consent, Store.**
Recommendation: The terms *Disclose, Consent,* and *Store* should all be given a defined meaning in the Bill.[10]

DNA information
DNA information should not be assumed to be privacy sensitive and potentially commercially useful only in the context of health. As an additional item of definition, we feel it should be included as ***sensitive information*** in its own right. **Recommendation:** Alter Amendment 27 to include, at section (a) item (x) DNA and genetic profile information of an individual.[11]

8
9
10
11

Related bodies corporate

The wide definition of organisations within which information can be freely disclosed is of concern. The effective extension of organisations to include entities related as defined under the Corporations Law makes the umbrella impossibly large for effective protection of consumers' rights to opt out of information sharing. It is also presumable that the broad definition cuts two ways, and "a request to the organisation not to receive direct marketing communications" will be required to be honoured throughout large corporate webs.

Confining the boundary to legal entities only may be commercially difficult, but an explicit test of the consumers' expectation, or a test of related or similar business activities using similar language to 2(a)(ii) would be appropriate. This would confine the net of free exchange to an extent more acceptable for consumers.

Recommendation: For Amendment 52 change the proposed clause 13B to read

(1) Despite paragraphs 13A(1)(a) and (b), each of the following acts or practices of an organisation that is a body corporate is not an ***interference with the privacy*** of an individual limited to the extent that it does not exceed the reasonable expectations of that individual:[12]

Small Business Exemption

The proposed definition of small business in Clause 6D as a business that has an annual turnover of $3,000,000 or less in a nominated *test month* will make it complex and variable for a consumer to judge if a business should be meeting privacy standards or not.

Section 6D(4)(c) uses the test that a small business is not eligible to be treated as one if it "discloses personal information about another individual to anyone else for a benefit, service or advantage". This embodies a peculiar logic – a small business does not need privacy control until a consumer can prove that it needs privacy control.

The ACA considers that a positive obligation on all business to observe proper privacy practice is more effective, and hence our **Recommendation** is that the exemptions for small business should be removed from the Bill.[13]

Political Parties

The ACA is sensitive to the needs for democratic processes to be protected. At the same time, it would be seem to set something of a double standard for political parties to be granted a global and sweeping exemption. If nothing else, it will contribute to the formation of special purpose micro-issue parties. We feel that the issues specific to any threat to democratic processes be identified, and any necessary exemption be granted specifically. Otherwise, it would seem best policy for political parties to set a best practice example in the management of personal information from their constituents.

Recommendation: The exemption for political parties should be refined to reflect actual concerns related to possible infringements on democratic processes.[14]

12

13

14

Application of National Privacy Principles

National Privacy Principles 2 (Use and Disclosure) and 6 (Access and Correction) should apply to existing data, although perhaps only after a phasing in period. The current drafting in clause 16C(3), that they do not, is in our view a serious deficiency in the Bill as proposed.

As discussed above, the question of the definition of collection is very material to this issue, but in any event, our **Recommendation** is that clause 16C(3) be changed to read:

National Privacy Principles 2 and 6 apply in relation to personal information collected before the commencement of this section only after a period of six months has passed from the commencement of the operation of this section.[15]

These points about definition of organisational scope and the use of existing data impact on consumer interests on a broader level than the individual. They will also function to confer commercial advantage to incumbent holders of consumer data, especially those in large corporations. This will potentially constitute a barrier to entry in some markets, and therefore confront consumers with the impost of less diversity and higher prices, while having a two-tier system of privacy protection.

Privacy Codes

The ACA considers that given the potential weakness of the proposed self-regulatory regime, the Privacy Codes approved by the Privacy Commissioner should also be subject to parliamentary review. To that end, we **recommend** that a section be inserted around Section 18BC thus:

> **18xx Privacy Codes disallowable**
>
> A Privacy Code under this Division is a disallowable instrument for the purposes of section 46A of the *Acts Interpretation Act 1901*.[16]

We are also concerned that the Privacy Commissioner can charge fees for access to the Register of privacy codes. We **recommend** that Section 18BG (4) be amended such that

> (4)Fees:
>
> (a) The Commissioner may not charge fees for making the register available to the public;
>
> (b) The Commissioner may charge fees providing copies of, or extracts from, the register, provided such fees are not unreasonable or excessive.[17]

We also **recommend** that Section 80E(4) referring to the Register of determinations of public interest be similarly amended.[18]

15

16

17

18

Comment on Schedule 3 - National Privacy Principles

Collection

The imperative of defining 'collection' was described earlier in this document.

Use and disclosure

Section (c), the Direct Marketing "secondary purposes" exception is convoluted and complex. The issue of the 'practicality' of seeking consent is entirely within the gift of the marketer. Once again, the 'privacy silo' problem of the self-regulatory model arises, making it almost certain that various Code Authorities will determine this question differently. Is the test of practicality money? How much money is impractical, in other words, how much is a consumers privacy worth?

Indeed, the Explanatory Memorandum to the Bill suggests 'Impracticability' in relation to the same form of words in relation to Health information in the following section (d) "must be something more than the incurring of some expense or effort in seeking an individual's consent to the use or disclosure. For example, an organisation may be unable to locate the present whereabouts of the individual for the purpose of seeking their consent, despite making reasonable efforts to contact that individual."

At the very least we **recommend** explanatory wording regarding 'Impracticability' given for Health information also apply to the Direct Marketing exemption.[19]

Our primary **Recommendation** is to define the direct mail specific provisions, section (c) using an opt-in approach:

> An organisation will not send unsolicited mail, except:
>
> (i) to persons with whom the organisation has a pre-existing business, professional or personal relationship, or
>
> (ii) to persons who have previously indicated their consent to receive mail from the organisation.[20]

In any event the qualification to principle 2, that at:

> 2.1(c)(iv) the organisation gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications;

gives a consumer a once only automatic chance at opting-out. It is our recommendation that the direct marketer should be required to offer an opt-out opportunity at each approach.

Our **Recommendation** is that 2.1(c)(iv) be redrafted to read:

> (iv) the organisation gives the individual the express opportunity at each time of contact to express a wish not to receive any further direct marketing communications; [21]

19

20

21

Section (d), the health information "secondary purposes" exception has particular problems. The same issues of practicality of seeking the consent of individuals apply here as to Direct Marketing, but with far greater possibility of consumer detriment.

We note the asymmetry of power accorded the Organisation in Note 2 to Subsection 2.1, which states that "Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it." Notwithstanding the explanatory notes about the interpretation of practicality in this context, the Individual is not given this same absolute right of control over their information as is bestowed on the organisational custodian of their data. We regard this as a fundamental flaw, perpetuating the power imbalance consumer face, which this Bill should remedy by giving consumers such control.

Our primary **Recommendation** regarding use of health information of an individual under the Health exception to the Use and Disclosure principle is that clauses 2.1(d) (ii) and (iii) be removed altogether, and clauses 2.1(d) (i) be amended to read:

> (i) it is impracticable for the organisation to seek the individuals consent before the use or disclosure, in which case only de-identified data may be provided.[22]

In any event, our **Recommendation** is that if the health information of an individual is used under the Health exception to the Use and Disclosure principle that an additional clause be inserted to the effect that:

> (iv) the individual must be informed within a reasonable time, in a way which does not intrude further on their privacy, of the use of their health data under the exceptions. granted by this Section.[23]

Data quality

The 'privacy silo' problem of the self-regulatory model makes it almost certain that various Code Authorities will determine the question of what 'reasonable steps' are differently.

Data security

Given that the primary purpose is the reason the consumer gave permission for the collection of the data in the first place, it our **Recommendation** that clause related to Data security 4.2 be amended to read:

> 4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the primary purpose for which it was collected.[24]

22

23

24

We would further **recommend** an additional clause relative to Data security 4.3:

> 4.3 An organisation must take steps to destroy or permanently de-identify personal information on the request of the individual to whom that personal information relates.[25]

Openness

We **recommend** that Openness Section 5.1 contain an additional clause, stating

> The organisation must take reasonable steps to make the document available to the general public.[26]

Access and correction

We feel the same test should apply to health information as general personal information, particularly since the test for general personal information is stronger. The same test should be applied to both. Therefore we **recommend** that Access and correction Section 6.1(b) be deleted.[27]

In addition, we feel it is important that the individuals have guaranteed access to their own data. We **recommend** that Access and correction Section 6.1(a) altered to read:

> (a) in the case of health information providing access would pose a serious threat and imminent to the life or health of any individual other than the individual to whom the information relates.

In any event, 6.1(b) should be similarly amended in the event that it is retained.[28]

Principle 6.1(c) states that access can be denied if "providing access would have an unreasonable impact on the privacy of other individuals." It should either be removed or the term 'unreasonable' defined much more clearly. In a self-regulatory environment the use of undefined terms will lead to differing and inconsistent interpretation and application of the principles. Similarly, 6.1(d) the request for access is frivolous or vexatious. Again in a self-regulatory environment these terms need to be much more clearly defined, or removed.

We **recommend** 6.1(c) and (d) should either be removed or the terms unreasonable, frivolous or vexatious defined much more clearly.[29]

We **recommend** 6.1(i),(j),(k) and 6.2 should not apply to health records and should be removed in relation to health information.[30]

A number of the exceptions, Section 6.1(f) in particular, embody a power asymmetry between the consumer and the organisation. In the particular case of section 6.1(f), providing access would reveal the intentions of an organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations. Some

25
26
27
28
29
30

providers to hide information from consumers who, providers believe, wish to complain could use this clause. We **recommend** clause 6.1(f) should be removed.[31]

The organisation is made the judge of what will prejudice negotiations as opposed to information that the consumer may need simply to negotiate on an equitable basis. Consumer complaint is likely then to be heard by an industry Code Authority. This situation illustrates the need for an appeal mechanism to a neutral authority that can make binding rulings. In any event we **recommend** inserting an Access and correction clause to the effect that:

> 6.7 If the organisation does not provide the individual with access to the information because of one or more of paragraphs 6.1 to 6.7 (inclusive), the organisation must agree to the use of mutually agreed arbitrator to review the reasonableness of decisions and actions by the organisation. Any ruling of the arbitrator shall be binding on the organisation.[32]

We do not believe consumers should be charged for access to their own information. Therefore we **recommend** that Access and correction clause 6.4 be amended to read:

> 6.4 An organisation must not charge for providing access to personal information.[33]

Sensitive Information

The operations of some non-profit organisations reach deeply into the lives of some consumers. We **recommend** that paragraph 10.1(d)(i) dealing with Sensitive information dealt with a non-profit organisation be amended to read:

> (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its non-commercial activities;[34]

Sections 10.2 and 10.3 dealing with health information are flawed in a similar way to the health information aspects of Use and Disclosure.

The only exception should be where law in an Act other than this requires the information. We do not feel the consumers' interests should be overridden by professional bodies, however constituted or conducted. We **recommend** section 10.2 dealing with Sensitive information, should be amended by removing paragraph 10.2(b)(ii).[35]

Health information should not be obtained about consumer without their consent for the purposes of "management, funding or monitoring". We **recommend** section 10.3 dealing with Sensitive information, should be amended by removing paragraph 10.3(a)(iii).[36]

31
32
33
34
35
36

We are very concerned by the question in 10.3(c) of who judges in the specific instance "purpose cannot be served by the collection of information that does not identify the individual or from which the individuals identity cannot reasonably be ascertained". It is in the very act of interpreting purportedly authoritative codes and guidelines that significant uncertainty for consumers arises. Therefore we **recommend** that paragraph 10.3(c) be deleted, and that de-identified data only be allowed for research relevant to public health or public safety purposes.[37]

We also reiterate our primary **Recommendation** regarding use of health information of an individual under the Health exception to the Use and Disclosure principle in this context, so clauses 10.3(d) (ii) and (iii) be removed altogether, and clauses 10.3(c) be amended to read:

> (c) it is impracticable for the organisation to seek the individuals consent to the collection, in which case only de-identified data may be collected.[38]

In any event, our **Recommendation** is that if the health information of an individual is used under the Health exception to the Sensitive principle that an additional clause be inserted 10.3(e) to the effect that:

> (e) the individual must be informed within a reasonable time, in a way which does not intrude further on their privacy, of the use of their health data under the exceptions. granted by this Section.[39]

In any event, we **recommend** that Sensitive information clause 10.4 be amended by removing the words "take reasonable steps to", so that the clause reads:

> 10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must permanently de-identify the information before the organisation discloses it.[40]

37

38

39

40

Summary of Recommendations

In summary therefore, the ACA considers that the following actions be made in relation to the Privacy Amendment (Private Sector) Bill 2000:

Recommendation 1: That the Bill be amended to provide penalties which apply to serious breaches.

Recommendation 2: That the Bill be amended to provide a mechanism by which decisions of industry Code Authorities can be appealed to the Privacy Commissioner, and that his findings become precedents for other Code Authorities. At the least a system of review under which the Privacy Commissioner can issue binding interpretation should be provided.

Recommendation 3: The Commissioner should be empowered, and indeed required, to undertake self directed research, and own motion investigations and audits, extending across the full range of code administration schemes, not just the default scheme.

Recommendation 4: That health provisions **either**; be removed from this Bill and dealt with under a separate code **or** that health is dealt with as an enforceable code directly supervised by the Privacy Commissioner.

Recommendation 5: That the provisions in relation to access to records be amended to be more consistent with public sector legislation that provides access to health records (See suggested amendments in relation to Principle 6.1 and 6.2 .)

Recommendation 6: That privacy provisions in relation to third party access to identified health records be amended so that access is only available to de-identified data where consumer consent has not been obtained (Principles 10.3 and 10.4).

Recommendation 7: That Use of personal information is defined as any operation or set of operations performed on personal data including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, including but not limited to the participation of that information in a decision to do or to omit to do, an act, and the utilisation of that information in any act.

Recommendation 8: Purpose is defined to ensure that information applicable to an individual that has been derived from personal information collected from the individual is protected to the same degree in terms of purpose and the operation of the other NPPs.

Recommendation 9: That *Collection* be defined to include update and correction of data items as well as original *de novo* collection, and that the collection of one item in a data set (defined as the set of data records related to a particular individual in an organisation) should then be deemed to have been collected at that point.

Recommendation 10: The terms *Disclose, Consent,* and *Store* should all be given a defined meaning in the Bill.

Recommendation 11: Alter Amendment 27 to include, at section (a) item (x) DNA and genetic profile information of an individual.

Recommendation 12: For Amendment 52 change the proposed clause 13B to read

(1) Despite paragraphs 13A(1)(a) and (b), each of the following acts or practices of an organisation that is a body corporate is not an ***interference with the privacy*** of an individual limited to the extent that it does not exceed the reasonable expectations of that individual:

Recommendation 13: that the exemptions for small business should be removed from the Bill.

Recommendation 14: The exemption for political parties should be refined to reflect actual concerns related to possible infringements on democratic processes.

Recommendation 15: is that clause 16C(3) be changed to read:

National Privacy Principles 2 and 6 apply in relation to personal information collected before the commencement of this section only after a period or six months has passed from the commencement of the operation of this section.

Recommendation 16: that a section be inserted around Section 18BC thus:

18xx Privacy Codes disallowable

A Privacy Code under this Division is a disallowable instrument for the purposes of section 46A of the *Acts Interpretation Act 1901*.

Recommendation 17: that Section 18BG (4) be amended such that

(4)Fees:

(a) The Commissioner may not charge fees for making the register available to the public;

(b) The Commissioner may charge fees providing copies of, or extracts from, the register, provided such fees are not unreasonable or excessive.

Recommendation 18: that Section 80E(4) referring to the Register of determinations of public interest be similarly amended.

Recommendation 19: At the very least explanatory wording regarding 'Impracticability' given for Health information also apply to the Direct Marketing exemption.

Recommendation 20: to define the direct mail specific provisions, section (c) using an opt-in approach:

An organisation will not send unsolicited mail, except:
(i) to persons with whom the organisation has a pre-existing business, professional or personal relationship, or
(ii) to persons who have previously indicated their consent to receive mail from the organisation.

Recommendation 21: that 2.1(c)(iv) be redrafted to read:

(iv) the organisation gives the individual the express opportunity at each time of contact to express a wish not to receive any further direct marketing communications;

Recommendation 22 (Primary): regarding use of health information of an individual under the Health exception to the Use and Disclosure principle is that clauses 2.1(d) (ii) and (iii) be removed altogether, and clauses 2.1(d) (i) be amended to read:

(i) it is impracticable for the organisation to seek the individuals consent before the use or disclosure, in which case only de-identified data may be provided.

Recommendation 23 (In any event): is that if the health information of an individual is used under the Health exception to the Use and Disclosure principle that an additional clause be inserted to the effect that:

(iv) the individual must be informed within a reasonable time, in a way which does not intrude further on their privacy, of the use of their health data under the exceptions. granted by this Section.

Recommendation 24: that clause related to Data security 4.2 be amended to read:

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the primary purpose for which it was collected.

Recommendation 25: an additional clause relative to Data security 4.3:

4.3 An organisation must take steps to destroy or permanently de-identify personal information on the request of the individual to whom that personal information relates.

Recommendation 26: that Openness Section 5.1 contain an additional clause, stating The organisation must take reasonable steps to make the document available to the general public.

Recommendation 27: that Access and correction Section 6.1(b) be deleted.

Recommendation 28: that Access and correction Section 6.1(a) altered to read:

(a) in the case of health information providing access would pose a serious threat and imminent to the life or health of any individual other than the individual to whom the information relates.

Recommendation 29 (In any event): 6.1(b) should be similarly amended in the event that it is retained.

Recommendation 30: 6.1(c) and (d) should either be removed or the terms reasonable, frivolous or vexatious defined much more clearly.

Recommendation 31: 6.1(i),(j),(k) and 6.2 should not apply to health records and should be removed in relation to health information.

Recommendation 32: clause 6.1(f) should be removed.

Recommendation 33: inserting an Access and correction clause to the effect that:

6.7 If the organisation does not provide the individual with access to the information because of one or more of paragraphs 6.1 to 6.7 (inclusive), the organisation must agree

to the use of mutually agreed arbitrator to review the reasonableness of decisions and actions by the organisation. Any ruling of the arbitrator shall be binding on the organisation.

Recommendation 34: that Access and correction clause 6.4 be amended to read:
6.4 An organisation must not charge for providing access to personal information. **recommend** that paragraph 10.1(d)(i) dealing with Sensitive information dealt with a non-profit organisation be amended to read:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its non-commercial activities;

Recommendation 35: section 10.2 dealing with Sensitive information, should be amended by removing paragraph 10.2(b)(ii).

Recommendation 36: section 10.3 dealing with Sensitive information, should be amended by removing paragraph 10.3(a)(iii).

Recommendation 37: that paragraph 10.3(c) be deleted, and that de-identified data only be allowed for research relevant to public health or public safety purposes.

Recommendation 38 (Primary): regarding use of health information of an individual under the Health exception to the Use and Disclosure principle in this context, so clauses 10.3(d) (ii) and (iii) be removed altogether, and clauses 10.3(c) be amended to read:

(c) it is impracticable for the organisation to seek the individuals consent to the collection, in which case only de-identified data may be collected.

Recommendation 39: is that if the health information of an individual is used under the Health exception to the Sensitive principle that an additional clause be inserted 10.3(e) to the effect that:

(e) the individual must be informed within a reasonable time, in a way which does not intrude further on their privacy, of the use of their health data under the exceptions. granted by this Section.

Recommendation 40: that Sensitive information clause 10.4 be amended by removing the words "take reasonable steps to", so that the clause reads:

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must permanently de-identify the information before the organisation disc
loses it.