

Our Ref: SLD:NK:5467

30 July 2010

The Manager
Communications Alliance Ltd
PO Box 444
Milsons Point NSW 1565

Dear Sir/Madam

SUBMISSIONS FOR REVIEW OF THE MOBILE PREMIUM SERVICES CODE (C637:2009)

Axis Legal Pty Limited (**Axis Legal**) is pleased to have the opportunity to submit to Communications Alliance Ltd (**CommsAlliance**) its review on the *Mobile Premium Service Industry Code C637:2009 (MPS Code)*.

The MPS Code was registered by the Australian Communications and Media Authority (**ACMA**) in May 2009 and came into effect on 1 July 2009.

BACKGROUND

Axis Legal is a Sydney based law firm specialising in IT, IP, Digital Media, Marketing and Advertising, and has had 5 years' experience in advising on legal issues arising in the mobile and premium rate service industry. Our firm has acted (and continues to act) for numerous mobile content providers and aggregators. It is safe to say that we are well versed in the intricacies of this industry, and the labyrinth of legislation and industry codes that apply.

Over the past 5 years, we have had numerous dealings with ACMA relating to compliance issues in these industries which as evidenced at the ACMA's website, irrespective of size or reputation. As a result of our communications with ACMA, our legal interpretation of the *Spam Act 2003 (Spam Act)* has resulted in modifications to the ACMA's form of Investigation Notice. Our firm also acted in the first mobile spam cases in Australia and has dealt with similar legal issues in the UK for its international clients. We thus are considered to be "veterans" in such an area that is still considered "emerging" in Australia.

As a legal advisor for numerous clients in relation to Premium SMS/MMS Service (**PSMS**), Axis Legal has an important stake in the *Telecommunications Act 1997 (Act)*, the Spam Act and the MPS Code.

Level 1, Suite 5B
2 - 12 Foveaux St
Surry Hills NSW 2010
PO Box K353
Haymarket NSW 1240
tel +612 8204 1100
fax +612 9211 3836
ABN 12 112 558 602

Intellectual Property
Information Technology & Internet
Media, Marketing & Advertising
Entertainment
Business Law
Dispute Resolution

Axis Legal recognises that the MPS Code aims to establish appropriate community safeguards and customer service requirements for PSMS by implementing rules and requirements for tighter advertising controls, double opt-in, and improved customer service and complaint handling.

Whilst Axis Legal fully supports the increased protection in the interest of the public, we are concerned that the MPS Code has had serious adverse ramifications which go beyond the purpose of protecting the public based on existing statutes and the common law. In particular, Axis Legal is of the opinion that the “double opt-in” requirement is inconsistent with statutes and the common law (see below). We also point out that the MPS Code is subject to the Spam Act and, where there is any conflict between the MPS Code and the Spam Act, the Spam Act will always prevail.

Our comment focuses on the double opt-in requirements, and specific comments and suggestions are as follows.

PARTICULAR SUBMISSIONS FOR REVIEW OF THE MPS CODE

1. DOUBLE OPT-IN

Clauses 5.1.1 and 5.1.2 of the MPS Code provide that a Content Supplier must not supply a service without receiving a customer’s Mobile Originated (**MO**) message. Clauses 4.3.1, 4.3.2, 4.4.1 and 4.4.2 of the MPS Code state that the MO Message is a responding message to the Content Supplier’s free message checking whether or not the customer’s initial request to purchase or subscribe to a PSMS is genuine. In other words, the MO Message is sent to a Content Supplier’s particular shortcode (as advertised) in order to confirm their wish to purchase or subscribe.

This is known as the “*Double Opt-In*” requirement. Clause 4.4 of the *Guidelines of Mobile Premium Service Industry Code G638:2009* (**Guidelines**) provides the reason for adopting this double opt-in requirement is as follows:

“This is essential to help ensure that the person requesting the subscription is also the owner of the handset”.

Axis Legal acknowledges that certain tools need to be adopted to verify the identity of the actual account holder when a PSMS is requested, but the double opt-in operates so as to require a Content Supplier to obtain **two independent confirmations** of consent from a customer before supplying a PSMS. In other words, a Content Supplier must obtain *additional* consent from a customer who has already provided his/her express/implied consent to purchase or subscribe to the services.

Axis Legal considers that this misapplication of the term “consent” under the MPS Code is inconsistent with the historical and long standing definition under statute and at common law.

1.1 Inconsistency with Statute

1.1.1 The Spam Act

The definition of “consent” under the Spam Act includes express and implied consent. Paragraph 2 of Schedule 2 of the Spam Act provides that:

*“For the purposes of this Act, **consent** means:*

(a) express consent; or

(b) consent that can reasonably be inferred from:

(i) the conduct; and

*(ii) the business and other relationships;
of the individual or organisation concerned”.*

According to the *Explanatory Memorandum of Spam Bill 2003 (Explanatory Memorandum)*, “express consent” relates to a person actively requesting the sending of messages from the service provider (the sender).

The Explanatory Memorandum also gives examples of what amounts to providing explicit consent at page 114-115, as follows:

- “• the person has subscribed to the sender’s electronic advertising mail list;
- *the person has ticked a box in information provided to the person which consents to future electronic receipt of advertising material;*
- *the person has specifically requested such material (either verbally or in writing) from the sender;*
- *a person has voluntarily entered into an agreement to have their electronic address provided to third-parties for marketing purposes.”*

Thus, if a person has specifically and voluntarily requested to purchase or subscribe to particular service (which of course must include all required information, such as sender details, costs, frequency (if relevant), helpline information and functional unsubscribe facility), it would amount to providing express consent. This would not contravene section 16(1) of the Spam Act, which only prohibits the sending of unsolicited commercial electronic messages (**CEMs**).

The Spam Act also envisages that a company may have a suite of services (or a Joint Venture with another company where the client database is shared and notified to its members as such), and the database members have already agreed to receive marketing CEMs from the company or its business’ partners so long as the services are of the kind that would be expected to be of interest. Therefore, if a customer subscribes to entertainment services then sending the customer CEMs for financial services will not be implied consent. This is a fairly standard requirement and appears in most company’s service terms and conditions and in Privacy notices.

Page 63 of the Explanatory Memorandum defines “sending” as a physical act done by a person:

“This penalty provision would cover the person who actually sent the message (ie by hitting the send button or dialling the relevant telephone number), the author of the message (who caused the message to be sent), or another person who authorised the message to be sent (even if they got a third party to send it on their behalf).

However in the case where a person’s computer has been hijacked and a spammer is sending messages in contravention of clause 16 without the computer owner’s knowledge, or where a virus has infected a person’s computer and results in the sending of messages in contravention of clause 16, then the computer owner would not be ‘sending’ the message in contravention of clause 16. The generally accepted meaning of the term ‘send’ involves some knowledge and initiation on behalf of the ‘sender’. The penalty attaches to the person, not the hardware (for example the computer or mobile phone). Therefore, while a person’s hijacked computer may have ‘sent’ the message the person themselves would not have sent or caused the message to be sent.”

Bearing in mind that at the time of drafting this Explanatory Memorandum, PSMS was not as prevalent in the market place, so the example provided of hijacking or spamming relates to email. Nevertheless, it does not alter the well understood definition of “to send”.

So, applying it to the contemporary concept of mobile phones and PSMS, it is undeniable that the actual behaviour of “sending” a message is exactly the same as the definition in the Explanatory Memorandum, that is by hitting the send button or dialling the relevant telephone number (which would include a shortcode). If someone sends a message by hitting a button on his/her mobile phone, it is regarded as “sending a message by himself/herself” unless it was done by “hijacker or spammer”. In this regard, a “spammer” refers to a person or company that is known to send spam (such as missed call marketing or actual scams as notified from time to time). It does not refer to Content Providers who comply with the Spam Act and Privacy Act.

We also wish to draw attention to section 18A of the *Acts Interpretation Act 1901*, which says:

“unless the contrary intention appears, where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings.”

The words “sending” and “unsolicited” can only mean what they are defined to mean according to a dictionary or as per the Explanatory Memorandum.

We also refer to section 4 of the *Legislative Instruments Act 2003* that defines “enabling legislation” as in relation to a legislative instrument to mean:

“the Act or legislative instruments, or the part of an Act or of a legislative instrument that authorises the making of the legislative instrument concerned.”

Therefore the meaning given to “sending” and “unsolicited” in the Explanatory Memorandum (as an enabling legislation) forms part of the Spam Act, and must be applied.

We thus submit that the MPS Code purports to invalidate the Spam Act definition of “consent” by rejecting that a request by a customer to receive PSMS is express consent, and by requiring a Content Supplier to obtain a customer’s consent twice even though the customer expressly consented to purchase the PSMS by sending a request message.

The way that the MPS Code currently operates is that a Content Provider will never be able to argue that there was express consent where a consumer physically requests the services by sending the relevant keyword to an advertised shortcode in order to purchase services. Moreover, if there is no express consent as defined, then it must also mean that the definition of “implied consent” has altered.

Suppose the situation that a provider sends a CEM to a customer and is fully compliant with the requirements of the Spam Act and other provisions of MPS Code, but has not implemented the “double opt-in”. How could the sender of the message be penalised under the MPS Code, but not under the Spam Act (which says this is express consent)?

Where there is inconsistency between the Spam Act and the MPS Code in relation to double opt-in, the Spam Act prevails.

1.1.2 The Privacy Act and Telecommunications Act

The concept of “consent” is also covered in the *Privacy Act 1988* (**Privacy Act**) and it has the same definition as provided in the Spam Act. Section 6 of the Privacy Act provides:

*“**consent** means express consent or implied consent.*

... ”

(2) For the purpose of this Act, an act or practice breaches an Information Privacy Principle if, and only if, it is contrary to, or inconsistent with, that Information Privacy Principle”

Section 14 of the Privacy Act also provides provisions regarding “consent” that:

“A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the individual concerned has consented to use of the information for that other purpose...”

We also draw attention to the *National Privacy Principles*, which is provided in Schedule 3 of the Privacy Act states that:

*“An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:*

(a) both of the following apply:

- (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
- (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; ...”

If a customer positively sends an SMS to subscribe to PSMS based on fully compliant advertising from his/her mobile phone, this is captured electronically by the Aggregator's software platform. It means that there is evidence that this initial communication was sent by the holder of that particular mobile phone number.

If a customer agrees to purchase or subscribe to a Content Supplier's PSMS via a direct request on his/her mobile phone, this can only mean that the person's mobile phone number has been willingly provided for the receipt of the PSMS. This is therefore not a breach of privacy. If there is no breach of the Privacy Act, then there is no breach at all.

In support, we draw attention to section 116A of the Telecommunications Act that says:

“...neither an industry code nor an industry standard derogates from a requirement made by or under the Privacy Act.”

We also note section 111B(1) of the Telecommunications Act, which defines an “unsolicited CEM” as:

*“an **unsolicited commercial electronic message** is a commercial electronic messages that is sent:*

- (a) without the consent of the relevant electronic account-holder; or
- (b) to a non-existent electronic address.”

Axis Legal submits that this also supports the existence of inconsistency and invalidity of the double opt-in requirement in the MPS Code (in relation to an MO Message) having regard to both the Privacy Act and the Telecommunications Act.

1.2 The Australian Constitution and Common Law

In *Mudginberri Station Pty Ltd v Langhorne* (1985) 7 FCR 482 at 490 the court upheld the plaintiff corporation's right to carry on its business without executive interference, saying:

“We think that, in the absence of any statutory prohibition, citizens of this country have a common law right to prepare goods for sale and to sell them here or overseas”.

In Australia, person generally has a right to do anything that is not expressly prohibited by law. This residual freedom applies equally for the benefit of corporate and natural persons. The implied freedom of trade is also found in section 92 of the *Constitution of the Commonwealth of Australia 1900* (**Constitution**).

The double opt-in requirement under the MPS Code hinders a Content Supplier from operating legitimate businesses freely. Axis Legal submits that the enforcement of the double opt-in requirement (for MO Message, which is not supported by either the Spam Act or Privacy Act) is clearly discrimination against legitimate PSMS businesses, and is potentially unconstitutional as it interferes with free trade in Australia.

1.3 Discrimination against PSMS Businesses

In the instance of traditional bargaining in the market place, once a customer expressly requests to buy goods, the vendor does not ask the consumer again to confirm his/her intention to purchase that item for fear of being in breach of the law. However, under the MPS code the same customer when purchasing a PSMS must express his/her intention twice to comply with the double opt-in requirement.

We consider that this harsh restriction is invalid and imposes harsh discriminatory requirements which single out a particular industry sector, namely Content Suppliers of the PSMS.

Axis Legal's Suggestions

In consideration of the above, Axis Legal submits that the double opt-in requirement as presently drafted must be removed from the MPS Code so as not to apply to the receipt of an MO Message, and the previous requirements under the *Mobile Premium Services Industry Scheme (MPSIS)* be reinstated. The original MPSIS correctly distinguished a request for PSMS via either a landline or over the internet versus a physical request being made for an owner's mobile phone. This sufficiently protects customers from being subscribed to, or purchasing services, unwillingly and without their knowledge.

Regard must also be had to the information provided by Content Providers through information about the PSMS provided in advertising, and supplying an unsubscribe process. Currently, customers who have actually purchased PSMS (or subscribed to them) have been able to plead ignorance to the law is being able to deny existence of an MO Message request.

2. MPS Register in CommsAlliance

Under clause 4.1 of the MPS Code, Aggregators and Content Suppliers must complete a registration process with the CommsAlliance.

Axis Legal understands and agrees that the aim of this requirement is to increase the visibility, and accountability of Content suppliers and Aggregators to their customers.

According to the Terms and Condition for Mobile Premium Services Register (**MPS Register**) on the CommsAlliance's website: the information relating to the services offered under a particular shortcode is stored in the MPS Register, and is provided to an Aggregator by a Content Supplier when it requests a new shortcode.

It is usual practice for Aggregators to require their client to complete forms describing the intended services and once a shortcode is provided, the Aggregator uploads this information onto the MPS Register on the client's behalf.

The 19 Service Finder's database is used by customers who want to obtain the name of the Content Supplier so as to identify the billed items appearing on the customer's mobile phone bill.

As evident, the only instance where registration of shortcodes in the MPS Register protects the public, would be when a shortcode or the name of a PSMS appears on a consumer's bill (eg "*XYZ ringtone*") that a consumer does not immediately recognise.

These sorts of queries arise because mobile phone bills are often issued to customers up to one month after the customer purchased the content, and the service is not always described adequately on these bills. In that case, the relevant information can be obtained by the customer through the 19 Service Finder.

Moreover, having regard to the fact that content suppliers usually use their brand when promoting their PSMS (rather than a corporate name, in a similar way that FMCGs will also advertise using a specific brand name for a product), having just the content supplier's name appearing in the 19 Service Finder is of little or no use to the customer in identifying what PSMS was purchased.

For example, one of our clients legitimately provides popular PSMS worldwide using a brand that does not incorporate its company name. Customers in Australia who purchase the PSMS upon viewing the advertisement, and then subsequently receives a mobile phone bill with these charges on it, only finds the company name and its overseas office phone number etc, with no reference to the brand of the PSMS on the 19 Service Finder.

If the customer then does an internet search of the company name to check what the billed was in relation to, the customer would have difficulty in immediately verifying the PSMS that was purchased. As a result, this does not prevent customers making complaints to either their Carrier, the TIO or to ACMA, even though it may later be found that the customers did in fact purchase the services (which are delivered to the customer's handset). This is clearly evident in that several complaints are found to be no more than an excuse to not pay a bill.

We believe that the shortcode information in the MPS Register must therefore have identifiable relevance to consumers.

Axis Legal's Suggestions

Axis Legal submits that a purchaser of the PSMS will easily recognise the brand and this alone would assist them to recall the fact he or she purchased the services.

Axis Legal suggests that the shortcode information listed by content suppliers in the MPS Register should include both the brand of the content supplied as well as the company name. This would reduce the number of complaints and be informative for customers.

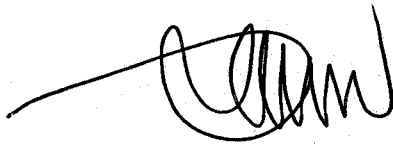
CONCLUSION

Once again, Axis Legal thanks CommsAlliance for allowing it the opportunity to provide comments on the MPS Code. In summary, the key points made in this submission are:

- the MPS Code should be amended to have double opt-in provision removed as it is inconsistent with the Spam Act and the Privacy Act and therefore invalid. The MPS Code imposes an undue restriction on the PSMS industry and is likely to be unconstitutional as it is invalid.
- the MPS Register and the 19 Service Finder should include the PSMS content brand name as well as the content provider's corporate name, in order for the appropriate information to be accessible by consumers.

We look forward to the outcome after this review of the MPS Code. Should you have any questions concerning this submission, please do not hesitate to contact me or Noel Kim of this office.

Yours faithfully
Axis Legal Pty Limited



Sara Delpopolo
Principal
 Phone: 02 8204 1100 Fax: 02 9211 3836
 Email: sdelpopolo@axislegal.com.au