



Ms Christiane Gillespie-Jones
Manager – Policy and Regulation
Communications Alliance Ltd
Level 9/32 Walker Street
North Sydney NSW 2060

Dear Ms Gillespie-Jones

Comments on the draft revised Telecommunications Consumer Protections Code

Thank you for your email of 25 October 2011 advising the Office of the Australian Information Commissioner (OAIC) of the release of the draft revised Industry Code: *Telecommunications Consumer Protections Code* (DR C628:2011) (TCP Code).

I understand that the revised TCP Code proposes enhanced obligations on suppliers in all areas governed by the TCP Code, especially in relation to advertising, the provision of pre-sales product information, the introduction of mandatory usage notifications, and complaint management. It also establishes a body to oversee the new framework for compliance with the TCP Code.

The OAIC has considered the draft revised TCP Code released by Communications Alliance Limited (Communications Alliance) and welcomes the opportunity to provide comment as part of the public consultation process. The OAIC supports the simplification of language and structure of the TCP Code and the inclusion of an introductory statement to assist both suppliers and consumers to better understand and interpret the TCP Code rules. However, the OAIC considers there is scope to provide further information and stronger privacy protections in the revised TCP Code, especially given that the *Telecommunications Consumer Protections Guideline* (G631:2009), which provided supporting information about compliance with the *Privacy Act 1988* (Cth) (Privacy Act), will be withdrawn upon registration of the revised TCP Code.

The OAIC is encouraged that several issues which were raised in previous consultations have been resolved in the revised TCP Code; but notes there remain some inconsistencies which have been highlighted in the attached comments.

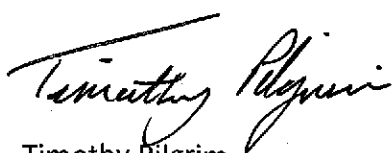
Many of the OAIC's comments relate to consistency between the TCP Code and the obligations contained within the Privacy Act and the binding Credit Reporting Code of Conduct. The OAIC notes that the Government intends to amend the Privacy Act, including the credit reporting provisions, in response to the Australian Law Reform Commission's report: *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108)¹. The

¹ See <http://www.alrc.gov.au/publications/report-108>.

Government has released exposure draft legislation, including draft Australian Privacy Principles which will apply to agencies and organisations and replace the National Privacy Principles and Information Privacy Principles that currently apply under the Privacy Act, as well as draft credit reporting provisions that will replace the current obligations in Part IIIA of the Privacy Act.² Additionally, the Government has indicated that industry will be required to develop a new binding Credit Reporting Code of Conduct, to be approved by the Information Commissioner.³

If you wish to discuss any aspect of these comments please contact Diana Weston on 02 9284 9631.

Yours sincerely



Timothy Pilgrim
Australian Privacy Commissioner

24 November 2011

² The exposure draft legislation was referred to the Senate Finance and Public Administration Committee. The exposure draft legislation and the Committee's reports are available at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/index.htm.

³ See *Enhancing National Privacy, Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (October 2009) (First Stage Response), response to ALRC Recommendation 54–59, p 103 available at <http://www.dpmc.gov.au/privacy/reforms.cfm>.

The Office of the Australian Information Commissioner's comments on the draft Telecommunications Consumer Protection Code (C628:2011)

The Office of the Australian Information Commissioner (OAIC) has reviewed the draft revised *Telecommunications Consumer Protections Industry Code* (DR C628:2011) (TCP Code) released by Communications Alliance Limited (Communications Alliance) and welcomes the opportunity to provide comments to Communications Alliance as part of the public consultation process.

The OAIC 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. The OAIC also considers that the protection of personal information should be a key element in any telecommunications consumer protection framework, and hopes these comments may assist in enhancing the existing privacy protections in the revised TCP Code.

CHAPTER 2 – DEFINITIONS AND INTERPRETATION

Definitions of 'Consumer' and 'Customer' – TCP Code 2.1, p 12

In earlier submissions to Communications Alliance, the OAIC has indicated that the definitions of 'Consumer' and 'Customer' in the TCP Code may be confusing when read in conjunction with Part IIIA of the *Privacy Act 1988* (Cth) (Privacy Act) which regulates consumer credit reporting.

The OAIC has previously identified that the definition of 'Consumer' in the TCP Code includes a 'business or non-profit organisation' seeking credit for not more than \$20,000, which would be considered commercial credit under Part IIIA of the Privacy Act. Under the Privacy Act, commercial credit does not attract the same obligations and protections as consumer credit. Therefore, Suppliers relying on the definition of 'Consumer' in the TCP Code may mistakenly undertake credit reporting in circumstances not permitted by Part IIIA of the Privacy Act. For example, the Privacy Act does not permit a supplier to list an overdue commercial credit account (a default) on an individual's consumer credit information file held by a credit reporting agency (CRA).⁴ Further, a supplier is only able to obtain an individual's consumer credit report from a CRA, in relation to an application for commercial credit with the individual's specific agreement.⁵

To assist Suppliers in understanding their obligations under the Privacy Act, the OAIC suggests that the revised TCP Code should clarify when a Supplier may undertake consumer credit reporting and include a definition of 'credit' which clearly distinguishes consumer and

⁴ See s 18E of the Privacy Act.

⁵ See s 18K(b) of the Privacy Act.

commercial credit. Ideally, such definitions should be consistent with the definitions contained within the Privacy Act.

In relation to the definition of 'Customer' in the TCP Code, the OAIC notes that in the original TCP Code (C628:2007), the term Customer is defined as:

a residential or small business customer who:

(a) is party to a Contract; or

(b) is eligible under the criteria set by a Supplier to enter into a Contract

to acquire a Telecommunications Product, other than for the purposes of resale.

A reference to a Customer includes a reference to their Authorised Representative.

In the revised TCP Code, the definition has been changed to:

a Consumer who has entered into a Customer Contract with a Supplier.

A reference to a Customer includes a reference to their Authorised Representative.

The OAIC considers that the amendment to the definition of Customer to include the term Consumer may further confuse Suppliers about their obligations under the Privacy Act as described above. The OAIC suggests that the original definition of Customer is preferable and less likely to mislead Suppliers.

Definition of 'Fraud' – TCP Code 2.1, p 14

The OAIC has previously commented that the definition of 'Fraud' in the TCP Code is inconsistent with the definition of 'serious credit infringement' in s 6(1) of the Privacy Act. Specifically, the non-payment for services is deemed to be Fraud in the TCP Code whereas in practical terms, because of the way CRAs allow such events to be reported, under Part IIIA of the Privacy Act only someone whose behaviour indicates they are intentionally avoiding payment of a debt would be considered as having committed a serious credit infringement.

This issue is addressed in part in the *Telecommunications Consumer Protections Guideline* (G631:2009) (Guideline); however, the OAIC understands that the Guideline, which accompanied the original TCP Code, will be withdrawn upon registration of the revised TCP Code. Given that the Guideline will be withdrawn, the OAIC suggests that this inconsistency should be clarified in the revised TCP Code.

Definition of 'Security Deposit' – TCP Code 2.1, p 18

Clause 6.5 of the revised TCP Code describes the rules that apply in the event that a 'Security Deposit' is required by a Supplier. The OAIC submitted in March and July 2007⁶ that it was not clear in the original TCP Code and Guideline that in some circumstances, the requirement for a customer to provide a Security Deposit as a condition of supply of the service may not amount to credit as defined by s 6 of the Privacy Act. The uncertainty arises because the Security Deposit appears to be a pre-payment for a set amount of expenditure to be offset against the proposed debt. If this is the case, it may not be permissible for a Supplier to undertake a credit check with a CRA (i.e. obtain a copy of the individuals' consumer credit report) as part of the Credit Assessment process when the relationship commences.

A Supplier is only permitted to obtain a credit report from a CRA in relation to an individual's application for credit.⁷ 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. The OAIC suggests that this issue should be clarified in clause 6.5 of the revised TCP Code.

CHAPTER 4 – CONSUMER SALES, SERVICE AND CONTRACTS

Personal Information – TCP Code 4.6.3, p 40

The OAIC welcomes the new provisions in the revised TCP Code relating to Personal Information. In particular, the OAIC supports the requirement that a Supplier must:

ensure that a Customer's Personal Information is protected from unauthorised use or disclosure and dealt with by the Supplier in compliance with all applicable privacy laws.

The OAIC is also encouraged by the new obligations on Suppliers regarding the storage and security of Customers' Personal Information, including the undertaking of an effective remedy in instances where the TCP code is breached. In the OAIC's view, these obligations will provide some degree of certainty for Consumers about how their personal information will be handled, and will also facilitate a more consistent understanding among Suppliers about their responsibilities to protect Personal Information.

The OAIC considers that this provision could be enhanced if there was an additional obligation on Suppliers when collecting Personal Information from a Consumer that they take reasonable steps to ensure Consumers are made aware of:

- (a) the identity of the organisation and how to contact it; and

⁶ See Karen Curtis, Privacy Commissioner to Jeni Floyd, Communications Alliance, Office of the Privacy Commissioner's Comments on Telecommunications Consumer Protection Industry Code (C628:2007) and Guideline (G631:2007), July 2007; and Linda King, Deputy Director Policy to Jeni Floyd, Communications Alliance, Office of the Privacy Commissioner's Comments regarding Billing and Credit Management sections of Telecommunications Consumer Protection Industry Code, March 2007.

⁷ See s 18K(1) of the Privacy Act.

- (b) the fact that he or she is able to gain access to the information; and
- (c) the purposes for which the information is collected; and
- (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
- (e) any law that requires the particular information to be collected; and
- (f) the main consequences (if any) for the individual if all or part of the information is not provided.

These requirements reflect the protections afforded in National Privacy Principle 1, in Schedule 3 of the Privacy Act.

Additionally, the OAIC considers clause 4.6.3 would be further strengthened by informing consumers of the obligation of suppliers to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date. Suppliers should also be obliged to provide consumers with access to their personal information and to correct information if the consumer establishes that the information is not accurate, complete and up-to-date. These requirements reflect the protections outlined in National Privacy Principles 3 and 6.

CHAPTER 6 – CREDIT AND DEBT MANAGEMENT

Credit and Debt Management – TCP Code 2.1, 6.1, 6.2 and 6.9, pp 12, 50–51, 59

The OAIC supports the simplified approach to the regulation of the provision and management of credit in connection with the supply of Telecommunications Products in the revised TCP Code, including the amendment to the definition of 'Credit Assessment' at 2.1 (p 12) of the revised TCP Code, so that it now means:

the process by which a Supplier determines the level of credit to be provided by it (if any) to a Consumer.

However, the OAIC notes that the Guideline which accompanied the original TCP Code provided detailed information about Credit Assessments, in particular, in relation to obligations under the Privacy Act. Given that the Guideline will be withdrawn upon registration of the revised TCP Code, it would be prudent to include some of this information in the revised TCP Code. The OAIC recommends that the revised TCP Code includes a requirement that any Credit Assessment complies with a Supplier's obligations under the Privacy Act and the Credit Reporting Code of Conduct in relation to the Consumer's Personal Information. Additionally, the revised TCP Code could replicate some of the examples that were included in clause 3.4 of the Guideline such as the requirement in s 18E(8)(c) of the Privacy Act which provides that a credit provider must not give to a CRA personal information relating to an individual if the credit provider did not, at the time of, or before, acquiring the information, inform the individual that the information might be disclosed to a CRA.

In its submission on the original TCP Code in March 2007, the OAIC commented that the TCP Code does not express that there are some instances where a credit check through a 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. This issue does not appear to have been addressed in the revised TCP Code. The OAIC suggests that Chapter 6 of the revised TCP Code clarify when Suppliers are not permitted to conduct credit checks.

The TCP Code provides timeframes for providing some information to CRAs; for example clauses 6.9.1(e), 6.9.1(f) and 6.9.1(g). The Privacy Act and Credit Reporting Code of Conduct also provide timeframes for the reporting of information to CRAs. For example, s 18F(3) of the Privacy Act requires information to be provided to CRAs 'as soon as practicable' in particular circumstances. Additionally, clause 2.5 of the Credit Reporting Code of Conduct requires a credit provider to 'immediately' advise a CRA that it has previously provided inaccurate information to a CRA.

While clause 6.9.1(f) of the TCP code explicitly recognises that the Privacy Act and Credit Reporting Code of Conduct specify timeframes perhaps similar recognition should be provided in other parts of the TCP Code. For example, clauses 6.9.1 (c) and 6.9.1(g) could provide that where the Privacy Act or Credit Reporting Code of Conduct specifies a shorter timeframe, that shorter timeframe applies. This may be of particular relevance if the timeframes in the Privacy Act and Credit Reporting Code of Conduct are amended as part of the privacy law reform process.

CHAPTER 8 – COMPLAINT HANDLING

Complaint handling charges – TCP Code 8.1, pp 72–75

The OAIC welcomes the amendments to the rules regarding complaint handling processes in the revised TCP Guidelines. In particular, the OAIC supports that the revised TCP Code emphasises that a Complaint handling process must be 'free of charge' unless one of the exceptions applies. The OAIC also supports the removal of some of the exceptions included in the original TCP Code and commends the new requirement that the 'Supplier must tell the Consumer about the options for external dispute resolution before levying any Charge'.

However, as previously submitted⁸, the OAIC considers that it is inappropriate for Suppliers to charge a fee for handling the substance of privacy complaints. The OAIC recommends

⁸ See Timothy Pilgrim, Deputy Privacy Commissioner to Margaret Fleming, Communications Alliance, Office of the Privacy Commissioner's comments on the scheduled review of the Telecommunications Consumer Protection Code (C628:2007) and Guidelines (G631:2009), 14 July 2010; Karen Curtis, Privacy Commissioner to Jeni Floyd, Communications Alliance, Office of the Privacy Commissioner's Comments on Telecommunications Consumer Protection Industry Code (C628:2007) and Guideline (G631:2007), July 2007; and Linda King, Deputy Director Policy to Jeni Floyd, Communications Alliance, Office of the Privacy Commissioner's Comments regarding Billing and Credit Management sections of Telecommunications Consumer Protection Industry Code, March 2007.

that the revised TCP Code should make explicit that privacy complaints will not be subject to a charge even when a Consumer requests access to information held by the Supplier about the Consumer which was collected by the Supplier more than 2 years prior to the date of the request or when the free provision of the information in the form requested is inconsistent with the usual business processes of the Supplier.