



Australian Government
Office of the Privacy Commissioner

Level 8 Piccadilly Tower
133 Castlereagh Street
Sydney NSW 2000
GPO Box 5218
Sydney NSW 2001

P +61 2 9284 9800
F +61 2 9284 9666
privacy@privacy.gov.au

Enquiries 1300 363 992
TTY 1800 620 241
www.privacy.gov.au

ABN 13 152 473 225

Ms Margaret Fleming
Program Manager
Communications Alliance Limited
Level 9/32 Walker Street
North Sydney NSW 2060

Dear Ms Fleming,

Review of the Telecommunications Consumer Protection Code (C628:2007) and Guidelines (G631:2009)

Thank you for your letter of 1 July 2010 drawing the Office of the Privacy Commissioner's (the Office) attention to the scheduled review of the Telecommunications Consumer Protection (TCP) Code and Guidelines. I understand that the TCP Code regulates the behaviour of telecommunications service providers in areas including billing, credit management, complaint handling, customer contracts and the information contained in advertising.

The Office has considered the Issues Paper on the Review of the TCP Code and Guidelines released by Communications Alliance Limited (Communications Alliance) and welcomes the opportunity to provide initial comments to Communications Alliance at the commencement of the TCP Code and Guidelines review process. The Office hopes that these comments, which are attached to this letter, will provide a useful starting point for the consideration of privacy issues within the context of the TCP Code and Guidelines. The Office would like to continue engaging with Communications Alliance and the TCP Code Review Steering Committee and Working Committees as the review process progresses.

If you wish to discuss any of the issues raised in this letter, please do not hesitate to contact Ms Leife Shallcross on 02 6247 4388.

Yours sincerely

Mr Timothy Pilgrim
Deputy Privacy Commissioner
14 July 2010

The Office of the Privacy Commissioner's comments on the scheduled review of the Telecommunications Consumer Protection (TCP) Code and Guidelines

The Office of the Privacy Commissioner (the Office) has considered the Issues Paper on the Review of the TCP Code and Guidelines (Issues Paper)¹ released by Communications Alliance Limited (Communications Alliance) and welcomes the opportunity to provide initial comments to Communications Alliance at the commencement of the TCP Code and Guidelines review process. The Office hopes that these comments will provide a useful starting point for the consideration of privacy issues within the context of the review of the TCP Code and Guidelines.

Privacy and the consumer protection framework

The Office acknowledges the public interest in promoting an environment where Australian consumers of telecommunication services are adequately protected against unfair business practices through an effective consumer protection framework. Further, the Office supports having the TCP Code and Guidelines provide consumers with clear, easy to understand and readily accessible advice on their rights and obligations. This will help enhance accountability measures and improve transparency and public confidence in the way in which the telecommunications industry transacts with consumers and handles consumer complaints.

The Office is of the view that the protection of personal information should be seen as a key element in any telecommunications consumer protection framework. At some stage, most Australian consumers will have their personal information handled by telecommunications service providers when they transact for the supply of telecommunications goods and services. It is therefore important to ensure the TCP Code and Guidelines have adequate privacy protections in place, including appropriate accountability mechanisms, for the collection, use and disclosure of a consumer's personal information.

Adopting this approach in the TCP Code and Guidelines recognises that individual consumers have a legitimate interest in controlling the dissemination of the personal information they provide to telecommunications providers. It also ensures that consumers are made aware of the ways in which their personal information will be handled so that, to the greatest extent possible, individuals maintain a measure of control over their personal information.

¹ The Issues Paper released by Communications Alliance Limited at the same time as comments on the TCP Code and Guideline Review was sought can be found at http://www.commsalliance.com.au/data/assets/word_doc/0006/23937/TCPC-Review-Issues-Paper-Public-Comment-July-2010.doc.

Technological change in the telecommunications industry

The Issues Paper suggests the TCP Code and Guidelines may warrant further consideration *within the context of the pace of technological development in the telecommunications industry.*² The Office is of the view that industry codes, such as the TCP Code, provide the telecommunications industry with the ability to respond more quickly to areas of potential concern arising out of the introduction of new and convergent technologies. Accordingly, the Office is supportive of the review *considering whether the TCP Code should incorporate any additional consumer protection mechanisms that arise out of the development of particular new technologies.*

The inherent nature of new or emerging technologies may make it problematic to attempt to forecast how they may impact on information handling practices and privacy more broadly. New technologies in the telecommunications industry may often greatly enhance the speed, efficiency and scope of information flows within and between organisations as well as in society generally. New technologies may permit the collection of ever greater amounts of information and make it far easier to copy, distribute and aggregate that information.

From a privacy perspective, the underlying stages of the information lifecycle are likely to remain the same: that is, information will be collected, stored, used, disclosed, corrected where necessary and, at some stage, destroyed. However, it may be the case that the new and convergent technologies may generate a need for organisation to review and clarify their privacy practices to ensure consumers are aware of the new ways in which their personal information may be handled.

To reduce the potential complexity for consumers in this area the Office suggests consideration be given to organisations using layered privacy policy. Layered privacy policies can be seen as an effective means of communicating the most important details about the personal information handling practices of an organisation in clear, easy to understand and readily accessible language. Further, it can assist in making sure consumers are fully informed about the collection, use and disclosure of their personal information. This may be particularly beneficial in circumstances where the provision of certain services to consumers, such as the download of applications for mobile devices, involves third parties.

Mobile Premium Services Code

The Office notes the suggestion in the Issues Paper that the review consider whether to incorporate the Mobile Premium Services Code into the TCP Code.³ The Office agrees it may be beneficial to give further consideration to this proposal during the review process. Generally, the Office believes there are benefits to consumers in

² Page 4 of the Issues Paper.

³ Page 4 of the Issues Paper.

having clear, easy to understand and readily accessible advice on their privacy rights located in one central document.

Outstanding issues from the 2007 TCP Code review process

During the TCP Code review process in 2007 the Office made a number of suggestions regarding improvements that could be made to the TCP Code. The Office set out these areas of concern in a letter to Ms Jeni Floyd, Compliance and Policy Manager of Communications Alliance, in July 2007. Communications Alliance indicated to the Office some of these issues would be prioritised for further review. A copy of the Office's letter to Ms Floyd is letter is at **Appendix A**.

Appendix A

Our reference: PO7-20-1
Your reference: C628:2007/G631:2007

Ms Jeni Floyd
Compliance and Policy Manager
Communications Alliance
PO Box 444
MILSONS POINT NSW 1565

Dear Ms Floyd

ACIF/ Communications Alliance Telecommunications Consumer Protections Industry Code C628:2007 and Guideline G631:2007

Thank you for your email of 15 May 2007 inviting comments on the draft *Telecommunications Consumer Protections Industry Code (the Code) and Guideline G631:2007 (the Guideline)* as part of the public consultation process. The annexure to this letter explains my Office's view on those aspects of the Code and Guideline that raise privacy related issues.

In general, the Office found that where privacy matters are dealt with in the Code, they are consistent with the obligations expressed in the Act. However, there are some inconsistencies between definitions in the Code and those in the Act which the Office submits could mislead consumers and suppliers; and some provisions that should be amended to ensure that they accurately reflect the obligations under the Act. Our detailed comments are set out in the attachment.

Again, thank you for providing my Office with the opportunity to comment on this Code during its development. If you wish to discuss any of our comments please contact Brian Kent on (02) 9284 9773 or by email to briankent@privacy.gov.au or Linda King on (02) 9284 9820 or by email to lindaking@privacy.gov.au.

Yours sincerely

Karen Curtis
Privacy Commissioner

July 2007

OPC Comments on Proposed Telecommunications Consumer Protections Industry Code and Guideline

Acronyms, Definitions and Interpretations (Code Chapter 2 / Guideline Chapter 2)

Definition of 'consumer' – Code 2.2 p8; Guideline 2.2 p8

The definition of 'consumer' in the Code is not materially the same as that found in the definition of 'credit' in s. 6(1) of the *Privacy Act 1988* (the Act) (or in the Uniform Consumer Credit Code). The definition in the Code is as follows:

Consumer

means:

- (a) *a person who acquires a Telecommunications Product for the primary purpose of personal or domestic use; or*
- (b) *a business or non-profit organisation which at the time it enters into the Contract:*
 - (i) *does not have a genuine and reasonable opportunity to negotiate the terms of the Contract; and*
 - (ii) *has or will have an annual spend with the Supplier which is, or is estimated on reasonable grounds by the Supplier to be, no greater than \$20,000, other than a person acquiring a Telecommunications Product for resale.*

The definition of 'credit' in the Act states:

' a loan sought or obtained by an individual from a credit provider that is intended to be used wholly or primarily for domestic, family or household purposes'.

As noted above, the definition in the Code provides that it be 'for the primary purpose of personal or domestic use' and includes a 'business or non-profit organisation' seeking credit for not more than \$20,000. Unless the Code or guideline says explicitly that the definition in the Code is not the same as in the Act, it may mislead service providers into undertaking (consumer) credit reporting in situations not permitted by Part IIIA.

Under Part IIIA part (b) of the definition of 'Consumer' in the Code would be considered commercial credit and therefore not attracting the various obligations and privileges outlined in Part IIIA. Under Part IIIA the credit provider is permitted to check the individual's consumer credit report but is required not only to serve a notice under s.18E(8)(c) but also obtain the consent of the individual which in most cases will need to be in writing (s.18K(1)(b) and 18K(1A)). Furthermore, Part IIIA does not permit the default listing of commercial loan on an individual's consumer credit file held by a credit reporting agency.

The Office previously raised this issue with the Communication Alliance in May 2005 when the C541:2003 Credit Management Code was reviewed, stating that:

Part IIIA of the Privacy Act regulates consumer credit and, in a very limited number of situations, commercial credit. This has the practical effect of prohibiting suppliers from

reporting a payment default on an individual's consumer credit file where, for example, a small business commits a payment default.

The code does not ... draw a distinction between consumer and commercial credit.

The Office considers that given the restrictions in Part IIIA of the Privacy Act on accessing personal information from individual's consumer credit files, ACIF may wish to consider including a clear definition of credit. This change may assist suppliers in understanding their obligations under the Privacy Act.

This issue was raised again in March 2007 when the Office reviewed the initial draft of the Consumer Protection Code. This issue could be addressed by amending the definition.

Definition of 'fraud' – Code 2.2 p8; Guideline 2.2 p10

The definition of 'fraud' in the Code is not the same as that used in the definition of 'serious credit infringement' in s6(1) of the Act. The non-payment for services is deemed to be fraud in the Code whereas in practical terms, because of the way credit reporting agencies allow such notifications to be reported, under Part IIIA of the Act only someone whose behaviour indicates they are intentionally avoiding payment of a debt would be considered as having committed a serious credit infringement. The Code defines fraud as follows:

Fraud

means dishonestly accessing or using a Supplier's Services, or attempting to do so, with the intent of:

- (a) deceiving the Supplier;*
- (b) not paying for the Services; or*
- (c) securing unlawful gain.*

This issue could be addressed by a note to the Code or Guideline.

Definition of 'security bond' – Code 2.2, 7.22 pp 12, 44; Guideline 2.2 p12

The Code, at clause 7.2.2, refers to Suppliers requiring Customers to provide a security bond. The definition of security bond in the Code states that it will be lodged to mitigate an assessed risk. It is important to note that a security bond is unlikely to be considered credit because the security bond is pre-payment for a set amount of expenditure to be offset against the proposed debt. If this is the case credit reporting may not be permitted by Part IIIA

The Office provided the following comments about this issue in March 2007 when reviewing the Consumer Protection Code:

In some circumstances, the requirement for a customer to provide a security bond as a condition of supply of the service may not amount to credit. For example, this could reasonably occur where the monetary amount of the security bond and any cap on proposed expenditure is set at the same amount at the beginning of the relationship. Under these circumstances it is doubtful that there is a contract, arrangement or understanding that a person is permitted to defer payment of a debt, or to incur a debt and defer its payment (in terms of the definition of a loan in s.6(1)) because the security bond is pre-payment for a set amount of expenditure to be offset against the proposed debt.

The definition of security bond states that it is to mitigate an assessed risk. If, however, there is no cap placed on bills at the commencement of the relationship, the security bond is merely notional. If this is the case, it may not be permissible for a supplier to undertake a credit check with a credit reporting agency as part of the credit assessment process when the relationship commences and no security bond is in place. It would also not be permissible to conduct credit checks at later stages of the relationship (for example as part of the 'credit management' process) where a security bond and cap are in place.

The Office suggests that these issues should be resolved and the aspects redrafted in the Code chapter and the guideline as they have the potential to mislead suppliers about their obligations in relation to conducting credit reports in these circumstances. The Office believes that this is an issue that warrants serious consideration, and potential substantive change to the content of the Telecommunications Consumer Protections Code Project

This issue could be addressed by a note to the Code or Guideline.

Credit Assessment – Code 2.2, 7.1 pp 8, 44; Guideline 2.2 p8

The Office made the following comments in March 2007 when reviewing the Consumer Protection Code:

The issue is that the Code does not express that there are some instances where a credit check through a Credit Reporting Agency (CRA) is not lawful, such as when a customer has a preference for a pre-paid service or where the customer is not certain which service he or she wishes to take up and merely wants more information. Suppliers may not necessarily understand when they are not permitted to conduct credit checks. The draft Code chapter and Guideline do not draw these issues out and may potentially mislead suppliers. This creates a risk management issue for suppliers and has the potential to lead to complaints being lodged with the Office.

As previously, we reiterate our view that these clauses need to be reviewed and made clear that a credit check with a CRA must only be made if supply is to be on the basis of credit.

Essentially, a credit check is unlawful in circumstances where the individual has a preference for a pre-paid service or is uncertain which service to take up and merely wants more information. This issue could be addressed by a note to the Code or Guideline.

Customer Information on Prices, Terms and Conditions (Code Chapter 4)

Providing information- Code 4.3.1, p24

The Office provided comments regarding this issue when the revised Billing Code (ACIF C542:2003) was released for public consultation in September 2006. It was our view that the provisions regarding access misstated NPP 6 because it indicated that access can be refused if the request is onerous, which is not one of the exceptions provided for under NPP 6.1(a)-(k). We note that the clause has now been amended to state that refusal of access is subject to the nature of the request and relevant legislation, and a note has been added to paragraph 4.3 of the Guideline referring to NPP 6.

The Office submits that these amendments may not be sufficient and recommends that the Code should expressly state that access cannot be refused unless one of the exceptions in NPP 6.1(a) to (k) applies.

This issue could be addressed by changing clause 4.3.1.

Billing (Code, Chapter 6)

Access Code 6.1.2 p34

The Code purports to deny access to billing information if it 'is not relevant to the Customer's use of the related good or service'. It is the Office's view that under NPP 6.1 there is no provision for withholding access founded on a subjective belief of the supplier that the information is irrelevant to the customer's use of the related goods or services. Our comment to Communications Alliance in September 2006 in relation to the Billing Code ACIF C542:2003 stated:

There are a number of exceptions under the NPPs that limit access to (say) the personal information of the individual themselves (NPP 6.1c) or to information that pre-dates the introduction of the NPPs and is no longer being used or disclosed and further that NPP 6.4 allows that reasonable charges can be levied for providing individuals with access. The meaning and intended effect of this clause is unclear, and may invite ambiguity.

Consequently, the Office requests clarification specifically of what 'not relevant to the Customer's period of use' means? This could be construed as way of fettering customers' rights of access to their own personal information which is from an earlier period. Such a restriction would not be consistent with the NPPs.

This issue could be addressed by changing the clause to require that Code members must provide an individual with access to personal information it holds about them unless one of the exceptions set out in NPP 6.1(a) to (k) applies. The Office suggests that this clause could refer to the requirements under NPP6.4 that allow organisations to levy a reasonable charge for providing access to personal information, subject to the charge not being excessive or being applied to the lodgement of the request, NPP6.4(a)-(b). Further the Code should state that where requests for access are refused in terms of the provisions under NPP6.1(a)-(k), individuals must be told why their request has been refused (NPP6.7).

Credit Management (Code Chapter 7)

Refusal to supply service - Code 7.2.6 p45

The Office made the following comments to Communications Alliance in March 2007 regarding Chapter 9 Credit Management which is part of the draft Telecommunications Consumer Protections Code and the Office considers that the issue raised is still valid. The Code does not state the obligations of credit providers to provide access to credit reports held by them. Instead it asks the individual to contact the credit reporting agency. The Code should mention that access is available to their credit files held both by the supplier in its role as a credit provider and the credit reporting agency (NPP 6.1 and s18H(2)).

The Office suggests that the accuracy of this clause could be improved by expanding it to include the requirements that exist s18H(2) as well as the requirements that exist under NPP6 (Access and Correction). Under s18H(2), a credit provider who has possession of a credit report, has an obligation to provide an individual with access to their report without charge.

The Office suggests that these requirements should be included in the clause 9.2.6 as well as at the relevant section in the Guideline.

This issue could be addressed by changing the clause to state that:

A credit provider in possession or control of a credit report containing personal information concerning an individual must take all reasonable steps to ensure that the individual can obtain access to that report.

Customer Transfer (Code Chapter 8)

Telemarketing –Code 8.2 p58

The Office received advice from the Australian Communications and Media Authority (ACMA) On 29 May 2007 stating that clauses 4.1.1 and 4.1.4 of the existing Customer Transfer Industry Code C546:2006 relating to telemarketing were no longer necessary due to the commencement of the Do Not Call Register (DNCR) Act and particularly the *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls Standard) 2007*. In light of this amendment we suggest that clause 8.2 could be removed.

Complaint handling (Code Chapter 9)

Charges - Code 9.3.1 p63

In relation to the Complaint Handling Industry Code C547:2004, the Office raised with Communications Alliance during July 2004 its concerns that it was inappropriate for suppliers to charge a fee for handling the substance of privacy complaints. As previously noted, this position is consistent with the Australian Standard on Complaint Handling (AS 4269) which states in part that ‘...complaint handling shall be at no charge to the complainant, subject to statutory requirements’.

This issue could be addressed by changing the clause or making a note to the Guidelines.

General Guidelines (Guideline Chapter 3)

Complying with the law - Guideline 3.4, p.17

There are two typographical errors:

- The current determination is entitled ‘*Credit Provider Determination No. 2006-04 (Classes of credit providers)*’ which took effect on 1 September 2006 (not ‘*Determination 2003 No.1... dated 14 February 2003*’), and which expires 31 August 2011. (As a general rule, the Office suggests that where the Code and Guideline refer

to Determinations made by the Privacy Commissioner, the expiry date of the Determination should be included).

- The reference to the provisions of Part IIA of the Privacy Act should be ‘Part IIIA’